IX10

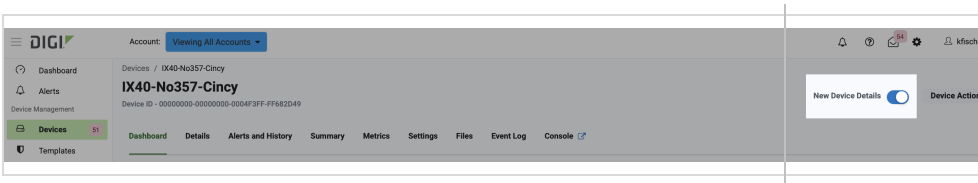
User Guide

Firmware version 25.2

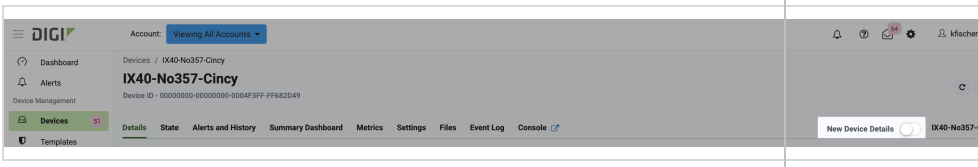
Revision history—90002399

Revision	Date	Description
V	April 2025	Release of Digi IX10 LTS firmware version 25.2. ■ **We've adopted a Long-Term Support (LTS) release strategy. What does this mean for you?** • *Increased stability and security.* Our LTS firmware is aligned with the Linux kernel LTS firmware, which means it is based on a stable and long-term supported version of the Linux kernel. This allows for regular security updates and bug fixes ensuring that the firmware benefits from the reliability and performance improvements provided by the LTS kernel. **Note** To see how we plan to respond to known security vulnerabilities in products that use the DAL OS firmware, see DAL Vulnerability Patch Policy on the digi.com website. • *Fewer releases.* Plan your updates without the pressure of a quarterly timebox. This is the first release of the LTS firmware. Patch releases for security or bug fixes will be released and announced throughout the year. Feature updates will be released and announced as they are ready. ■ **"Premium features" has been renamed to "Subscriptions".** The word *Subscriptions* more accurately describes the services in which you have enrolled and the ongoing payments associated with them. ■ **Assign a static address to a network interface on a device with IPv6 enabled.** When using IPv6, you can now assign a static address to a network interface on your device, ensuring consistent identification and connectivity of devices on the network. ■ **Improved disconnect/reconnect to Digi Remote Manager for a device when upgrading cellular modem firmware over the air (OTA).** Device downtime is minimized so service is minimally interrupted. ■ **New banner notification in the Web UI and CLI.** A new banner notice has been added to the web UI and CLI to indicate when the configuration of a device is being managed by a template in Digi Remote Manager. This is useful so that configuration changes to that device are not made locally. If there are issues with the device, then it is important to know that the configuration is enforced

		remotely and any changes you may make to the device for testing purposes or fixes may be overwritten by the template. ■ **Regional cellular modem firmware bundles are now available.** Certain modems - Sierra EM9191 (Asia PAC) and EM7690 (worldwide) - have a lot of carrier-specific firmware images. Due to size constraints of the file system on the IX10, not all of these images could be included. Now you can choose the firmware bundle for your specific cellular modem. ■ **IPsec is now supported in FIPS mode.** It's now easier for you to meet the federal security standards required by FIPS and keep sensitive data safe during transmission. ■ **FIPS mode is automatically enabled when PR mode is enabled.** When in PR mode, It's now easier for you to meet the federal security standards required by FIPS and keep sensitive data safe during transmission. **Tip** For more information about this release, see the digi.com blog post, New Features in Digi Remote Manager and Our First LTS Firmware Release for DAL OS.
U	February 2025	Release of Digi IX10 firmware version 24.12. ■ **New user guide** - There's a new **Modem firmware user guide**! With added functionality in DAL OS 24.12.x firmware and Remote Manager, there's now even more ways to upgrade the modems in or attached to your Digi routers. Make sure to review the **Before you begin** topic too because the options available to you depend on the DAL OS firmware version you are running. ■ **Additional query state categories added** - Are you running DAL OS firmware 24.9 or newer on your devices? See the new categories added to the device-specific query state view in Remote Manager. Monitor device status in real time for Watchdog, Location, DHCP leases, SureLink, and many more groups! **Note** The new query state metrics in the updated view do not replace datastream metrics. However, datastream metrics will be phased out later this year as we enhance query state metrics with additional categories. How you see this new information depends on whether you using the legacy or new device details view. • Click the **Details** tab and then select a group (for example, Ethernet) to see its status. The **New Device Details** toggle key must be on to see this view.



- Click the **State** tab and then select a group (for example, Ethernet) to see its status. **The New Device Details** toggle key must be off to see this view.



- If you enable Primary Responder Mode, your device will reboot and the device's configuration will change to use the this mode. There are certain firmware features that are disabled in this mode. For more information, see Differences between standard firmware operation and Primary Responder mode.
- FIPS mode is automatically enabled when PR mode is enabled.
- Restoring a backup configuration file is disabled. For more information, see Restore the device configuration.
- The **system custom-default-config** CLI command available in release 24.12 cannot be run in Primary Responder mode.
- Add or remove custom default configuration files using the **system custom-default-config** CLI command.

  Note This new CLI command replaces the **system backup / type custom-defaults** and **system backup / remove custom-defaults**.

- Python is no longer included as part of the base DAL OS firmware for the IX20 and IX30 routers.

  Note If you require Python in your environment and your device is running 24.12.x or newer firmware, see Install Python for information about installing it separately from the firmware.

Tip For more information about this release, see the blog post, Digi Software Enhancements for DAL OS 24.12 Firmware and Digi Remote Manager.

T	November 2024	Release of Digi IX10 firmware version 24.9. **CAUTION!** For the EX, IX, and TX product lines, upgrade to 24.6 before 24.9. Firmware 24.6 has firmware encryption support and is a step-update.

- **Modem firmware updates**: There's no more guesswork about the carrier you need to choose when upgrading modem firmware. Now, choose a firmware bundle based on the type of modem you have. There's no need to know and/or specify the carrier because every firmware upgrade package includes all of the carrier images supported by Digi routers. The The modem firmware update is done using the modem firmware bundle ota CLI commands.
- **New EDP client written in Rust**: The new client connector for how devices establish their connections to Digi Remote Manager, provides a faster connection, reduces data consumption, and includes Watchdog support.
- **Configuration validation and automated rollback to maintain remote access to your devices**:
  Maintain remote access to your devices that have DAL OS 24.9 firmware or newer. Any configuration changes made by a template that result in devices losing connection to Remote Manager are automatically rolled back. To see whether configuration changes were rolled back, you can view the history of a device. For more information, see the Templates user guide.
- **Cellular connectivity enhancements**:
  - Modem manager has been updated to version 1.22.0.
  - Modems are tracked by name instead of index.
  - Default modem signal/status update interval changed from 30s to 10s.
  - Default PDP context changed from 2 to 1.
  - PDP context ID stored & read from mm.json to ensure stability when updating from 24.6 to 24.9.
- **Miscellaneous enhancements**:
  - No authentication SMTP option: Send emails without encryption.
  - Download peer settings: If you are using a Digi device as a WireGuard server and you have a lot of client devices connected to it, you now have the option to download the template with all the settings and use it to configure other devices.
  - Confirmation is now required to perform a system factory erase in the CLI.
  - `DefaultIP` renamed to `SetupIP` in reporting metrics and CLI configuration.
  - Network type, band, and signal strength are now included in speed test information reported from the device to Digi Remote Manager.
  - **Primary Responder mode**:
    - SSH is disabled by default.
    - Users are now prompted to enable two-factor authentication when changing their password.

		■ **Modbus hardening**:Take a look at the new Modbus hardening topic and use case about enhancing the security and reliability of Modbus communications between devices over your network. ■ **Digi 360**: See the new Digi 360 Home page and FAQs. **What's coming** When accessing the device locally through the Web UI or CLI, you will be able to see more metrics in **Settings** > **Status**, such as connection status and network details. Though not much else changes in this release, the work behind the scenes is foundational. Coming soon, data streams in Digi Remote Manager will be replaced with a comprehensive view about the status of your devices. What you see in the local Web UI or CLI is what you will see in Digi Remote Manager. **Tip** For more information about this release, see the blog post called, "Announcing the Latest Digi Software Solutions for DAL OS 24.9 Firmware" on digi.com.
S	July 2024	Release of DigiIX10 firmware version 24.6. **Note** Firmware encryption support has been added. This release is a step update for the future 24.9+ release. ■ System time synchronization: You can now configure how often you want your IX10 to synchronize its system time. Configure the duration of the synchronization (default is set to 1 day), as well as continue to have it synchronize at start-up and when there is a change in the default route. See System time synchronization for more information. ■ New **Device managed public key** setting for WireGuard VPN: For server mode, enable the IX10 to generate a public and private key pair for a peer. See Configure the WireGuard VPN. ■ New metrics views for the Watchdog service: View metrics in the local web UI or use the new CLI command. See test failures in Digi Remote Manager. See Watchdog service. ■ **Isolate clients** setting: Now enabled by default in the **Network** > **SD-WAN** > **Wi-Fi** > **Access Points** configuration. This prevents all clients attached via Wi-Fi from communicating with other clients on the same access point. ■ Ethernet port setting change: The new default **Type** setting for the Ethernet port is now **Hybrid IP Address** (**Interfaces** > **ETH** > **IPv4** > **Type**). The Ethernet port acts as a WAN (DHCP client) but automatically changes to LAN DHCP server if no WAN connections occurs within one minute of reboot. The benefit is for customers provisioning or staging these routers. There is no need to insert a SIM card in each device or make local UI changes for every device if you just want to get it online to upgrade device or modem

		firmware and apply some basic configuration settings for provisioning or staging purposes. See Review default settings. ■ **Enable event log uploads** setting: This setting (**Monitoring** > **Device** event logs) is now enabled by default. Uploading event logs to Digi Remote Manager now occurs automatically. ■ New **default trusted zones**: There were no default trusted zones set up by default. The service could be accessed from any zone. Now, it can be accessed via three trusted zones: Default, Edge, and IPsec. See Configure the Modbus gateway.
R	April 2024	Release of Digi IX10 firmware version 24.3: ■ WireGuard VPN - Configure a WireGuard VPN where your device can act as a client or as a server. ■ System watchdog - Two new configuration settings: • **Interface tests** - Configure a reboot of the interfaces you configure after a specified amount of time. • **Modem monitoring** - Configure a power cycle of the modem after an initial timeout instead of that timeout being reported as a failure. ■ SNMP trap and email notification for events - Configure an SNMP v2 trap and/or email notification to be sent when an event occurs. ■ Configure a GRE tunnel - Configure your tunnel to use Ethernet over GRE (**GRETAP** setting). ■ Configure cellular modem(s) - Configure your cellular modem(s) to include or exclude certain 4G bands. ■ Serial disconnect - Disconnect any users connected to a serial port configured for one of these modes: Login, Remote Access, PPP Dial-in, or Modem Emulator. ■ Serial port information - Display information about the serial ports on the Dashboard. **Tip** For more information about this release, see the blog post called, "Announcing the Latest Digi Software Solutions for DAL OS 24.3 Firmware" on digi.com.
P	January 2024	Release of Digi IX10 firmware version 23.12: ■ Updated Active SIM slot definition: Configure cellular modem. ■ FIPS feature is available for all DAL devices. Enable FIPS mode ■ Link OSPF routes through a DMVPN tunnel and allow for redirection of packets between spokes. Configure a DMVPN spoke. ■ New setting which allows device to initiate a Realport connection to a remote server. Configure the RealPort service.

		■ New **After** option for the SIM preference schedule. Configure cellular modem. ■ New **BOOTP dynamic allocation** option. Configure a DHCP server. ■ Renamed SureLink **Attempts** configuration setting to **Surelink test failures** to better indicate what this setting does. ■ New **Telnet Login** setting to control whether a user must supply credentials when opening a Telnet connection to access a serial port on a service. Configure serial authentication. ■ New Advanced watchdog **Modem check and recovery** setting to control whether watchdog will monitor initialization of the IX10 cellular modem. Watchdog service. **Tip** For more information about this release, see Announcing the Latest Digi Software Solutions for DAL OS 23.12 Firmware and Digi Remote Manager on digi.com.
N	October 2023	Release of DigiIX10 firmware version 23.9: ■ Register a device to DRM: • Added a link to the Dashboard of the local web UI to register and add the device to Digi Remote Manager. ■ Updated Dashboard: • Updated the layout of the Dashboard page of the web UI to combine the network interface and cellular modem details into a single Network Activity panel. ■ Primary Responder: • Added Primary Responder mode setting to lock down the device to comply with AT&T FirstNet and Verizon Response. ■ Domain allow list: • Added a Domain allow list feature to control what domains are accessible through the Digi device. ■ Fallback: • Added a fallback server setting to control which DNS server is used as the fallback in the event that no configured or DHCP-obtained DNS servers are available. ■ MACsec tunnel: • Added information about adding a MACsec tunnel.
M	July 2023	Release of DigiIX10 firmware version 23.6: ■ Serial port options: • For **PPP Dial-in** mode, added the **Default Route** option to control whether a default route gets added for the PPP interface. • Documented the new **Modem emulator** mode, which allows serial ports to act as a dial-up modem emulator for handling incoming AT

		dial-ins. ■ Advanced Watchdog options: • Added **System** > **Advanced Watchdog** options to all devices. ■ Digi Remote Manager support: • Each time a device connects to Digi Remote Manager after the device boots (or re-boots), the device now immediately uploads all health metrics. ■ VPN: • Added new **Enable open routing** configuration setting (**VPN** > **IP tunnels**) to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel. ■ Networking: • Added new **TCP retries2** configuration setting (**Network** > **Advanced**) to control the number of times an unacknowledged TCP data packet will be retransmitted before the connection is considered lost.
L	May 2023	Release of Digi IX10 firmware version 23.3: ■ Surelink: • Redesigned Surelink configuration settings. • Added **show surelink state** Admin CLI command to display the overall pass/fail status of enabled Surelink tests. ■ New configuration settings for LXC containers: • **Start on boot** to configure the container to start when the system boots. • **Restart timeout** to configure the container to restart if it stops. • **Optional parameters** to include optional parameters for the container. • **Mounted directories** to setup shared directories between the host filesystem and the container. ■ Added a **AT&T LWM2M support** setting to enable or disable AT&T lightweight M2M on cellular modems. ■ VPN: • DMVPN phase 1 spoke support with NHRP or mGRE, including compatibility with Cisco DMVPN hubs. • Added support for SHA2 ciphers for IKEv2 IPsec tunnels. ■ Disabled mDNS by default for improved cellular performance. ■ If the device has a configured **System** > **Name**, it is now displayed on the Dashboard.
K	December 2022	Release of Digi IX10 firmware version 22.11: ■ Updated the Linux kernel to version 5.19.

		■ The intelliFlow feature now integrates with Digi Remote Manager to provide aggregated insights and analytics for all Digi devices in your environment. ■ Added an MQTT broker service, including support for: • Multiple MQTT clients with unique topics and authentication credentials. • Pre-shared key encryption with multiple configurable keys. • Pattern filtering for topic access control. ■ Added FIPS mode, to provide Federal Information Processing Standards (FIPS) 140-2 compliance. ■ Added support for Next-hop routing protocol (NHRP). ■ Added support for mGRE tunnels. ■ Added support for ICMP redirect messages. ■ Added a polling interval to control how often the cellular modem is polled for signal strength and other status. ■ New commands: **tail** and **grep**. ■ Add **Timeout** option to modem **Carrier Scan** window in the Web UI. ■ Added advanced watchdog to: • Monitor critical services and reboot the device if those services fail. • Monitor memory usage and log errors or reboot the device based on current memory usage. ■ Added the ability to have serial port data written to the system log. • Removed options in the local web UI and Admin CLI for manually starting, stopping, and clearing serial logs. These actions are now controlled under the data logging configuration settings.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2025 Digi International Inc. All rights reserved.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Customer support

Gather support information: Before contacting Digi technical support for help, gather the following information:

- Product name and model
- Product serial number (s)
- Firmware version
- Operating system/browser (if applicable)
- Logs (from time of reported issue)
- Trace (if possible)
- Description of issue
- Steps to reproduce

Contact Digi technical support: Digi offers multiple technical support plans and service packages. Contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (IX10 User Guide, 90002399 L) in the subject line of your email.

Contents

What's coming 6

IX10 User Guide

DAL OS Vulnerability Patch Policy 26
Digi 360 27
    Frequently asked questions 27

Digi IX10 Quick start

Step 1: What's in the box 31
Step 2: Gather accessories 32
Step 3: Connect your device 33
Apply Dielectric Grease over SIM Contacts 33
Step 4: Connect DC power 34
Step 5: Set up access to Digi Remote Manager 34
Step 6: Register your device 35
Step 7: Complete setup 35
Step 8: Configure the cellular APN 35

Digi IX10 hardware reference

Digi IX10 features and specifications 36
IX10 accessories 36
IX10 front and side views 36
IX10 LEDs 37
    Power (PWR) 38
    SIM 38
    LTE 38
    Signal quality indicators 39
    Ethernet Link and Activity 40
    Cellular signal quality explained 40
IX10 power supply requirements 42
Digi IX10 serial connector pinout 42
    10-pin serial cabling options 43
QR code definition 43

Digi IX10 hardware setup

Install SIM cards 45

Apply Dielectric Grease over SIM Contacts ... 46
SIM removal ... 46
Tips for improving cellular signal strength ... 46
Connect data cables ... 46
Mount the IX10 device ... 46
Attach to a mounting surface by using the mounting tabs ... 47
Attach to DIN rail with clip ... 47

Firmware configuration

Review IX10 default settings ... 51
Local WebUI ... 51
Digi Remote Manager ... 51
Default interface configuration ... 51
Other default configuration settings ... 53
Primary Responder mode ... 53
Differences between standard firmware operation and Primary Responder mode ... 54
Enable Primary Responder mode ... 54
Change the default password for the admin user ... 56
Configuration methods ... 57
Using Digi Remote Manager ... 58
Access Digi Remote Manager ... 58
Using the local web interface ... 59
Review the dashboard ... 59
Log out of the web interface ... 60
Review the dashboard ... 60
Use the local REST API to configure the IX10 device ... 61
Use the GET method to return device configuration information ... 61
Use the POST method to modify device configuration parameters and list arrays ... 63
Use the DELETE method to remove items from a list array ... 64
Using the command line ... 65
Access the command line interface ... 65
Log in to the command line interface ... 65
Exit the command line interface ... 66

Central management

Digi Remote Manager support ... 68
Certificate-based enhanced security ... 68
Configure your device for Digi Remote Manager support ... 68
Collect device health data and set the sample interval ... 75
Event log upload to Digi Remote Manager ... 78
Reach Digi Remote Manager on a private network ... 80
Pinhole method ... 80
Proxy server method ... 80
VPN Tunnel method ... 80
Log in to Digi Remote Manager ... 80
Use Digi Remote Manager to view and manage your device ... 82
Add a device to Remote Manager ... 82
Add a device to Remote Manager using information from the label ... 82
Add a device to Remote Manager using your Remote Manager login credentials ... 83
Configure multiple IX10 devices by using Digi Remote Manager configurations ... 84
View Digi Remote Manager connection status ... 85
Learn more ... 86

Interfaces

Wireless Wide Area Networks (WWANs) 88
- Configure SureLink active recovery to detect modem failures 88
- Configure the device to reboot when a failure is detected 103
- Disable SureLink 116
- Using cellular modems in a Wireless WAN (WWAN) 124
- Configure a Wireless Wide Area Network (WWAN) 143
- Show WWAN status and statistics 153
- Delete a WWAN. 155

Local Area Networks (LANs) 157
- About Local Area Networks (LANs) 159
- Configure a LAN 159
- Change the default LAN subnet 166
- Change the LAN address type 167
- Show LAN status and statistics 168
- Delete a LAN 170
- Configure an interface to operate in passthrough mode 171
- DHCP servers 177

Virtual LANs (VLANs) 193
- Create a trunked VLAN route 195
- Create a VLAN using switchport mode 196

Show SureLink status and statistics 199
- Show SureLink State 199
- Show SureLink status for all interfaces 199
- Show SureLink status for a specific interface 200
- Show SureLink status for all IPsec tunnels 200
- Show SureLink status for a specific IPsec tunnel 201
- Show SureLink status for all OpenVPN clients 201
- Show SureLink status for a specific OpenVPN client 202

Serial port

- Default serial port configuration 203
- Serial mode options 203
- View serial port information 203

Default serial port configuration 203
Configure Login mode for a serial port 204
Configure Remote Access mode for a serial port 208
Configure Application mode for a serial port 224
Configure PPP dial-in mode for a serial port 226
Configure UDP serial mode for a serial port 233
Configure Modem emulator mode for a serial port 244
Configure Modbus mode for a serial port 247
Configure RealPort mode using the Digi Navigator 250
- Installation and configuration process 251
- Digi Navigator features 251
- Install the Digi Navigator 251
- Configure RealPort on a Digi device from the Digi Navigator 253
- Install and configure RealPort on your computer 254
- Digi Navigator application features 256

Advanced RealPort configuration without using the Digi Navigator 267
- Windows Operating System 267
- Linux Operating System 267

Download the RealPort driver ... 267
Configure RealPort on your computer ... 268
Configure the serial port for RealPort mode ... 269
Configure the RealPort service ... 273
Disconnect a user from a serial port ... 275
Show serial port status and statistics ... 277
Serial Status page ... 277
Review the serial port message log ... 279

Routing

IP routing ... 282
Configure a static route ... 283
Delete a static route ... 286
Policy-based routing ... 287
Configure a routing policy ... 288
Example: Dual WAN policy-based routing ... 295
Example: Domain-based routing with dual WAN ... 297
Example: Route traffic to a specific WAN interface based on the client MAC address ... 300
Routing services ... 305
Configure routing services ... 306
Show the routing table ... 308
Dynamic DNS ... 309
Configure dynamic DNS ... 310
Virtual Router Redundancy Protocol (VRRP) ... 314
VRRP+ ... 315
Configure VRRP ... 315
Configure VRRP+ ... 318
Example: VRRP/VRRP+ configuration ... 326
Configure device one (master device) ... 326
Configure device two (backup device) ... 330
Show VRRP status and statistics ... 335

Virtual Private Networks (VPN)

IPsec ... 339
IPsec data protection ... 339
IPsec mode ... 339
Internet Key Exchange (IKE) settings ... 339
Authentication ... 340
Configure an IPsec tunnel ... 340
Configure IPsec failover ... 366
Configure SureLink active recovery for IPsec ... 369
Show IPsec status and statistics ... 384
Debug an IPsec configuration ... 385
Configure a Simple Certificate Enrollment Protocol client ... 386
Example: SCEP client configuration with Fortinet SCEP server ... 393
Show SCEP client status and information ... 398
OpenVPN ... 400
Configure an OpenVPN server ... 401
Configure an OpenVPN Authentication Group and User ... 410
Configure an OpenVPN client by using an .ovpn file ... 414
Configure an OpenVPN client without using an .ovpn file ... 417
Configure SureLink active recovery for OpenVPN ... 421

Show OpenVPN server status and statistics 436
Show OpenVPN client status and statistics 437
Generic Routing Encapsulation (GRE) 439
Configuring a GRE tunnel 439
Show GRE tunnels 444
Example: GRE tunnel over an IPSec tunnel 445
Dynamic Multipoint VPN (DMVPN) 459
Configure a DMVPN spoke 460
L2TP 466
Configure a PPP-over-L2TP tunnel 466
L2TP with IPsec 476
Show L2TP tunnel status 476
L2TPv3 Ethernet 478
Configure an L2TPv3 tunnel 478
Show L2TPV3 tunnel status 482
MACsec 484
Configure a MACsec tunnel 484
NEMO 486
Configure a NEMO tunnel 487
Show NEMO status 491
WireGuard VPN 492
Configure the WireGuard VPN 493

Services

Allow remote access for web administration and SSH 502
Configure the web administration service 505
Configure SSH access 515
Use SSH with key authentication 522
Generating SSH key pairs 522
Configure telnet access 525
Configure DNS 530
Show DNS server 536
Simple Network Management Protocol (SNMP) 537
SNMP Security 537
Configure Simple Network Management Protocol (SNMP) 537
Download MIBs 542
Location information 544
Enable modem GNSS support 545
Configure the device to use a user-defined static location 547
Configure the device to accept location messages from external sources 549
Forward location information to a remote host 551
Configure geofencing 558
Show location information 569
Modbus gateway 570
Configure the Modbus gateway 571
Modbus hardening 584
Show Modbus gateway status and statistics 585
System time synchronization 588
Configure the system time synchronization 588
Manually set the system date and time 593
Network Time Protocol 593
Configure the device as an NTP server 594
Show status and statistics of the NTP server 599
Configure a multicast route 600

Enable service discovery (mDNS) 602
Use the MQTT broker service 605
Show MQTT broker information 615
Use the iPerf service 616
Example performance test using iPerf3 621
Configure the ping responder service 621
Example performance test using iPerf3 625

Applications

Develop Python applications 627
Set up the IX10 for Python development 628
Create and test a Python application 628
Python modules 632
The use(led) function 656
Releasing the LEDs to system control 656
Use Python to control the color of multi-colored LEDs 657
Example: Set the LTE connection indicator to flashing purple 658
Set up the IX10 to automatically run your applications 666
Configure scripts to run automatically 667
Show script information 674
Stop a script that is currently running 675
Start an interactive Python session 676
Run a Python application at the shell prompt 677
Configure scripts to run manually 678
Task one: Upload the application 679
Task two: Configure the application to run automatically 680
Start a manual script 684
Python versions and corresponding DAL OS firmware versions 685

User authentication

IX10 user authentication 687
User authentication methods 687
Add a new authentication method 689
Delete an authentication method 691
Rearrange the position of authentication methods 692
Authentication groups 694
Change the access rights for a predefined group 696
Add an authentication group 698
Delete an authentication group 702
Local users 704
Change a local user's password 705
Configure a local user 707
Delete a local user 714
Terminal Access Controller Access-Control System Plus (TACACS+) 717
TACACS+ user configuration 718
TACACS+ server failover and fallback to local authentication 719
Configure your IX10 device to use a TACACS+ server 719
Remote Authentication Dial-In User Service (RADIUS) 724
RADIUS user configuration 725
RADIUS server failover and fallback to local configuration 725
Configure your IX10 device to use a RADIUS server 726
LDAP 729

LDAP user configuration ... 731
LDAP server failover and fallback to local configuration ... 732
Configure your IX10 device to use an LDAP server ... 732
Configure serial authentication ... 737
Disable shell access ... 739
Set the idle timeout for IX10 users ... 741
Example user configuration ... 743
Example 1: Administrator user with local authentication ... 743
Example 2: RADIUS, TACACS+, and local authentication for one user ... 745

Firewall

Firewall configuration ... 753
Create a custom firewall zone ... 753
Configure the firewall zone for a network interface ... 755
Delete a custom firewall zone ... 756
Port forwarding rules ... 758
Configure port forwarding ... 758
Delete a port forwarding rule ... 762
Packet filtering ... 765
Configure packet filtering ... 765
Enable or disable a packet filtering rule ... 769
Delete a packet filtering rule ... 770
Configure custom firewall rules ... 772
Configure Quality of Service options ... 774
Web filtering ... 783
Configure web filtering with Cisco Umbrella ... 783
Configure web filtering with manual DNS servers ... 786
Verify your web filtering configuration ... 788
Show web filter service information ... 791

Containers

Use Digi Remote Manager to deploy and run containers ... 793
Use an automation to start the container ... 796
Upload a new LXC container ... 797
Configure a container ... 798
Starting and stopping the container ... 803
Starting the container ... 803
Stopping the container ... 804
View the status of containers ... 804
Show status of all containers ... 804
Show status of a specific container ... 805
Schedule a script to run in the container ... 805
Create a custom container ... 808
Create the custom container file ... 808
Test the custom container file ... 809

System administration

Review device status ... 811
Configure system information ... 812
Update system firmware ... 814

Manage firmware updates using Digi Remote Manager ... 814
Python and DAL OS firmware updates ... 815
Certificate management for firmware images ... 815
Downgrading ... 815
Dual boot behavior ... 819
Upgrade cellular modem firmware ... 820
Update modem firmware over the air (OTA) ... 821
Update modem firmware by using a local firmware file ... 822
Reboot your IX10 device ... 824
Reboot your device immediately ... 824
Schedule reboots of your device ... 825
Erase device configuration and reset to factory defaults ... 826
Custom factory default settings ... 830
Locate the device by using the Find Me feature ... 832
Configure a power profile ... 833
Enable FIPS mode ... 836
Configuration files ... 838
Save configuration changes ... 838
Save configuration to a file ... 839
Restore the device configuration ... 840
Schedule system maintenance tasks ... 843
Disable device encryption ... 848
Re-enable cryptography after it has been disabled. ... 849
Configure the speed of your Ethernet port ... 851
Watchdog service ... 853
Configure the Watchdog service ... 853
View Watchdog metrics ... 856

Monitoring

intelliFlow ... 860
Enable intelliFlow ... 861
Configure service types ... 863
Configure domain name groups ... 865
Use intelliFlow to display average CPU and RAM usage ... 868
Use intelliFlow to display top data usage information ... 869
Use intelliFlow to display data usage by host over time ... 871
Configure NetFlow Probe ... 872

File system

The IX10 local file system ... 878
Display directory contents ... 878
Create a directory ... 879
Display file contents ... 880
Copy a file or directory ... 880
Move or rename a file or directory ... 881
Delete a file or directory ... 882
Upload and download files ... 883
Upload and download files by using the WebUI ... 883
Upload and download files by using the Secure Copy command ... 884
Upload and download files using SFTP ... 885

Diagnostics

Perform a speedtest ... 888
Generate a support report ... 888
    Support report overview ... 889
View system and event logs ... 893
    View System Logs ... 893
    View Event Logs ... 895
Configure syslog servers ... 897
Configure options for the event and system logs ... 899
Configure an email notification for a system event ... 904
Configure an SNMP trap for a system event ... 905
Analyze network traffic ... 906
    Configure packet capture for the network analyzer ... 907
    Example filters for capturing data traffic ... 916
    Capture packets from the command line ... 917
    Stop capturing packets ... 918
    Show captured traffic data ... 919
    Save captured data traffic to a file ... 920
    Download captured data to your PC ... 921
    Clear captured data ... 922
Use the ping command to troubleshoot network connections ... 924
    Ping to check internet connection ... 924
    Stop ping commands ... 924
Use the traceroute command to diagnose IP routing problems ... 924

Digi IX10 regulatory and safety statements

RF exposure statement ... 926
Federal Communication (FCC) Part 15 Class B ... 926
    Radio Frequency Interference (RFI) (FCC 15.105) ... 926
European Community - CE Mark Declaration of Conformity (DoC) ... 926
IFETEL ... 927
Maximum transmit power for radio frequencies ... 928
Innovation, Science, and Economic Development Canada (IC) certifications ... 928
RoHS compliance statement ... 929
Special safety notes for wireless routers ... 929
Special installation instructions and warnings ... 930
Product disposal instructions ... 931

Safety warnings

English ... 932
Bulgarian--български ... 933
Croatian--Hrvatski ... 933
French--Français ... 934
Greek--Ελληνικά ... 935
Hungarian--Magyar ... 935
Italian--Italiano ... 936
Latvian--Latvietis ... 937
Lithuanian--Lietuvis ... 937
Polish--Polskie ... 938
Portuguese--Português ... 938
Slovak--Slovák ... 939

Slovenian--Esloveno 940
Spanish--Español 940

Digi IX10 Certifications

International EMC (Electromagnetic Compatibility) and safety standards 941

Command line interface

Access the command line interface 943
Log in to the command line interface 943
Exit the command line interface 944
Execute a command from the web interface 944
Display help for commands and parameters 946
The help command 946
The question mark (?) command 946
Display help for individual commands 947
Use the Tab key or the space bar to display abbreviated help 947
Auto-complete commands and parameters 948
Available commands 949
Use the scp command 950
Display status and statistics using the show command 951
show config 952
show system 952
show network 952
Device configuration using the command line interface 953
Execute configuration commands at the root Admin CLI prompt 953
Display help for the config command from the root Admin CLI prompt 953
Configuration mode 955
Enable configuration mode 955
Enter configuration commands in configuration mode 955
Save changes and exit configuration mode 956
Exit configuration mode without saving changes 956
Configuration actions 956
Display command line help in configuration mode 957
Move within the configuration schema 960
Manage elements in lists 960
The revert command 963
Enter strings in configuration commands 964
Example: Create a new user by using the command line 965
Command line reference 967
ain calibrate 967
ain calibration-reset 967
analyzer clear 967
analyzer save 967
analyzer start 968
analyzer stop 968
cat 968
clear dhcp-lease ip-address 968
clear dhcp-lease mac 968
container create 969
container delete 969
cp 969
dio state 969

grep 970
help 970
ls 971
mkdir 972
modem at 972
modem at-interactive 972
modem firmware bundle ota check 972
modem firmware bundle ota download 972
modem firmware bundle ota list 973
modem firmware bundle ota update 973
modem firmware check 973
modem firmware list 973
modem firmware ota check 974
modem firmware ota download 974
modem firmware ota list 974
modem firmware ota update 974
modem firmware update 975
modem pin change 975
modem pin disable 975
modem pin enable 976
modem pin status 976
modem pin unlock 976
modem puk status 976
modem puk unlock 977
modem reset 977
modem scan 977
modem sim-slot 977
modem sms send 978
modem sms send-binary 978
monitoring metrics upload 978
monitoring 979
monitoring metrics upload 979
more 979
mv 979
ping 979
poweroff 980
pyinstall 980
reboot 980
rm 980
scp 982
config directory: show command 982
show ain 982
show analyzer 982
show arp 983
show bluetooth-scanner log 983
show bluetooth-scanner nearby 983
show bluetooth-scanner static-candidate 983
show bluetooth-scanner static-confirmed 983
show cloud 984
show config 984
show containers 984
show dhcp-lease 984
show dio 985
show dns 985
show eth 985

show event 985
show hotspot 985
show ipsec 986
show l2tp lac 986
show l2tp lns 986
show l2tpeth 986
show location 987
show log 987
show manufacture 987
show modbus-gateway 987
show modem 988
show mqtt 988
show nemo 988
show network 988
show ntp 989
show openvpn client 989
show openvpn server 989
show route 989
show scep-client 989
show scripts 990
show serial 990
show surelink interface 990
show surelink ipsec 990
show surelink openvpn 991
show surelink state 991
show system 991
show version 991
show vrrp 991
show web-filter 992
iperf 992
ssh 992
system backup 993
system cloud register 993
system custom-default-config current 993
system custom-default-config file 994
system custom-default-config remove 994
system disable-cryptography 994
system duplicate-firmware 994
system factory-erase 994
system find-me 995
system firmware ota check 995
system firmware ota list 995
system firmware ota update 995
system firmware update 996
system power ignition off_delay 996
system restore 996
system script start 996
system script stop 996
system serial clear 997
system serial copy 997
system serial ipport 997
system serial restart 998
system serial save 998
system serial show 998
system storage format 998

system storage mount 999
system storage show 999
system storage unmount 999
system support-report 999
system time set 999
system time sync 1000
system time test 1000
tail 1000
telnet 1000
traceroute 1001
vtysh 1002

IX10 User Guide

The Digi IX10 is a rugged, secure and reliable LTE industrial router powered by an enhanced operating system that supports any utility or industrial application.

This online guide helps site administrators configure and manage Digi IX10 devices. This guide assumes administrators are familiar with network basics, such as network terminology, architecture, interfaces, and related concepts.

DAL OS Vulnerability Patch Policy

Digi has created a vulnerability patch policy to document the guidelines and procedures we plan to take to identify, assess, and remediate security vulnerabilities in our DAL OS firmware integrated into Enterprise (EX), Industrial (IX) and Transportation routers (TX), device and serial servers (Connect EZ), console servers and USB-connected devices. Specifically, this policy outlines how quickly and effectively patches need to be applied to mitigate risks from potential threats. The policy protects against cyberattacks but also ensures that out firmware is in compliance with regulatory standards.

The DAL Vulnerability Patch Policy is documented on the digi.com website, and covers the following topics:

- Objective
- Scope
- Audience
- Introduction
- Reporting Potential Vulnerabilities
- Assessing Potential Vulnerabilities
- Information and Resolution Timelines
- Resolution of Potential Vulnerabilities
- Receiving Information on Potential Vulnerabilities

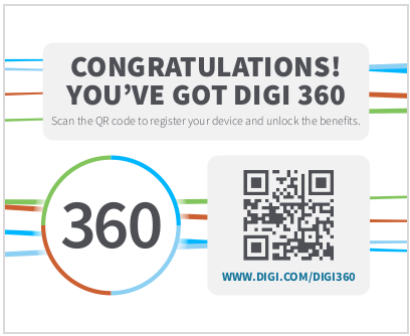
Digi 360

Digi 360 is a subscription-based solution that includes software, services, and device support for your cellular network and IoT ecosystem. The main components of Digi 360 include:

- **Digi Remote Manager software**: Configuration, deployment, management, protection, and analysis of your IX10 routers and network. Go to the Digi Remote Manager product page on the Digi website for more information.
- **Customer Care service**: Help that is always available: all day, every day, for the duration of your Digi 360 subscription.
- **IX10** router: Hardware with DAL OS firmware to support your network infrastructure.
- **Limited lifetime warranty service**: IX10 protection for the length of your Digi 360 subscription.

For more information, see the Digi 360 FAQs.

A **CONGRATULATIONS!** sticker is now included on the outside of EX, IX, and TX router boxes. This sticker means you have the Digi 360 subscription and all of your devices have Digi 360 licenses. Scan that QR code or go to the Digi 360 page on digi.com for information about your subscription, including benefits and warranty. You can also access your Customer Portal from that same page to register new routers to your Digi account.



Frequently asked questions

Where do I register my Digi 360 routers?

If you are a Digi customer, register your devices in the Digi Customer Portal, https://my.digi.com.

What information do I need to register my Digi 360 routers?

- Item number found on your Digi purchase order.
- Serial number for each device you need to register.
- Reseller or Distributor from whom you purchased your devices, if applicable.
- Extended contract and length terms, if applicable.

- Remote Manager Primary Account Administrator Username and Email or Customer ID #, if needed

How long do I have to register my Digi 360 routers in the Customer portal?

You have 48 hours to register your routers in the Customer portal, https://my.digi.com.

Do I need to register my Digi 360 s in the Customer Portal or Digi Remote Manager?

Digi Customer Operations or your Reseller will register the routerss for you. Though rare, you may have to register your own routerss in the Customer portal and/or Digi Remote Manager. For information about how to do so, see Digi IX10 Quick start.

Will I be notified when my routers are registered?

Yes, you will receive an email confirming registration. You will also receive Digi Remote Manager login credentials.

What are the available durations of a Digi 360 subscription?

Digi 360 is available in one-, two-, or 4-year subscriptions.

When will I be notified that my Digi 360 subscription will expire?

Yes. You will be notified at least 60 days before and then again 30 days before your Digi 360 subscription expires.

Can I update my current Digi Remote Manager license to a Digi 360 subscription?

Yes. You can update your current Digi Remote Manager license to a Digi 360 subscription as long as you are running DAL OS and the warranty on those devices has not yet expired.

What are the advantages of a Digi 360 subscription?

The advantages of a Digi 360 subscription include the following:

- Faster deployment of devices and network.
- Manage a complex ecosystem of IoT devices.
- Update multiple devices simultaneously.
- Accurately predict operating expenses.
- Manage your device and network lifecycle.
- Enhance the value of your network.
- Protect your investments.
- Achieve ROI.

Can I renew a suspended Digi 360 subscription during the suspension period?

You may renew your suspended subscription during the suspension period. If you renew during this period and Digi receives payment before this period is over, the renewed subscription will be backdated. The renewed subscription will start on the first day after your original subscription ended.

Does Digi offer planning and deployment services?

Yes. Digi Professional Services can help you set up your IoT network from start to finish, including:

- Project planning
- Web app, mobile app, Python, and bash script development
- Device retrofits
- Deployment

Are there additional value-added services available?

Yes. You can expand your Digi 360 subscription to include the following services:

- Containers
- WAN bonding
- Mobile VPN

Go to the Digi website, https://www.digi.com/products/iot-software-services/value-added-services, for more information.

Does my Digi 360 subscription and my value-added services subscription terms, like start and end dates, have to be the same?

No. The start and end dates of your Digi 360 subscription and your value-add services do not have to be the same.

If I do not plan to purchase a Digi 360 **subscription, can I still renew my current license?**

Yes. You can renew your current license.

Digi IX10 Quick start

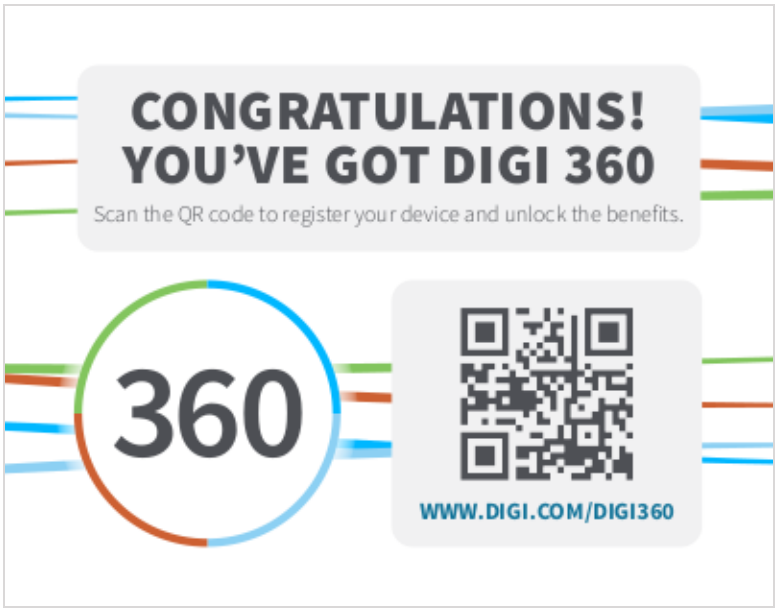
Migrating from a WR-series device? Click here for information and tools to set up your new IX-series router.

Welcome to the IX10 router quick start guide. In this guide, we will outline the essential steps to set up your routers, which are the foundation of your cellular network and IoT ecosystem.

You're here because you scanned the QR code on the Welcome card that came inside the router box.

CAUTION! Do not lose the extra product label card that comes with each IX10 router! Every router you receive from Digi has a unique password. This password appears on the product label on the bottom of the router, and on the extra product label card. You must use this password to add and then configure the router. You can change the password, but if you factory reset the router, you will need to use this unique password again.

A CONGRATULATIONS! sticker is now included on the outside of EX, IX, and TX router boxes. This stickers means you have the Digi 360 subscription and all your devices have Digi 360 licenses. Scan the QR code or go to the Digi 360 page on digi.com for information about your subscription, including benefits and warranty. You can also access your Customer Portal from that same page to activate new routers and link them to your Digi account.



For a majority of customers, your new routers may already be linked to your Digi customer account, as well as to Digi Remote Manager. If they are, then you do not need to activate them. If you have any questions about whether you need to activate or register your routers, contact your Reseller or visit Digi Technical Support.

To get your routers set up and connected to the internet and registered in Digi Remote Manager:

Step 1: What's in the box

When you open the IX10 package, look for the following:

- **Digi IX10 device**

  The Digi IX10 has a product label on the bottom of the device. The label includes product identification information and the default password assigned to the device. The IX10 also includes a terminal connector for the power supply installed in the power input.

- **Insert cards**

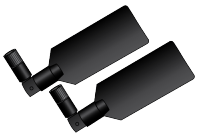
- **Digi IX10 label**

  Printed copy of the product label on the bottom of your device. You can affix this label to the top or side of the device such that you can access the label after the device is mounted, or store the label in a safe place for future reference.

Step 2: Gather accessories

Accessories may be purchased with the IX10 device, or you can provide your own.

Here's the list of accessories used in this *Quick start*:

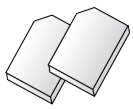


Antennas
Two cellular antennas, ordered separately.

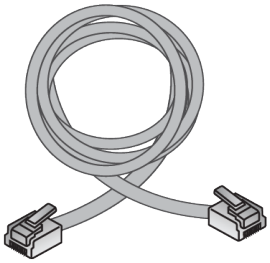
Power supply
Ordered separately.

DIN rail clip
Ordered separately. For optionally clipping the IX10 to a DIN rail.

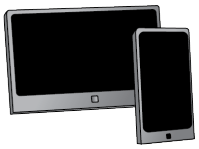
Laptop or personal computer
Use an Ethernet cable to connect your IX10 to a laptop or PC.



SIM card(s)
If you intend to configure cellular WWAN access at this time, acquire SIM cards as needed. Note the carrier, network APN (Access Point Name), and SIM pin (if any) for each card.



Ethernet cable



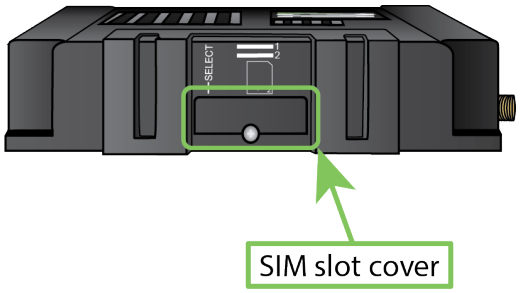
Smart phone or tablet
Optional: Use a smart phone or tablet to automatically register your IX10 in your Digi Remote Manager account and connect to your cellular network. See Add a device to Remote Manager using information from the label.

Step 3: Connect your device

1. **Insert SIM card(s)**

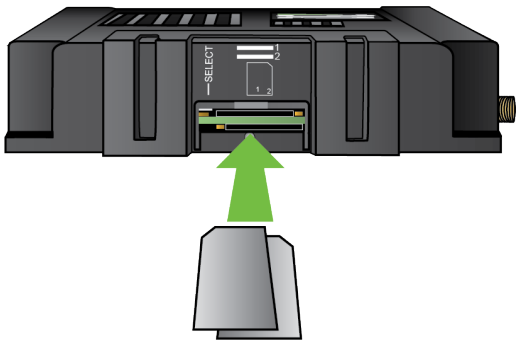
   Insert your activated 2FF SIM card provided by your cellular carrier into the device:

   a. Use a Philips #0 driver to remove the SIM slot cover.



   b. For high-vibration environments, apply a thin layer of dielectric grease to the SIM contacts.

   c. Insert the SIM card into the SIM 1 (top) socket. Insert the end of the SIM card with the chamfered corner positioned as indicated. Push the SIM in until it clicks into place.



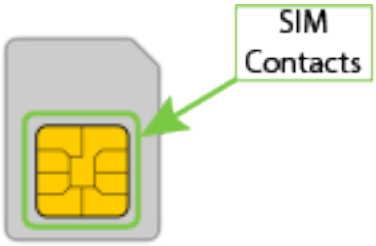
   d. After SIM card is installed, use a Philips #0 driver to secure the SIM slot cover. Torque screw to 2 in lbs (225 mN m) maximum.

Apply Dielectric Grease over SIM Contacts

Note Digi recommends using either the Loctite®LB 8423 Dielectric Grease or Synco Lube® Silicone Dielectric Grease.

a. Use a sheet of paper or cardboard over the area where you intend to work.

b. Use isopropyl alcohol and a cotton-tipped applicator to gently clean the SIM contacts. Using isopropyl alcohol requires a well vented environment. Demineralized water can also be used as an alternative.



c. Once the surface is clean and dry, apply a small amount of dielectric grease in a thin layer over the contacts. Use a new cotton-tipped applicator to work the grease smoothy over the contacts. Apply gentle pressure.

d. When the dielectric grease has been applied, insert the SIM into the SIM slot as described above.

2. **Attach cellular antennas**

   Securely tighten each antenna using the barrel connector at the base of the antenna.

Step 4: Connect DC power

1. Use an Ethernet cable to connect the Ethernet port to your PC.

Step 5: Set up access to Digi Remote Manager

- If you already have a Digi Remote Manager account, skip to Digi IX10 Quick start.
- If you prefer to configure the device locally rather than using Remote Manager, see Firmware configuration in the *IX10 User Guide*.

To set up access to Remote Manager:

1. Go to my.digi.com to create a new Remote Manager account.

   You will receive an email from Remote Manager after your registration is complete.

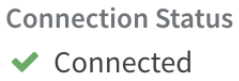
2. Click the link in the email to go to Remote Manager and click **Forgot Password** to set up your login and password.
3. Log intoRemote Manager.

Step 6: Register your device

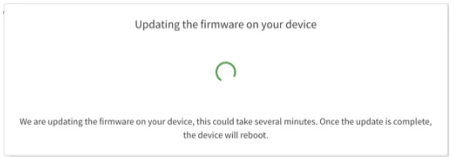
1. Register the device as instructed by the Remote Manager Getting Started wizard.

Step 7: Complete setup

1. The device should connect within a couple of minutes.



2. If newer firmware is available, Remote Manager will prompt you to update the device. Click **Update** to update the firmware. Remote Manager will perform the update in the background and let you know when the device is up to date.



3. Click **Done** when the firmware update is complete.

Step 8: Configure the cellular APN

If you installed a SIM in Step 1: Connect DC power, the device will attempt to setup the APN automatically. However, if your SIM was set up with a custom APN, you will need to configure it manually:

1. Navigate to the **Settings** tab in the Remote Manager**Device Details** view.
2. Expand the **Config** menu item and click on the **Network** settings menu.
3. Expand **Interfaces** > **Modem** > **modem** > **APN list** > **APN list 1**.
4. For **APN**, enter the custom APN provided by your cellular provider.
5. Click **Apply**.
6. Navigate back to the **Details** tab and watch for confirmation of cellular connectivity.

Digi IX10 hardware reference

Digi IX10 features and specifications

The Digi IX10 key features include:

- Industrial grade components.
- Operating temperatures:

  -40C to +70C/-40F to +158F.
- LTE CAT 4 modem with two SIM slots.
- 10/100 BaseT Ethernet port for high-speed connectivity.

For a detailed list of IX10 hardware specifications, see https://www.digi.com/products/networking/cellular-routers/industrial/digi-ix10#specifications.

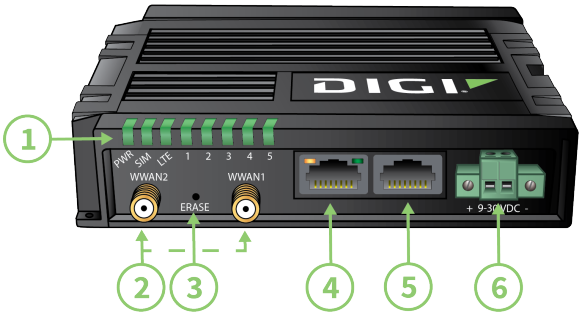
IX10 accessories

When accessories are purchased with the IX10 device, the following are provided:

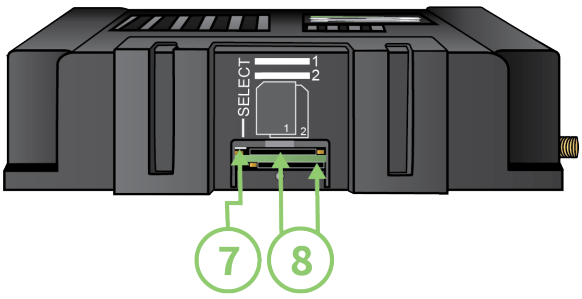
- Cellular antennas.
- Power supply.
- Ethernet cable.
- DIN rail mounting clip.

IX10 front and side views

The following figure shows the front view of the IX10.



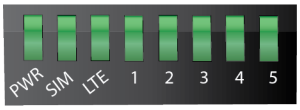
Item	Decription
1. **LEDs**	See IX10 LEDs.
2. **Antenna connectors**	Main (WWAN1) and auxiliary (WWAN2) cellular antenna connectors.
3. **ERASE** button	See Erase device configuration and reset to factory defaults.
4. **Ethernet port**	LAN-enabled by default.
5. **Serial port**	See Digi IX10 serial connector pinout for information about the serial port pin-out.
6. **Power supply**	Reverse polarity protection. IX10 power supply requirements.



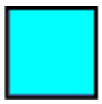
Item	Decription
7. **SELECT**	The **SELECT** button is used to manually toggle between the two SIM slots.
8. **SIM slots**	See Install SIM cards for more details. **WARNING!** *Are you using consumer-grade SIM cards in a device that is subject to shock, vibration, or material expansion/contraction due to seasonal temperature variations?* If so, these extreme conditions can lead to contact fretting and unexpected SIM card failure. Digi strongly recommends using industrial-grade SIMs instead of consumer-grade SIMs. Industrial-grade SIMs are designed for extreme environments and are constructed of heavier-gauge materials and extended-temperature electronic components.

IX10 LEDs

The IX10 LEDs are located on the top front panel. . During bootup, the front-panel LEDs light up in sequence to indicate boot progress.

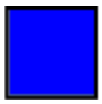


Power (PWR)

	Off No power.
	Solid green Device has power but is not connected to the internet.
	Flashing green/cyan Device has power and is in the process of connecting to the internet.
	**Solid cyan** Device has power and is connected to the internet.

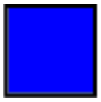
SIM

Indicates that a SIM is in use:

	Off No SIM is present
	Solid green SIM1 is active.
	**Solid blue** SIM 2 is active
	Solid red SIM failure.

LTE

Indicates that the status of the cellular module and the ETH Ethernet port connection:

	Solid yellow (or orange) Initializing or starting up.		
	Flashing yellow (or orange) In the process of connecting to the cellular network and to a device on its ETH port.		**Flashing white** ETH port connection established and in the process of connecting to the cellular network.
	Flashing green Connected to 2G or 3G[1] and is in the process of connecting to any device on its ETH port, or nothing is connected to the port.		**Solid green** Connected to 2G or 3G and also has a device linked to its ETH port.
	Flashing blue Connected to 4G LTE and in the process of connecting to a device on its ETH port.		**Solid blue** Connected to the 4G LTE and also has a device link to its ETH port.
	Alternating Red/yellow (or orange) Upgrading firmware. **WARNING!** DO NOT POWER OFF DURING FIRMWARE UPGRADE.		

Signal quality indicators

LEDs labeled **1** through **5** Indicate the cellular service quality level.

Signal bars	Weighted dBm	Signal strength %	Quality
	-113 to -99	0% to 23%	Bad
	-98 to -87	24% to 42%	Marginal
	-86 to -76	43% to 61%	OK
	-75 to -64	62% to 80%	Good
	-63 to -51	81% to 100%	Excellent

The weighted dBm measurements are negative numbers, meaning values closer to zero denote a larger number. For example, a -85 is a better signal than -90.

Note See Cellular signal quality explained for more information regarding how signal strength is calculated and subsequently displayed via the LED indicators.

Ethernet Link and Activity

The LEDs on the **ETH** port indicate that the Ethernet network interface is up and there is activity on the network interface.

Left LED (on top of port connector)

- **Off**: No Ethernet link detected.
- **Solid green**: Ethernet link detected.
- **Blinking green**: Indicates Ethernet traffic.

Right LED (on top of port connector)

- **Off**: No Ethernet link detected.
- **Solid amber**: 10/100 Mbps link detected.

Cellular signal quality explained

Cellular signal quality refers to the strength and reliability of the signal from a cellular network to the IX10. The quality of the signal is visually represented using LED bars on the front of the router: the more bars that are lit the better the signal quality. An algorithm is used to determine the signal quality, with each cellular network using a different algorithm.

2G algorithm

For the 2G cellular network, the algorithm is determined using one parameter to calculate signal strength: RSSI[1].

```
RSSI > -80, bars=5
-89 < RSSI <= -80, bars=4
-98 < RSSI <= -89, bars=3
-104 < RSSI <= -98, bars=2
RSSI <= -104, if we're connected to the cellular network, bars=1, if not bars=0
```

3G algorithm

For the 3G cellular network (including HSPA+), the algorithm is determined using one parameter to calculate signal strength: RSSI.

```
RSSI > -80, bars=5
-90 < RSSI <= -80, bars=4
-100 < RSSI <= -90, bars=3
-106 < RSSI <= -100, bars=2
RSSI <= -106, if we're connected to the cellular network, bars=1, if not bars=0
```

1 Received Signal Strength Indicator

4G LTE algorithm

For the 4G LTE cellular network, the algorithm is determined using three parameters to calculate signal strength: RSSI, RSRP[1], and SNR[2].

```
RSRP > -85, rsrp_bars=5
-95 < RSRP <= -85, rsrp_bars=4
-105 < RSRP <= -95, rsrp_bars=3
-115 < RSRP <= -105, rsrp_bars=2
-199 < RSRP <= -115, if we're connected to the cellular network, rsrp_bars=1,
if not rsrp_bars=0
```

If RSRP <= -199, the device uses the RSSI as the value with the same algorithm:

```
SNR >= 13, snr_bars=5
4.5 <= SNR < 13, snr_bars=4
1 <= SNR < 4, snr_bars=3
-3 < SNR < 1, snr_bars=2
-99 < SNR <= -3, if we're connected to the cellular network, snr_bars=1, if not
snr_bars=0
```

Once the values are determined, the IX10 router uses the lesser of the two ranges, which is then visually represented by the signal bars.

5G algorithm

For the 5G cellular network, the algorithm is determined using three parameters to calculate signal strength: RSRP, RSRQ[3], and SINR[4].

```
RSRP >= -65, rsrp_bars=5
-80 <= RSRP < -65, rsrp_bars=4
-90 <= RSRP < -80, rsrp_bars=3
-110 <= RSRP < -90, rsrp_bars=2
-140 <= RSRP < -110, rsrp_bars=1
RSRP < -140, rsrp_bars=0
```

```
RSRQ >= 6, rsrq_bars=5
-7 <= RSRQ < 6, rsrq_bars=4
-19 <= RSRQ < -7, rsrq_bars=3
-31 <= RSRQ < -19, rsrq_bars=2
-43 <= RSRQ < -31, rsrq_bars=1
RSRQ < -43, rsrq_bars=0
```

```
SINR >= 30, sinr_bars=5
15 <= SINR < 30, sinr_bars=4
5 <= SINR < 15, sinr_bars=3
-5 <= SINR < 5, sinr_bars=2
-23 <= SINR < -5, sinr_bars=1
SINR < -23, sinr_bars=0
```

Once the **sinr_bars**, **rsrq_bars**, and **rsrp_bars** values are determined, the IX10 router uses the lesser of the three ranges, which is then visually represented by the signal bars.

---

1 Referenced Signal Received Power

2 Signal-to-Noise Ratio

3 Reference Signal Received Quality

4 Signal-to-Interface + Noise Ratio

IX10 power supply requirements

IX10 is intended to be powered by a certified power supply with output rated at either 12 VDC/0.75 A or 24 VDC/0.375 A minimum.

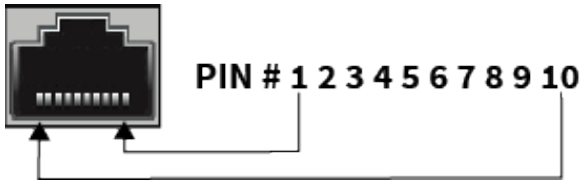
- Use the Digi power supply accessory kit 76002104.
- If you are providing the DC power source with a non-Digi power supply, you must use a certified LPS power supply rated at either 12 VDC/0.75 A or 24 VDC/0.375 A minimum. The voltage tolerance supports +/- 10% (9 VDC to 30 VDC) at 9 Watts minimum.
- For installations requiring protective earth grounding, connect the -ve terminal of the power connector to the system protective earth with a minimum 1mm2 stranded single insulated cable. Crimp terminals should be used for all connections.

Digi IX10 serial connector pinout

Note The IX10 supports both the RS232 and RS458 serial interfaces.
- When using the RS485 interface, signals TxD/RxD+ and TxD/RxD- are electrically tied internally and do not require external support.
- If using the cable assembly accessory (76000723), the wire labels are marked for the RS422 serial interface and can be ignored. Signal labels TxD+ and RxD+, along with either the ground (GND) or signal ground (SG), are sufficient.

The IX10 is a DTE device. The pinout for the 10 pin RJ-50 serial connector is as follows:

Pin number	RS232 signal	RS485 half-duplex signal
1	RI	
2	DSR	
3	RTS	
4	GND	GND
5	Tx	TxD/RxD+
6	Rx	TxD/RxD-
7	GND	SG
8	CTS	
9	DTR	
10	DCD	



10-pin serial cabling options

Digi offers several cabling options for connecting a 10 pin RJ-45/RJ-50 serial port to DB9 and DB25 serial connectors. Digi recommends the RJ45/Bare Wire 48 inch cable, part number 76000723, which provides a customizable connector to connect EIA 422/485 Devices to Digi MEI products that have 10 pin RJ45 connectors. The *PortServer TS, Digi Connect, and Digi One Products Cable Guide* also provides information about additional Digi cabling options.

QR code definition

A QR code is printed on the label attached to the device and on the loose label included in the box with the device components. The QR code contains information about the device.

QR code items

Semicolon separated list of:

ProductName;DeviceID;Password;SerialNumber;SKUPartNumber-SKUPartRevision

Example

IX10;00000000-00000000-112233FF-FF445566;PW1234567890;50001001-00

Digi IX10 hardware setup

This chapter contains the following topics:

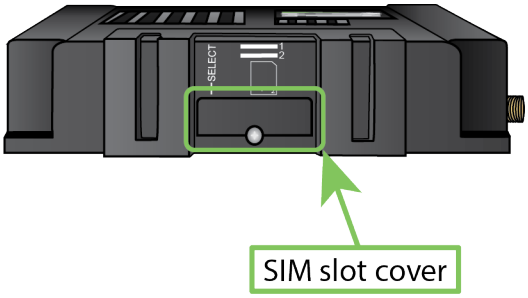
Install SIM cards 45
Connect data cables 46
Mount the IX10 device 46

Install SIM cards

WARNING! *Are you using consumer-grade SIM cards in a device that is subject to shock, vibration, or material expansion/contraction due to seasonal temperature variations?* If so, these extreme conditions can lead to contact fretting and unexpected SIM card failure. Digi strongly recommends using industrial-grade SIMs instead of consumer-grade SIMs. Industrial-grade SIMs are designed for extreme environments and are constructed of heavier-gauge materials and extended-temperature electronic components.

To install SIM cards:

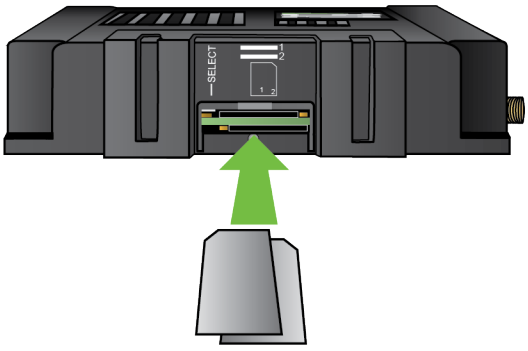
1. Use a Philips #0 driver to remove the SIM slot cover.



2. For high-vibration environments, apply a thin layer of dielectric grease to the SIM contacts.

   Note If the IX10 device is used in an environment with high vibration levels, SIM card contact fretting may cause unexpected SIM card failures. To protect the SIM cards, Digi strongly recommends that you apply a thin layer of dielectric grease to the SIM contacts prior to installing the SIM cards. See Apply Dielectric Grease over SIM Contacts for instructions.

3. Insert the SIM card(s) into the SIM sockets. Insert the end of each SIM card with the chamfered corner positioned as indicated. Push the SIM in until it clicks into place.

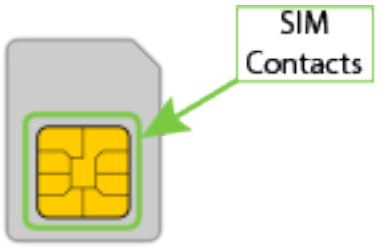


4. After SIM cards are installed, use a Philips #0 driver to secure the SIM slot cover. Torque screw to 2 in lbs (225 mN m) maximum.

Apply Dielectric Grease over SIM Contacts

Note Digi recommends using either the Loctite®LB 8423 Dielectric Grease or Synco Lube®Silicone Dielectric Grease.

1. Use a sheet of paper or cardboard over the area where you intend to work.
2. Use isopropyl alcohol and a cotton-tipped applicator to gently clean the SIM contacts. Using isopropyl alcohol requires a well vented environment. Demineralized water can also be used as an alternative.



3. Once the surface is clean and dry, apply a small amount of dielectric grease in a thin layer over the contacts. Use a new cotton-tipped applicator to work the grease smoothy over the contacts. Apply gentle pressure.
4. When the dielectric grease has been applied, insert the SIM into the SIM slot as described above.

SIM removal

The IX10 has a PUSH-PUSH SIM connector. To insert, push each SIM in until it clicks, and repeat for removal. When you push to eject, the SIM ejects back out about 1/8 inch.

Tips for improving cellular signal strength

If the signal strength LEDs or the signal quality for your device indicate **Poor** or **No service**, try the following things to improve signal strength:

- Move the device to another location.
- Try connecting a different set of antennas, if available.
- Purchase a Digi Antenna Extender Kit: Antenna Extender Kit, 1m.

Connect data cables

The IX10 supports two types of data ports:

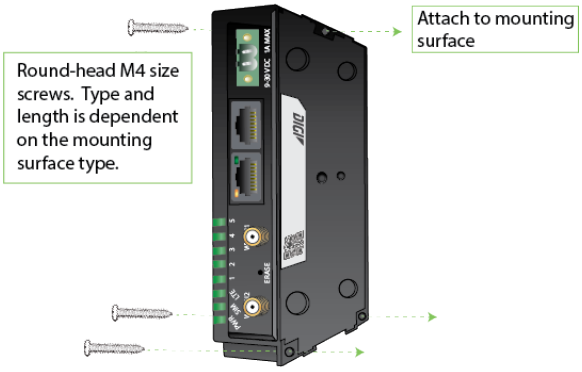
- **Ethernet** (RJ-45): Use a Cat 5e or Cat 6 Ethernet cable.
- **Serial** (RJ-50): Use a serial cable with an RJ-50 connector to connect to the IX10 device. See 10-pin serial cabling options for information about Digi's 10-pin RJ-50 cables.

Mount the IX10 device

There are two options for mounting the IX10 device:

- Attach to a mounting surface by using the mounting tabs.
- Attach to DIN rail with clip.

Attach to a mounting surface by using the mounting tabs



Attach to DIN rail with clip

The DIN rail clip is an optional accessory included when the IX10 is purchased with accessories. You can attach the din rail clip directly to the device either on the back or the bottom of the device.

1. Attach the DIN rail clip to the back of the device:
   a. Attach the DIN rail clip to the back of the device with the screws provided.

b. Set the IX10 device onto a DIN rail and gently press until the clip snaps into the rail.

2. Attach the DIN rail clip to the bottom of the device:
   a. Attach the DIN rail clip to the bottom of the device with the screws provided.

WARNING! Using screws longer than 5.0 mm will cause damage to the IX10.

b. Set the IX10 device onto a DIN rail and gently press until the clip snaps into the rail.

WARNING! If being installed above head height on a wall or ceiling, ensure the device is fitted securely to avoid the risk of personal injury. Digi recommends that this device be installed by an accredited contractor.

Firmware configuration

This chapter contains the following topics:

Review IX10 default settings 51
Primary Responder mode 53
Change the default password for the admin user 56
Configuration methods 57
Using Digi Remote Manager 58
Access Digi Remote Manager 58
Using the local web interface 59
Review the dashboard 60
Use the local REST API to configure the IX10 device 61
Using the command line 65

Review IX10 default settings

You can review the default settings for your IX10 device by using the local WebUI or Digi Remote Manager:

Local WebUI

1. Log into the IX10 WebUI as a user with Admin access. See Using the local web interface for details.
2. On the menu, click **System** > **Device Configuration**.

Digi Remote Manager

1. If you have not already done so, connect to your Digi Remote Manager account.
2. From the menu, click **Devices** to display a list of your devices.
3. Locate your device as described in Use Digi Remote Manager to view and manage your device.
4. Click the **Device ID**.
5. Click **Settings**.
6. Click to expand **Config**.

The following tables list important factory default settings for the IX10.

Default interface configuration

Interface type	Preconfigured interfaces	Devices	Default configuration
Wireless Wide Area Network (WWAN)	▪ **Modem**	▪ **Modem**	▪ Firewall zone: External ▪ WAN priority: Metric=3 ▪ SIM failover after 5 attempts ▪ SureLink enabled for IPv4

Interface type	Preconfigured interfaces	Devices	Default configuration
Local Area Network (LAN)	▪ **ETH**	▪ Ethernet: **ETH**	▪ Firewall zone: Internal ▪ IP Address: 192.168.2.1/24 ▪ DHCP server enabled ▪ LAN priority: Metric=5 ▪ Ethernet port Type: Hybrid IP address Note The new default **Type** setting for the Ethernet port is now **Hybrid IP Address** (Interfaces > ETH > IPv4 > Type). The Ethernet port acts as a WAN (DHCP client) but automatically changes to LAN DHCP server if no WAN connections occurs within one minute of reboot. The benefit is for customers provisioning or staging these routers. There is no need to insert a SIM card in each device or make local UI changes for every device if you just want to get it online to upgrade device or modem firmware and apply some basic configuration settings for provisioning or staging purposes.
	▪ **Loopback**	▪ Ethernet: **Loopback**	▪ Firewall zone: Loopback ▪ IP address: 127.0.0.1/8

Interface type	Preconfigured interfaces	Devices	Default configuration
	▪ **Setup IP**	▪ Ethernet: **ETH**	▪ Firewall zone: Setup ▪ IP address 192.168.210.1/24
	▪ **Setup Link-local IP**	▪ Ethernet: **ETH**	▪ Firewall zone: Setup ▪ IP address 169.254.100.100/16

Other default configuration settings

Feature	Configuration
Central management	▪ Digi Remote Manager enabled as the central management service.
Security policies	▪ Packet filtering allows all outbound traffic. ▪ SSH and web administration: • Enabled for local administration • Firewall zone: Internal
Monitoring	▪ Device heath metrics uploaded to Digi Remote Manager at 60 minute interval. ▪ SNMP: Disabled
Serial port	▪ Enabled ▪ Serial mode: Remote Access ▪ Label: None ▪ Baud rate: ▪ Data bits: 8 ▪ Parity: None ▪ Stop bits: 1 ▪ Flow control: None

Primary Responder mode

You can use the Primary Responder mode configuration setting to manually enable the IX10 device to be in an AT&T FirstNet-compliant mode (Primary Responder mode). When a device is in Primary Responder mode, certain firmware features are disabled. See Differences between standard firmware operation and Primary Responder mode.

The Primary Responder mode configuration setting is available in the 23.9.x and newer firmware. This replaces the Primary Responder firmware that was available prior to the 23.9.x firmware release.

Enable Primary Responder Mode

If you enable Primary Responder Mode, your device will reboot and the device's configuration will change to use the new mode. There are certain firmware features that are disabled in this mode.

Disable Primary Responder Mode

If you disable Primary Responder mode, the device's configuration is erased and the device will reboot. You will then need to reconfigure the device to the desired configuration.

Differences between standard firmware operation and Primary Responder mode

The device firmware version 23.9 and later has a Primary Responder mode that can be enabled on any device. When enabled, the device acts as a Primary Responder (PR) device with a security hardened, feature-restricted firmware targeted to comply with AT&T, FirstNet, and Verizon ResponseVerify security requirements.

When Primary Responder mode is enabled, the following features are not available:

- Telnet access has been removed.
- Raw TCP listeners for serial ports have been removed.
- Wi-Fi:
  - WPA1 encryption has been removed.
  - Any preconfigured access points are disabled by default.
- SSH is disabled by default.
- Users are prompted to enable two-factor authentication.
- A notification will appear in both the Web UI and CLI if the DAL device has Primary Responder mode enabled, but there are local users who do not have two-factor authentication enabled.
- Internal serial console port is disabled by default.
- USB ports are disabled by default.
- FIPS mode is automatically enabled when PR mode is enabled.
- Restoring a backup configuration file is disabled (Restore the device configuration).
- The **system custom-default-config** CLI command available in release 24.12 cannot be run in Primary Responder mode.

Enable Primary Responder mode

You can manually enable the Primary Responder mode configuration setting to change your device to Primary Responder mode.

Note When Primary Responder mode is enabled, some features on your device will not be available. See Differences between standard firmware operation and Primary Responder mode.

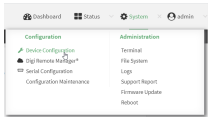
To enable Primary Responder mode:

Web

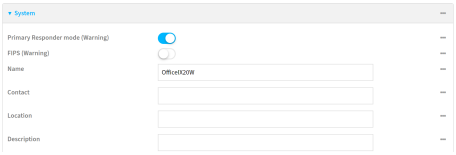
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. On the Dashboard, verify the current firmware version installed on the device. In the Device section, look at the **Firmware Version** field and verify that the version is 23.9.x or above.

   Note If the firmware version is not 23.9.x or above, you must update the firmware to 23.9.x before you can continue.

3. Access the device configuration:
   Remote Manager:
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.
   Local Web UI:
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
4. Click **System**.

   
5. Enable **Primary Responder mode**.
   The device will reboot and the device's configuration will change to use the new mode.
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable Primary Responder mode:

```
(config)> system primaryresponder true
(config)>
```

   The device will reboot and the device's configuration will change to use the new mode.
4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Change the default password for the admin user

The unique, factory-assigned password for the default **admin** user account is printed on the bottom label of the device and on the loose label included in the package.

If you erase the device configuration or reset the device to factory defaults, the password for the **admin** user will revert to the original, factory-assigned default password.

To change the default password for the admin user:

Web

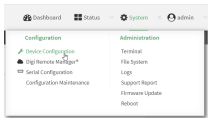
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

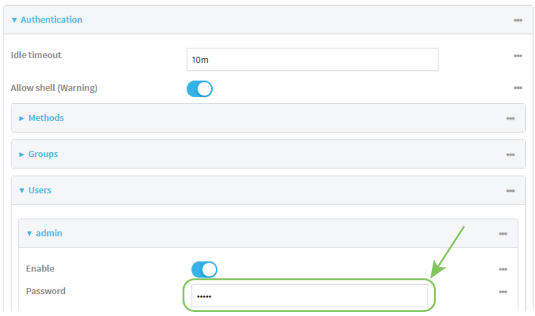
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Users** > **admin**.
4. Enter a new password for the admin user.The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

   Note If the Primary Responder feature is enabled, the password must be at least 10 characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set a new password for the admin user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

```
(config)> auth user admin password new-password
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configuration methods

There are two primary methods for configuring your IX10 device:

- Web interface.

  The web interface can be accessed in two ways:

  - Central management using the Digi Remote Manager, a cloud-based device management and data enablement platform that allows you to connect any device to any application, anywhere. With the Remote Manager, you can configure your IX10 device and use the configuration as a basis for a Remote Manager configuration which can be applied to

other similar devices. See Central management for more information about using the Remote Manager to manage and configure your IX10 device.

- The local web interface. See Using the local web interface for more information about using the local web interface to manage and configure your IX10 device.

> **Note** Changes made to the device's configuration by using the local web interface will not be automatically reflected in Digi Remote Manager. You must manually refresh Remote Manager for the changes to be displayed.

Web-based instructions in this guide are applicable to both the Remote Manager and the local web interface.

- Command line.

  A robust command line allows you to perform all configuration and management tasks from within a command shell. Both the Remote Manager and the local web interface also have the option to open a terminal emulator for executing commands on your IX10 device. See Using the command line for more information about using the command line to manage and configure your IX10 device.

In this guide, task topics show how to perform tasks:

Web

Shows how to perform a task by using the local web interface.

Command line

Shows how to perform a task by using the command line interface.

Using Digi Remote Manager

By default, your IX10 device is configured to use Digi Remote Manager as its central management server. Devices must be registered with Remote Manager using one of the following options:

- As part of the getting started process. See the Quick Start Guide for information.
- If you have not registered the device already, you can do so using the Device ID, MAC address, IMEI, or your Remote Manager login credentials. See Add a device to Remote Manager.

For information about configuring central management for your IX10 device, see Central management.

Access Digi Remote Manager

To access Digi Remote Manager:

1. If you have not already done so, go to https://myaccount.digi.com/ to sign up for a Digi Remote Manager account.
2. Check your email for Digi Remote Manager login instructions.
3. Go to remotemanager.digi.com.
4. Enter your user name and password. The Digi Remote Manager Dashboard appears.

Using the local web interface

To connect to the IX10 local Web UI:

1. Use an Ethernet cable to connect the IX10's **ETH** port to a laptop or PC.
2. Open a browser and go to **192.168.210.1**.
3. Log into the device using a configured user name and password.

   The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.

Review the dashboard

After logging in, the local web admin dashboard is displayed.

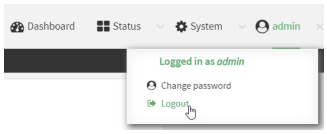
The dashboard shows the current state of the device.

Dashboard area	Description
Network activity	■ Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices. ■ Displays the status of the network interfaces configured on the device. ■ Provides information about the signal strength and technology of the cellular modem(s).
Digi Remote Manager	Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See Using Digi Remote Manager. The links in this section enable you to do the following: ■ **Launch Digi Remote Manager**: Click **Go To Digi Remote Manager** to open the Digi Remote Manager login page. ■ **Add a device to Remote Manager**: Click **Register device in new account** to add a device to Remote Manager using your Remote Manager login credentials.
Device	Displays the IX10 device's status, statistics, and identifying information.
Serial Ports	Displays information about the serial ports on the IX10. Each serial port is identified by port name or number, followed by the serial port mode configured for the port. The icons next to the port name or number shows the serial port status: ■ **Empty circle**: Port is not connected. ■ **Green circle**: Active connection on the port. ■ **Red X**: No signal, which is an error state where the port is not available. ■ **Down arrow**: One of the control signals is not active. This icon may display For for ports configured in **Remote Access** serial port mode and that have a signal monitor enabled (CTS or DCD) in the **Monitoring Settings** section. You can click the icons at the top of the section to access other pages: ■ **Blue "i"**: Click to access the Serial Status page.

Dashboard area	Description
	▪ **Blue wrench**: Click to access the Serial Configuration page.
Services	Displays an option for the Watchdog service if it has been enabled.

Log out of the web interface

- On the main menu, click your user name. Click **Log out**.



Review the dashboard

After logging in, the local web admin dashboard is displayed.

The dashboard shows the current state of the device.

Dashboard area	Description
Network activity	▪ Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices. ▪ Displays the status of the network interfaces configured on the device. ▪ Provides information about the signal strength and technology of the cellular modem(s).
Digi Remote Manager	Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See Using Digi Remote Manager. The links in this section enable you to do the following: ▪ **Launch Digi Remote Manager**: Click **Go To Digi Remote Manager** to open the Digi Remote Manager login page. ▪ **Add a device to Remote Manager**: Click **Register device in new account** to add a device to Remote Manager using your Remote Manager login credentials.
Device	Displays the IX10 device's status, statistics, and identifying information.
Serial Ports	Displays information about the serial ports on the IX10. Each serial port is identified by port name or number, followed by the serial port mode configured for the port. The icons next to the port name or number shows the serial port status: ▪ **Empty circle**: Port is not connected. ▪ **Green circle**: Active connection on the port. ▪ **Red X**: No signal, which is an error state where the port is not available.

Dashboard area	Description
	▪ **Down arrow**: One of the control signals is not active. This icon may display For for ports configured in **Remote Access** serial port mode and that have a signal monitor enabled (CTS or DCD) in the **Monitoring Settings** section. You can click the icons at the top of the section to access other pages: ▪ **Blue "i"**: Click to access the Serial Status page. ▪ **Blue wrench**: Click to access the Serial Configuration page.
Services	Displays an option for the Watchdog service if it has been enabled.

Use the local REST API to configure the IX10 device

Your IX10 device includes a REST API that can be used to return information about the device's configuration and to make modifications to the configuration. You can view the REST API specification from your web browser by opening the URL:

https://*ip-address*/cgi-bin/config.cgi

For example:

https://192.168.210.1/cgi-bin/config.cgi

Use the GET method to return device configuration information

To return device configuration, issue the **GET** method. For example, using **curl**:

```
$ curl -k -u admin https://ip-address/cgi-bin/config.cgi/value/path -X GET
```

where:

- *ip-address* is the IP address of the IX10 device.
- *path* is the path location in the configuration for the information being returned.

  To determine allowed values for *path* from the Admin CLI:

  1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
  2. At the command line, type **config** to enter configuration mode:

     ```
     > config
     (config)>
     ```
  3. At the config prompt, type **?** (question mark):

     ```
     (config)> ?
     auth            Authentication
     cloud           Central management
     firewall        Firewall
     ```

```
monitoring          Monitoring
network             Network
serial              Serial
service             Services
system              System
vpn                 VPN

(config)>
```

The allowed values for *path* are listed in the first (left) column.

4. To determine further allowed path location values by using the **?** (question mark) with the path name:

```
(config> service ?

Services

 Additional Configuration
 ------------------------------------------------------------------------------
dns                 DNS
iperf               IPerf
location            Location
mdns                Service Discovery (mDNS)
modbus_gateway      Modbus Gateway
multicast           Multicast
ntp                 NTP
ping                Ping responder
snmp                SNMP
ssh                 SSH
telnet              Telnet
web_admin           Web administration

(config)> service
```

For example, to use **curl** to return the ssh configuration:

```
$ curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/value/service/ssh -X GET
Enter host password for user 'admin':
{
ok": true,
     "result": {
          "type": "object",
          "path": "service.ssh"
,         "collapsed": {
"acl.zone.0": "internal"
,
"acl.zone.1": "edge"
,
"acl.zone.2": "ipsec"
,
"acl.zone.3": "setup"
,
"enable": "true"
,
```

```
"key": ""
,
"mdns.enable": "true"
,
"mdns.name": ""
,
"mdns.type": "_ssh._tcp."
,
"port": "22"
,
"protocol.0": "tcp"
            }
      }
}
$
```

You can also use the **GET** method to return the configuration parameters associated with an item:

```
curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/keys/service/ssh -X GET
Enter host password for user 'admin':
{ "ok": true, "result": [ "acl", "custom", "enable", "key", "mdns", "port", "protocol" ] }
$
```

Use the POST method to modify device configuration parameters and list arrays

Use the POST method to modify device configuration parameters

To modify configuration parameters, use the **POST** method with the **path** and **value** parameters.

```
$ curl -k -u admin "https://ip-address/cgi-bin/config.cgi/value?path=path&value=new_value" -X POST
```

where:

- *path* is the path to the configuration parameter, in dot notation (for example, **ssh.service.enable**).
- *new_value* is the new value for the parameter.

For example, to disable the ssh service using **curl**:

```
$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=service.ssh.enable&value=false" -X
POST
Enter host password for user 'admin':
{ "ok": true }
$
```

Use the POST method to add items to a list array

To add items to a list array, use the **POST** method with the **path** and **append** parameters. For example, to add the external firewall zone to the ssh service:

```
$ curl -k -u admin "https://192.168.210.1/cgi-
bin/config.cgi/value?path=service.ssh.acl.zone&append=true&value=external" -X POST
Enter host password for user 'admin':
{ "ok": true, "result": "service.ssh.acl.zone.4" }
$
```

Use the POST method to add objects to a list array

Objects in an array that require one or more underlying values can be set using the **collapsed** URI parameter. We recommend including the -g option as well, to instruct curl to turn off globbing. The below example would add a new static route for the WAN interface for the 1.2.4.0/24 destination network:

```
$ curl -g -k -u admin "https://192.168.210.1/cgi-
bin/config.cgi/value?path=network.route.static&append=true&collapsed[dst]=1.2.4.0/24&collapsed
[interface]=/network/interface/wan" -X POST
Enter host password for user 'admin':
{ "ok": true, "result": "network.route.static.1" }
$
```

Use the DELETE method to remove items from a list array

To remove items from a list array, use the **DELETE** method. For example, using **curl**:

```
$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=path
```

where *path* is the path to the list item, including the list number, in dot notation (for example, **service.ssh.acl.zone.4**).

For example, to remove the external firewall zone to the ssh service:

1. Use the **GET** method to determine the SSH service's list number for the external zone:

```
$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=service/ssh/acl/zone -X GET
{
    "ok": true,
    "result": {
        "type": "array",
        "path": "service.ssh.acl.zone"
,       "collapsed": {
"0": "internal"
,
"1": "edge"
,
"2": "ipsec"
,
"3": "setup"
,
"4": "external"
        }
    }
}
$
```

2. Use the **DELETE** method to remove the external zone (list item 4).

```
$ curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/value?path=service.ssh.acl.zone.4 -X
DELETE
Enter host password for user 'admin':
{ "ok": true }
$
```

Using the command line

The Digi IX10 device provides a command-line interface that you can use to configure the device, display status and statistics, update firmware, and manage device files.

See Command line interface for detailed instructions on using the command line interface and see Command line reference for information on available commands.

Access the command line interface

You can access the IX10 command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

You can also access the command line interface in the WebUI by using the **Terminal**, or the Digi Remote Manager by using the **Console**.

To access the command line, your device must be configured to allow access, and you must log in as a user who has been configured for the appropriate access.

For further information about configuring access to these services, see:

- Serial: Serial port
- WebUI: Configure the web administration service
- SSH: Configure SSH access
- Telnet: Configure telnet access

Log in to the command line interface

Command line

1. Connect to the IX10 device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See Access the command line interface for more information.

   Note Telnet is not available when Primary Responder mode has been enabled for the device. For information about Primary Responder mode, see Differences between standard firmware operation and Primary Responder mode.

   - For serial connections, the default configuration is:
     - **9600** baud rate
     - **8** data bits
     - **no** parity
     - **1** stop bit
     - **no** flow control
   - For SSH and telnet connections, the Setup IP address of the device is **192.168.210.1** on the .

2. At the login prompt, enter the username and password of a user with Admin access:

```
login: admin
Password: **********
```

   The default username is **admin**. The default unique password for your device is printed on the device label.

3. Depending on the device configuration, you may be presented with another menu, for example:

```
Access selection menu:

    a: Admin CLI
    s: Shell
    q: Quit

Select access or quit [admin] :
```

   Type **a** or **admin** to access the IX10 command line.

You will now be connected to the Admin CLI:

```
Connecting now...
 Press Tab to autocomplete commands
 Press '?' for a list of commands and details
 Type 'help' for details on navigating the CLI
 Type 'exit' to disconnect from the Admin CLI

>
```

See Command line interface for detailed instructions on using the command line interface.

Exit the command line interface

Command line

1. At the command prompt, type **exit**.

```
> exit
```

2. Depending on the device configuration, you may be presented with another menu, for example:

```
Access selection menu:

    a: Admin CLI
    s: Shell
    q: Quit

Select access or quit [admin] :
```

   Type **q** or **quit** to exit.

Central management

This chapter contains the following topics:

Digi Remote Manager support 68
Certificate-based enhanced security 68
Configure your device for Digi Remote Manager support 68
Reach Digi Remote Manager on a private network 80
Log in to Digi Remote Manager 80
Use Digi Remote Manager to view and manage your device 82
Add a device to Remote Manager 82
Configure multiple IX10 devices by using Digi Remote Manager configurations 84
View Digi Remote Manager connection status 85
Learn more 86

Digi Remote Manager support

Digi Remote Manager is a hosted remote configuration and management system that allows you to remotely manage a large number of devices. Remote Manager includes a web-based interface that you can use to perform device operations, such as viewing and changing device configurations and performing firmware updates. Remote Manager servers also provide a data storage facility. The Digi Remote Manager is the default cloud-based management system, and is enabled by default.

To use Remote Manager, you must set up a Remote Manager account. To set up a Remote Manager account and learn more about Digi Remote Manager, go to http://www.digi.com/products/cloud/digi-remote-manager.

To learn more about Remote Manager features and functions, see the *Digi Remote Manager User Guide*.

Certificate-based enhanced security

Beginning with firmware version 22.2.9.x, the default URL for the device's Remote Manager connection is edp12.devicecloud.com. This URL is required to utilize the client-side certificate support. Prior to release 22.2.9.x, the default URL was my.devicecloud.com.

- If your Digi device is configured to use a non-default URL to connect to Remote Manager, updating the firmware will not change your configuration. However, if you erase the device's configuration, the Remote Manager URL will change to the default of edp12.devicecloud.com.
- If you perform a factory reset by pressing the **ERASE** twice, the client-side certificate will be erased and you must use the Remote Manager interface to reset the certificate. Select the device in Remote Manager and select **Actions** > **Reset Device Certificate**.
- The certificate that is provided to the client by Remote Manager is signed by a specific certificate authority, and the device is expecting that same certificate authority. If your IT infrastructure uses its own certificate-based authentication, this might cause the device to interpret the certificate provided by Remote Manager as being from an incorrect certificate authority. If this is the case, you need to include an exception to allow edp12.devicecloud.com to authenticate using its own certificate.

The new URL of edp12.devicecloud.com is for device communication only. Use https://remotemanager.digi.com for user interaction with remote manager.

Firewall issues

To utilize the certificate-based security, you may need to open a port through your firewall for egress connectivity to edp12.devicecloud.com. TCP port 3199 is used for communication with Remote Manager.

Configure your device for Digi Remote Manager support

By default, your IX10 device is configured to use for central management.

Additional configuration options

These additional configuration settings are not typically configured, but you can set them as needed:

- Disable the Digi Remote Manager connection if it is not required. You can also configure an alternate cloud-based central management application.
- Change the reconnection timer.
- The non-cellular keepalive timeout.
- The cellular keepalive timeout.
- The keepalive count before the Remote Manager connection is dropped.
- SMS support.
- HTTP proxy server support.

To configure your device's Digi Remote Manager support:

Web

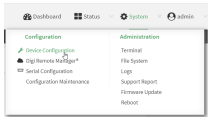
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

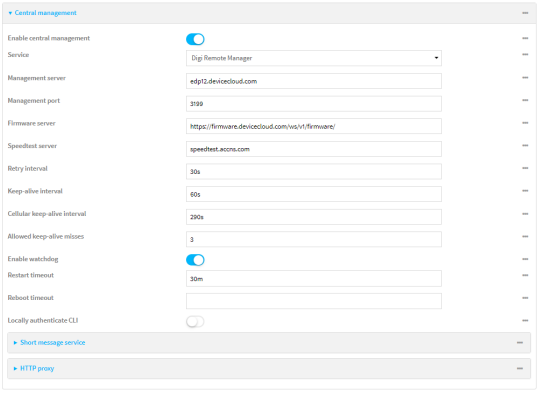
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **Central management**.

   The Central management configuration window is displayed.



   Digi Remote Manager support is enabled by default. To disable, toggle off **Enable central management**.

4. For **Service**, select **Digi Remote Manager**.
5. (Optional) For **Management server**, type the URL for the central management server.

   The default varies depending on firmware versions:

   - Firmware version 22.2.9.x and newer, the default is the edp12.devicecloud.com. This server is for device-connectivity only, and uses enhanced security through certificate-based communication. See Digi Remote Manager support for further infomation.
   - Firmware prior to version 22.2.9.x, the default is the Digi Remote Manager server, https://remotemanager.digi.com.

6. (Optional) For **Management port**, type the destination port for the remote cloud services connection. The default is **3199**.
7. **Firmware server** should normally be left at the default location.
8. (Optional) For **Speedtest server**, type the name or IP address of the server to use to test the speed of the device's internet connection(s).
9. (Optional) For **Retry interval**, type the amount of time that the IX10 device should wait before reattempting to connect to remote cloud services after being disconnected. The default is 30 seconds.

   Allowed values are any number of hours, minutes, or seconds, and take the format ***number*** {**h|m|s**}.

   For example, to set **Retry interval** to ten minutes, enter **10m** or **600s**.
10. (Optional) For **Keep-alive interval**, type the amount of time that the IX10 device should wait between sending keep-alive messages to remote cloud services when using a non-cellular interface. The default is 60 seconds.

    Allowed values are any number of hours, minutes, or seconds, and take the format ***number*** {**h|m|s**}.

    For example, to set **Keep-alive interval** to ten minutes, enter **10m** or **600s**.
11. (Optional) For **Cellular keep-alive interval**, type the amount of time that the IX10 device should wait between sending keep-alive messages to remote cloud services when using a cellular interface. The default is 290 seconds.

Allowed values are any number of hours, minutes, or seconds, and take the format ***number*** {**h|m|s**}.

For example, to set **Cellular keep-alive interval** to ten minutes, enter **10m** or **600s**.

12. (Optional) For **Allowed keep-alive misses**, type the number of allowed keep-alive misses. The default is **3**.
13. **Enable watchdog** is used to monitor the connection to Digi Remote Manager. If the connection is down, you can configure the device to restart the connection, or to reboot. The watchdog is enabled by default. To configure the Watchdog service and view metrics, see Watchdog service.
14. If **Enable watchdog** is enabled:
    a. (Optional) For **Restart Timeout**, type the amount of time to wait before restarting the connection to the remote cloud services, once the connection is down.

    Allowed values are any number of hours, minutes, or seconds, and take the format ***number***{**h|m|s**}.

    For example, to set **Restart Timeout** to ten minutes, enter **10m** or **600s**.

    The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is 30 minutes.

    b. (Optional) For **Reboot Timeout**, type the amount of time to wait before rebooting the device, once the connection to the remote cloud servicesis down. By default, this option is not set, which means that the option is disabled.

    Allowed values are any number of hours, minutes, or seconds, and take the format ***number***{**h|m|s**}.

    For example, to set **Reboot Timeout** to ten minutes, enter **10m** or **600s**.

    The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is disabled.
15. (Optional) Enable **Locally authenticate CLI** to require a login and password to authenticate the user from the remote cloud services CLI. If disabled, no login prompt will be presented and the user will be logged in as **admin**. The default is disabled.
16. (Optional) Configure the IX10 device to communicate with remote cloud services by using SMS:
    a. Click to expand **Short message service**.
    b. **Enable** SMS messaging.
    c. For **Destination phone number**, type the phone number for the remote cloud services:
        - Within the US: **12029823370**
        - International: **447537431797**
    d. (Optional) Type the **Service identifier**.
17. (Optional) Configure the IX10 device to communicate with remote cloud services via one of two methods: Pinhole or Proxy server.
    If using the Pinhole method, refer to the following
    If using the Proxy server method:
    a. Click to expand **HTTP Proxy**.
    b. **Enable** the use of an HTTP proxy server.
    c. For **Server**, type the hostname of the HTTP proxy server.

d. For **Port**, type or select the port number on the HTTP proxy server that the device should connect to. The default is **2138**.

18. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Digi Remote Manager support is enabled by default. To disable Remote Manager support:

```
(config)> cloud enable false
(config)>
```

4. (Optional) Set the URL for the central management server.

```
(config)> cloud drm drm_url url
(config)>
```

   The default varies depending on firmware versions:

   - Firmware version 22.2.9.x and newer, the default is the edp12.devicecloud.com. This server is for device-connectivity only, and uses enhanced security through certificate-based communication. See Digi Remote Manager support for further infomation.
   - Firmware prior to version 22.2.9.x, the default is the Digi Remote Manager server, https://remotemanager.digi.com.

5. (Optional) Set the amount of time that the IX10 device should wait before reattempting to connect to the remote cloud services after being disconnected. The minimum value is ten seconds. The default is 30 seconds.

```
(config)> cloud drm retry_interval value
```

   where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

   For example, to set **the retry interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> cloud drm retry_interval 600s
(config)>
```

6. (Optional) Set the amount of time that the IX10 device should wait between sending keep-alive messages to the Digi Remote Manager when using a non-cellular interface. Allowed values are from 30 seconds to two hours. The default is 60 seconds.

```
(config)> cloud drm keep_alive value
(config)>
```

where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

For example, to set **the keep-alive interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> cloud drm keep_alive 600s
(config)>
```

7. (Optional) Set the amount of time that the IX10 device should wait between sending keep-alive messages to the Digi Remote Manager when using a cellular interface. Allowed values are from 30 seconds to two hours. The default is 290 seconds.

   ```
   (config)> cloud drm cellular_keep_alive value
   (config)>
   ```

   where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

   For example, to set **the cellular keep-alive interval** to ten minutes, enter either **10m** or **600s**:

   ```
   (config)> cloud drm cellular_keep_alive 600s
   (config)>
   ```

8. Set the number of allowed keep-alive misses. Allowed values are any integer between **2** and **64**. The default is **3**.

   ```
   (config)> cloud drm keep_alive_misses integer
   (config)>
   ```

9. The **watchdog** is used to monitor the connection to remote cloud services. If the connection is down, you can configure the device to restart the connection, or to reboot. The watchdog is enabled by default. To disable:

   ```
   (config)> cloud drm watchdog false
   (config)>
   ```

10. If **watchdog** is enabled:
    a. (Optional) Set the amount of time to wait before restarting the connection to the remote cloud services, once the connection is down.

       where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

       For example, to set **restart_timeout** to ten minutes, enter either **10m** or **600s**:

       ```
       (config)> cloud drm restart_timeout 600s
       (config)>
       ```

       The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is 30 minutes.

    b. (Optional) Set the amount of time to wait before rebooting the device, once the connection to the remote cloud servicesis down. By default, this option is not set, which means that the option is disabled.

where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

For example, to set **reboot_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> cloud drm reboot_timeout 600s
(config)>
```

The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is disabled.

11. **firmware_url** should normally be left at the default location. To change:

```
(config)> cloud drm firmware_url url
(config)>
```

12. (Optional) Set the hostname or IP address of the speedtest server. The default is speedtest.accns.com.

```
(config)> cloud drm speedtest_server name
(config)>
```

13. (Optional) Determine whether to require a login and password to authenticate the user from the remote cloud services CLI:

```
(config)> cloud drm cli_local_auth true
(config)>
```

If set to **false**, no login prompt will be presented and the user will be logged in as **admin**. The default is **false**.

14. (Optional) Configure the IX10 device to communicate with remote cloud services by using SMS:
    a. **Enable** SMS messaging:

```
(config)> cloud drm sms enable true
(config)>
```

    b. Set the phone number for Digi Remote Manager:

```
(config)> cloud drm sms destination value
(config)>
```

    where *value* is either:
    - Within the US: **12029823370**
    - International: **447537431797**

    c. (Optional) Set the service identifier:

```
(config)> cloud drm sms sercice_id id
(config)>
```

15. (Optional) Configure the IX10 device to communicate with remote cloud services by using an HTTP proxy server:

a. **Enable** the use of an HTTP proxy server:

```
(config)> cloud drm proxy enable true
(config)>
```

b. Set the hostname of the proxy server:

```
(config)> cloud drm proxy host hostname
(config)>
```

c. (Optional) Set the port number on the proxy server that the device should connect to. The default is 2138.

```
(config)> cloud drm proxy port integer
(config)>
```

16. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

17. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Collect device health data and set the sample interval

You can enable or disable the collection of device health data to upload to Digi Remote Manager, and configure the interval between health sample uploads. By default, device health data upload is enabled, and the health sample interval is set to 60 minutes. Each time a device connects to Digi Remote Manager after the device boots (or re-boots), the device immediately uploads all health metrics.

To avoid a situation where several devices are uploading health metrics information to Remote Manager at the same time, the IX10 device includes a preconfigured randomization of two minutes for uploading metrics. For example, if **Health sample interval** is set to five minutes, the metrics will be uploaded to Remote Manager at a random time between five and seven minutes.

To disable the collection of device health data or enable it if it has been disabled, or to change the health sample interval:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

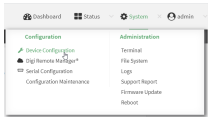
   b. Click the **Device ID**.

   c. Click **Settings**.

d. Click to expand **Config**.

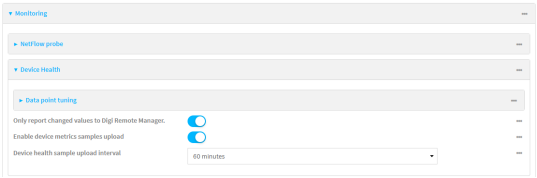
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring** > **Device Health**.



4. (Optional) Click to expand **Data point tuning**.

   Data point tuning options allow to you configure what data are uploaded to the Digi Remote Manager. All options are enabled by default.

5. **Only report changed values to Digi Remote Manager** is enabled by default.

   When enabled:

   - The device only reports device health metrics that have changed health metrics were last uploaded. This is useful to reduce the bandwidth used to report health metrics.
   - All metrics are uploaded once every hour.

   When disabled, all metrics are uploaded every **Health sample interval**.

6. Device health data upload is enabled by default. To disable, toggle off **Enable Device Health samples upload**.
7. For **Health sample interval**, select the interval between health sample uploads.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Device health data upload is enabled by default. To enable or disable:
   - To enable:

     ```
     (config)> monitoring devicehealth enable true
     (config)>
     ```

   - To disable:

     ```
     (config)> monitoring devicehealth enable false
     (config)>
     ```

4. The interval between health sample uploads is set to 60 minutes by default. To change:

   ```
   (config)> monitoring devicehealth interval value
   (config)>
   ```

   where *value* is one of **1**, **5**, **15**, **30**, or **60**, and represents the number of minutes between uploads of health sample data.

5. By default, the device will only report health metrics values to Digi Remote Manager that have changed health metrics were last uploaded. This is useful to reduce the bandwidth used to report health metrics. This is useful to reduce the bandwidth used to report health metrics. Even if enabled, all metrics are uploaded once every hour.

   To disable:

   ```
   (config)> monitoring devicehealth only_send_deltas false
   (config)>
   ```

   When disabled, all metrics are uploaded every **Health sample interval**.

6. (Optional) Tuning parameters allow to you configure what data are uploaded to the Digi Remote Manager. By default, all tuning parameters are enabled.

   To view a list of all available tuning parameters, use the **show** command:

   ```
   (config)> show monitoring devicehealth tuning
   all
       cellular
           rx
               bytes
                   enable true
           tx
               bytes
                   enable true
       eth
           rx
               bytes
                   enable true
           tx
               bytes
                   enable true
       serial
           rx
   ```

```
                bytes
                    enable true
            tx
                bytes
                    enable true
cellular
    1
            rx
                bytes
                    enable true
                packets
                    enable true
...
                                (config)>
```

To disable a tuning parameter, set its value to false. For example, to turn off all reporting for the serial port:

```
(config)> monitoring devicehealth tuning all serial rx bytes enabled false
(config)> monitoring devicehealth tuning all serial tx bytes enabled false
(config)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Event log upload to Digi Remote Manager

Your device is automatically configured to upload the event log to Digi Remote Manager. These logs are uploaded every 60 minutes.

Change the upload interval

To change how often the event logs are uploaded to Digi Remote Manager:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

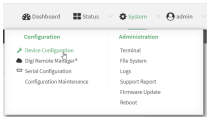
   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.

d. Click to expand **Config**.

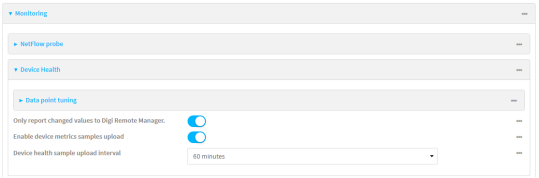
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring** > **Device event logs**.



4. For **Device event log upload interval**, change the interval between health sample uploads. The default is **60 minutes**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The interval between event log uploads is set to 60 minutes by default. To change:

```
(config)> monitoring events interval value
(config)>
```

   where *value* is one of **1**, **5**, **15**, **30**, or **60**, and represents the number of minutes between uploads of health sample data.
4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Reach Digi Remote Manager on a private network

If your company has a private network and you have devices that need to reach Digi Remote Manager, there are several methods available:

- **Pinhole**: a communication port on your network not protected by the firewall which allows the application on the device to reach Digi Remote Manager.
- **Proxy server**: a dedicated software system equipped with its own IP address that runs on your network and acts as an intermediary between the device and Digi Remote Manager.
- **VPN Tunnel**: a virtual private network that offers a secure, encrypted connection between a device and the internet.

Pinhole method

Using the pinhole method requires your network administrator to remove the firewall connection on a communication port. For more information, see Firewall concerns for outbound EDP connections to Digi Remote Manager.

Proxy server method

The device is capable of connecting through an HTTP proxy, such as Squid, but it is up to the network administrator to decide which HTTP proxy type to use.

To enable a proxy server and enter the server and port in Digi Remote Manager, see step 17 in Configure your device for Digi Remote Manager support.

Tip To see instructions for setting up Squid and then configuring a device (not DAL) to reach Digi Remote Manager, see the Digi Quick Note, Connecting to Digi Remote Manager Through Web Proxy. Though this Quick Note references older technology and device types, it may provide a network administrator with concrete examples from which they can draw correlations to newer technology and devices.

VPN Tunnel method

Configuring a VPN tunnel to communicate with Digi Remote Manager is a two-step process. One step is done by your organization's network administrator and the other by Digi Support.

Step 1: Set up the VPN tunnel

Your organization's network administrator needs to set up a VPN tunnel on your network, which will be used to communicate with Digi Remote Manager through the Digi cloud service.

Step 2. Contact Digi Support.

Digi Support configures the Digi cloud service to allow your VPN to communicate with Digi Remote Manager. Contact Digi Support at https://www.digi.com/contactus.

Log in to Digi Remote Manager

To log in to Remote Manager:

1. In a web browser, go to remotemanager.digi.com.
2. Type your username.
3. Click **Continue**.

4. Type your password.
5. Click **Login**.

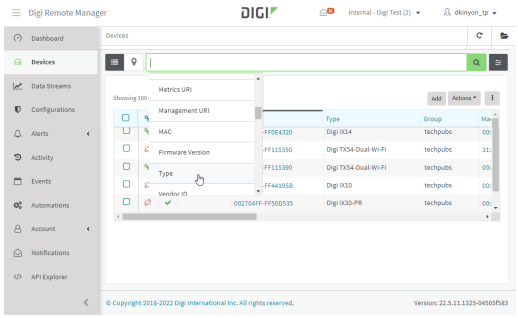
   If you used the same browser tab/window to log in again, you will see the page you were on in your previous session. If you opened a new browser tab/window to log in, you will see the default fleet Dashboard page.

Tip If you cannot remember your password, go to remotemanager.digi.com, type your username and then click **Forgot username?**. You will be asked to provide your email address associated with your user account. If you are not sure that you have a user account, talk with your Remote Manager administrator.

Use Digi Remote Manager to view and manage your device

To view and manage your device:

1. If you have not already done so, connect to your Digi Remote Manager account.
2. From the menu, click **Devices** to display a list of your devices.
3. Use the Filter bar to locate the device you want to manage. For example, to search by type of device:
   a. Click the Advanced Search button ( )
   b. Click in the filter bar.



   c. Type the type of device (for example, IX10).

Add a device to Remote Manager

There are several options for adding a device to Remote Manager.

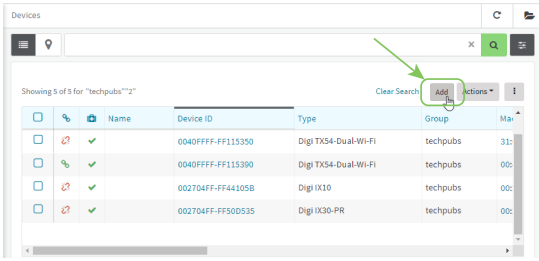
- **Device label information.** Use the information on the device label (e.g., Device ID, MAC address, Password) to add a new device to Remote Manager. See Add a device to Remote Manager using information from the label.
- **Digi Remote Manager credentials.** Use your Remote Manager credentials to add a device to Remote Manager when you do not have the device password. See Add a device to Remote Manager using your Remote Manager login credentials.

Add a device to Remote Manager using information from the label

Tip If you do not have access to the device label, you can add the device using your Remote Manager login credentials. See Add a device to Remote Manager using your Remote Manager login credentials.

1. If you have not already done so, connect to your Digi Remote Manager account.
2. From the menu, click **Devices** to display a list of your devices.

3. Click **Add**.



4. Type the Device ID, MAC Address, or IMEI.
5. For **Device Default Password**, enter the default password on the printed label packaged with your device. The same default password is also shown on the label affixed to the bottom of the device.
6. (Optional) Complete the other fields.
1. Click **Add Device**.
   Remote Manager adds the IX10 device to your account and it appears in the **Device Management** view.

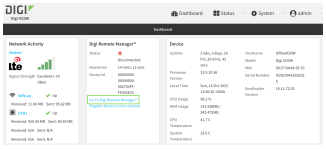
Add a device to Remote Manager using your Remote Manager login credentials

If you want to add a device to Remote Manager, and you do not have its password, you can add it using your Remote Manager login credentials.

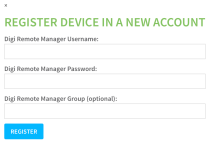
To add a device using your Remote Manager credentials:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the dashboard, in **Digi Remote Manager** status pane, click **Register device in new account**.



3. The **Register Device in New Account** page displays.



4. For **Digi Remote Manager Username**, type your Remote Manager username.
5. For **Digi Remote Manager Password**, type your Remote Manager password.
6. For **Digi Remote Manager Group (optional)**, type the group to which the device will be added, if needed.
7. Click **Register**.

The device is added to Remote Manager.

Command line

1. Log into the IX10 local command line as a user with full Admin access rights.
2. Register a device.

```
(register) [group STRING] password STRING username STRING
```

where:

- group: group to add device in Digi Remote Manager.
- password: Digi Remote Manager password (required).
- username: Digi Remote Manager username (required).

1. Click **Apply** to save the configuration and apply the change.
2. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

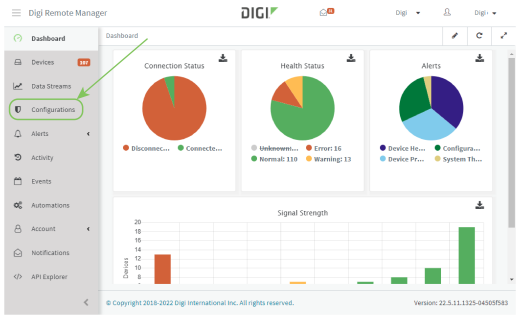
Configure multiple IX10 devices by using Digi Remote Manager configurations

Digi recommends you take advantage of Remote Manager configurations to manage multiple IX10 devices. A Remote Manager configuration is a named set of device firmware, settings, and file system options. You use the configuration to automatically update multiple devices and to periodically scan devices to check for compliance with the configuration. See the *Digi Remote Manager User Guide* for more information about Remote Manager configurations.

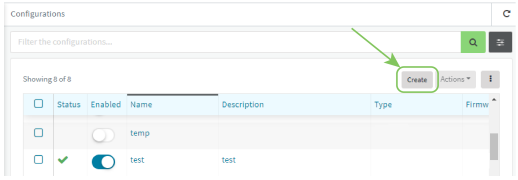
Typically, if you want to provision multiple IX10 routers:

1. Using the IX10 local WebUI, configure one IX10 router to use as the model configuration for all subsequent IX10s you need to manage.
2. Register the configured IX10 device in your Remote Manager account.

3. In Remote Manager, create a configuration:
   a. From the Dashboard, select Configurations.



   b. Click **Create**.



   c. Enter a **Name** and an optional **Description** for the configuration, and select the **Groups**, **Device Type**, and **Firmware Version**.
   d. Click **Save and continue**.
   e. Click **Import from device** and select the device configured above.
   f. Click **Import**.
   g. At the **Settings** page, configure any desired configuration overrides and click **Continue**.
   h. At the **File System** page, make any desired changes to the files that were imported from the device and click **Continue**.
   i. At the Automations page, click **Enable Scanning**, make any other desired changes, and click **Save**.

Digi Remote Manager provides multiple methods for applying configurations to registered devices. You can also include site-specific settings with a profile to override settings on a device-by-device basis.

View Digi Remote Manager connection status

To view the current Digi Remote Managerconnection status from the local device:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
   The dashboard includes a Digi Remote Manager status pane:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show cloud command to view the status of your device's connection to Remote Manager:

```
> show cloud

Device Cloud Status
-------------------

Status    : Connected
Server    : edp12.devicecloud.com Device ID : 00000000-00000000-89E1FE-7550D7>
```

1. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Learn more

To learn more about Digi Remote Manager features and functions, see the *Digi Remote Manager User Guide*.

Interfaces

IX10 devices have several physical communications interfaces. These interfaces can be bridged in a Local Area Network (LAN) or assigned to a Wide Area Network (WAN).

This chapter contains the following topics:

Wireless Wide Area Networks (WWANs) 88
Local Area Networks (LANs) 157
Virtual LANs (VLANs) 193
Show SureLink status and statistics 199

Wireless Wide Area Networks (WWANs)

A Wireless Wide Area Network (WWAN) provides connectivity to the internet or a remote network through a cellular connection. A WWAN configuration consists of the following:

- A cellular modem.
- Several networking parameters for the WAN, such as firewall configuration and IPv4 and IPv6 support.
- Several parameters controlling failover.

Configure SureLink active recovery to detect modem failures

Problems can occur beyond the immediate modem connection that prevent some IP traffic from reaching its destination. Normally this kind of problem does not cause the IX10 device to detect that the modem has failed, because the connection continues to work while the core problem exists somewhere else in the network.

Using Digi SureLink, you can configure the IX10 device to regularly probe connections through the modem to determine if the modem connection has failed.

Required configuration items

- By default, SureLink is enabled for the preconfigured **Modem** interface. The default configuration tests the DNS servers configured for the interface.

  When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the IX10 device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.
- The type of tests to be performed:
  - **Ping test**: Uses ICMP to determine connectivity. The default behavior is to ping the interface gateway, which means that an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
  - **DNS test**: Performs a DNS query to the named DNS server.
  - **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.
  - **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
  - **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.
  - **Custom test**: Tests the interface with custom commands.
  - **TCP connection test**: Tests that the interface can reach a destination port on the configured host.
  - **Test another interface's status**: Tests the status of another interface.
- The actions to take to recover connectivity in the event of failed tests:
  - **Change default gateway**: Increases the interface's metric to change the default gateway. This recovery action is enabled by default for the preconfigured WWAN interface.

- **Restart interface**This recovery action is enabled by default for the preconfigured WWAN interface.
- **Reset modem**: This recovery action is enabled by default for the preconfigured WWAN interface.
- **Switch to alternate SIM**: Switches to an alternate SIM. This recovery action is enabled by default for the preconfigured WWAN interface.
- **Reboot device**.
- Execute custom **Recovery commands**.
- **Powercycle the modem**. This recovery action is enabled by default for the preconfigured WWAN interface.
- Two options also apply to every type of action:
  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

Additional configuration items

- The behavior of the IX10 device upon test failure:
  - The default behavior, which is to restart the **Modem** interface.
  - SIM switching (also enabled by default).
  - Reset the modem.
  - Reboot the device.
- The interval between connectivity tests.
- The number of probe failures before the Modem interface is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.
- If the type of probe test is:
  - Ping: Configure the number of bytes in the ping packet.
  - Interface status: Configure the amount of time that the interface is down before it is considered to have failed, and the amount of time it takes to make an initial connection before it is considered down.
- Additional test targets.
- If more than one test target is configured, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.

Order of precedence for SureLink actions

SureLink recovery actions are preformed in the order that they are configured. As a result, if you include the **Reboot Device** with other SureLink recovery actions, it should be the last action in the recovery action list. Otherwise, the device will reboot and all recovery actions listed after the **Reboot Device** action will be ignored.

To configure the IX10 device to regularly probe connections through the WWAN:

Web

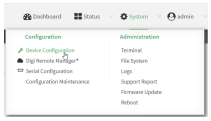
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

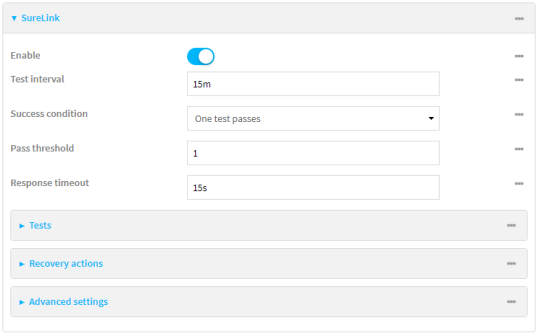
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Create a new WWAN or select an existing one:
   - To create a new WWAN, see Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WWAN, click to expand the appropriate WWAN.
5. After creating or selecting the WWAN, click **SureLink**.

6. (Optional) Change the **Test interval** between connectivity tests.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Interval** to ten minutes, enter **10m** or **600s**.

   The default is 15 minutes.
7. (Optional) If more than one test target is configured, for **Success condition**, select either:
   - **One test passes**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **All test pass**: All tests need to pass for SureLink to consider the interface to be up.

8. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
9. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

   The default is 15 seconds.
10. Click to expand **Tests**.

    By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

    a. Click .

    New tests are enabled by default. To disable, click to toggle off **Enable**.

    b. Type a **Label** for the test.

    c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.

    d. Select the **Test type**.

    Available test types:

    - **Ping test**: Uses ICMP to determine connectivity.

      If **Ping test** is selected, complete the following:

      - **Ping target:** The type of target for the ping, one of:
        - **Hostname or IP address** of an external server.
          - **Ping host**: hostname or IP address of the server.
        - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
        - The **Interface address**.
        - The **Interface DNS** server.
      - **Ping payload size:** The number of bytes to send as part of the ping payload.
    - **DNS test**: Performs a DNS query to the named DNS server.

      If **DNS test** is selected, complete the following:

      - **DNS server**: The IP address of the DNS server.
    - **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

      If **HTTP test** is selected, complete the following:

      - **Web server**: The URL of the web server.

- **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **Test the interface status** is selected, complete the following:

  - **Down time**: The amount of time that the interface is down before the test can be considered to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Down time** to ten minutes, enter **10m** or **600s**.
  - **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.
- **Custom test**: Tests the interface with custom commands.

  If **Custom test** is selected, complete the following:

  - The **Commands to run to test**.
- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

  If **TCP connection test** is selected, complete the following:

  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.
- **Test another interface's status**: Tests the status of another interface.

  If **Test another interface's status** is selected, complete the following:

  - **Test interface**: The interface to test.
  - **IP version**: The type of IP connection, one of:
    - **Any**: Either the IPv4 or IPv6 connection must be up.
    - **Both**: Both the IPv4 or IPv6 connection must be up.
    - **IPv4**: The IPv4 connection must be up.
    - **IPv6**: The IPv6 connection must be up.
  - **Expected status**: The status required for the test to past.
    - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

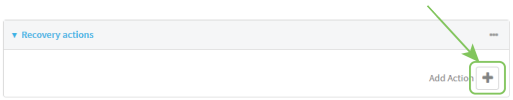
e. Repeat for each additional test.

11. Add recovery actions:
    a. Click to expand **Recovery actions**.

       By default, there are two preconfigured recovery actions:

       - **Update routing**: Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
       - **Restart interface**.

    b. Click ♑



       New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

    c. Type a **Label** for the recovery action.
    d. For **Recovery type**, select **Reboot device**.
    e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

       - **Change default gateway**: Increases the interface's metric to change the default gateway.

         If **Change default gateway** is selected, complete the following:

         - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
         - **Increase metric to change active default gateway**: Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
         - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

       - **Restart interface**.

         If **Restart interface** is selected, complete the following:

         - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
         - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

       - **Reset modem**: This recovery action is available for WWAN interfaces only.

         If **Reset modem** is selected, complete the following:

         - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
         - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Switch to alternate SIM**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **Switch to alternate SIM** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Reboot device**.

  If **Reboot device** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- Execute custom **Recovery commands**.

  If **Recovery commands** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - The **Commands to run to recovery connectivity**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Powercycle the modem**. This recovery action is available for WWAN interfaces only.

  If **Powercycle the modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

f. Repeat for each additional recovery action.

12. (Optional) Configure advanced SureLink parameters:
    a. Click to expand **Advanced settings**.
    b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

    The default is 300 seconds.

c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

The default is 300 seconds.

d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.

13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new WWAN, or edit an existing one:
   - To create a new WWAN, see Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WWAN, change to the WWAN's node in the configuration schema. For example, for a WWAN named **my_wwan**, change to the **my_wwan** node in the configuration schema:

```
(config)> network interface my_wwan
(config network interface my_wwan)>
```

4. Enable SureLink.

   By default, SureLink is enabled for the preconfigured WWAN (modem).

```
(config network interface my_wwan)> surelink enable true
(config network interface my_wwan)>
```

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

   To add additional tests:

   a. Add a test:

```
(config network interface my_wwan)> add surelink tests end
(config network interface my_wwan surelink tests 1)>
```

   b. New tests are enabled by default. To disable:

```
(config network interface my_wwan surelink tests 1)> enable false
(config network interface my_wwan surelink tests 1)>
```

c. Create a label for the test:

```
(config network interface my_wwan surelink tests 1)> label string
(config network interface my_wwan surelink tests 1)>
```

d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config network interface my_wwan surelink tests 1)> ipv6 true
(config network interface my_wwan surelink tests 1)>
```

e. Set the test type:

```
(config network interface my_wwan surelink tests 1)> test value
(config network interface my_wwan surelink tests 1)>
```

where *value* is one of:

- **ping**: Uses ICMP to determine connectivity.

  If **ping** is selected, complete the following:

  - Set the **ping_method**:

    ```
    (config network interface my_wwan surelink tests 1)> ping_method value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is one of:

    - **hostname**: The hostname or IP address of an external server.
      - Set **ping_host** to the hostname or IP address of the server:

        ```
        (config network interface my_wwan surelink tests 1)> ping_host hostname/IP_address
        (config network interface my_wwan surelink tests 1)>
        ```

    - **interface_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - **interface_address**.
    - **interface_dns**: The interface's DNS server.

  - Set the number of bytes to send as part of the ping payload:

    ```
    (config network interface my_wwan ipsec tunnel ipsec_example surelink tests 1)> ping_size int
    (config network interface my_wwan surelink tests 1)>
    ```

- **dns**: Performs a DNS query to the named DNS server.

  If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

```
(config network interface my_wwan surelink tests 1)> dns_server IP_address
(config network interface my_wwan surelink tests 1)>
```

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **http** is set, set the URL of the web server.

  ```
  (config network interface my_wwan surelink tests 1)> http url
  (config network interface my_wwan surelink tests 1)>
  ```

- **dns_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **interface_up** is set, complete the following:

  - Set the amount of time that the interface is down before the test can be considered to have failed.

    ```
    (config network interface my_wwan surelink tests 1)> interface_down_time value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number*{w|d|h|m|s}**.

    For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

    ```
    (config network interface my_wwan surelink tests 1)> interface_down_time 600s
    (config)>
    ```

  - Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

    ```
    (config network interface my_wwan surelink tests 1)> interface_timeout value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number*{w|d|h|m|s}**.

    For example, to set **interface_timeout** to ten minutes, enter either **10m** or **600s**:

    ```
    (config network interface my_wwan surelink tests 1)> interface_timeout 600s
    (config)>
    ```

- **custom_test**: Tests the interface with custom commands.

  If **custom_test** is set, set the commands to run to perform the test:

```
(config network interface my_wwan  surelink tests 1)> custom_test_commands "string"
(config network interface my_wwan surelink tests 1)>
```

- **tcp_connection**: Tests that the interface can reach a destination port on the configured host.

  If **tcp_connection** is selected, complete the following:

  - Set the hostname or IP address of the host to create a TCP connection to:

    ```
    (config network interface my_wwan surelink tests 1)> tcp_host hostname/IP_
    address
    (config network interface my_wwan surelink tests 1)>
    ```

  - Set the TCP port to create a TCP connection to.

    ```
    (config network interface my_wwan surelink tests 1)> tcp_port port
    (config network interface my_wwan surelink tests 1)>
    ```

- **other**: Tests the status of another interface.

  If **other** is selected, complete the following:

  - Set the interface to test.
    i. Use the **?** to determine available interfaces:
    ii. Set the interface. For example:

    ```
    (config network interface my_wan surelink tests 1)> other_interface
    /network/interface/eth1
    (config network interface my_wan surelink tests 1)>
    ```

  - Set the type of IP connection:

    ```
    (config network interface my_wwan surelink tests 1)> other_ip_version value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is one of:

    - **any**: Either the IPv4 or IPv6 connection must be up.
    - **both**: Both the IPv4 or IPv6 connection must be up.
    - **ipv4** The IPv4 connection must be up.
    - **ipv6**: The IPv6 connection must be up.

  - The status required for the test to past.

    ```
    (config network interface my_wwan surelink tests 1)> other_status value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is one of:

    - **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

6. Add recovery actions:

a. Type **...** to return to the root of the configuration:

```
(config network interface my_wwan surelink tests 1)> ...
(config)>
```

b. Add a recovery action:

```
(config)> add network interface my_wwan surelink actions end
(config network interface my_wwan surelink actions 0)>
```

c. New actions are enabled by default. To disable:

```
(config network interface my_wwan surelink actions 0)> enable false
(config network interface my_wwan surelink actions 0)>
```

d. Create a label for the action:

```
(config network interface my_wwan surelink actions 0)> label string
(config network interface my_wwan surelink actions 0)>
```

e. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

```
(config network interface my_wwan surelink actions 0)> modem_action value
(config network interface my_wwan surelink actions 0)>
```

where *value* is one of:

- **update_routing_table**: Increases the interface's metric to change the default gateway.

  If **update_routing_table** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config network interface my_wwan surelink actions 0)> test_failures int
    (config network interface my_wwan surelink actions 0)>
    ```

    The default is **3**.

  - Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

    ```
    (config network interface my_wwan surelink actions 0)> metric_adjustment_modem
    int
    (config network interface my_wwan surelink actions 0)>
    ```

    The default is **100**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config network interface my_wwan surelink actions 0)> override_interval int
(config network interface my_wwan surelink actions 0)>
```

- **restart_interface**.

  If **restart_interface** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config network interface my_wwan surelink actions 0)> test_failures int
    (config network interface my_wwan surelink actions 0)>
    ```

    The default is **3**.
  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

    ```
    (config network interface my_wwan surelink actions 0)> override_interval int
    (config network interface my_wwan surelink actions 0)>
    ```

- **reset_modem**.

  If **reset_modem** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config network interface my_wwan surelink actions 0)> test_failures int
    (config network interface my_wwan surelink actions 0)>
    ```

    The default is **3**.
  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

    ```
    (config network interface my_wwan surelink actions 0)> override_interval int
    (config network interface my_wwan surelink actions 0)>
    ```

- **switch_sim**: Switches to an alternate SIM.

  If **switch_sim** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config network interface my_wwan surelink actions 0)> test_failures int
    (config network interface my_wwan surelink actions 0)>
    ```

    The default is **3**.
  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

    ```
    (config network interface my_wwan surelink actions 0)> override_interval int
    (config network interface my_wwan surelink actions 0)>
    ```

- **modem_power_cycle**.

If **modem_power_cycle** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config network interface my_wwan surelink actions 0)> test_failures int
(config network interface my_wwan surelink actions 0)>
```

  The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config network interface my_wwan surelink actions 0)> override_interval int
(config network interface my_wwan surelink actions 0)>
```

- **reboot_device**.

  If **reboot_device** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config network interface my_wwan surelink actions 0)> test_failures int
(config network interface my_wwan surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config network interface my_wwan surelink actions 0)> override_interval int
(config network interface my_wwan surelink actions 0)>
```

- **custom_action**: Execute custom recovery commands.

  If **custom_action** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config network interface my_wwan surelink actions 0)> test_failures int
(config network interface my_wwan surelink actions 0)>
```

    The default is **3**.

  - Set the commands to run to attempt to recovery connectivity.

```
(config network interface my_wwan surelink actions 0)> custom_action_commands_
modem "string"
(config network interface my_wwan surelink actions 0)>
```

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config network interface my_wwan surelink actions 0)> override_interval int
(config network interface my_wwan surelink actions 0)>
```

f. Repeat for each additional recovery action.

7. Optional SureLink configuration parameters:

a. Type **...** to return to the root of the configuration:

```
(config network interface my_wwan surelink actions 0)> ...
(config)>
```

b. Set the test interval between connectivity tests:

```
(config)> network interface my_wwan surelink interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink interval 600s
(config)>
```

The default is **15m**.

c. If more than one test target is configured, set the success condition:

```
(config)> network interface my_wwan surelink success_condition value
(config)>
```

where *value* is either:

- **one**: Only one test needs to pass for Surelink to consider an interface to be up.
- **all**: All tests need to pass for SureLink to consider the interface to be up.

d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

```
(config)> network interface my_wwan surelink pass_threshold int
(config)>
```

The default is **1**.

e. Set the amount of time that the device should wait for a response to a test failure before considering it to have failed:

```
(config)> network interface my_wwan surelink timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink timeout 600s
(config)>
```

The default is **15s**.

f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

```
(config)> network interface my_wwan surelink advanced delayed_start value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **delayed_start** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink advanced delayed_start 600s
(config)>
```

The default is **300s**.

g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

```
(config)> network interface my_wwan surelink advanced backoff_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **backoff_interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink advanced backoff_interval 600s
(config)>
```

The default is 300 seconds.

h. The **interface_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

```
(config)> network interface my_wwan surelink advanced interface_gateway hostname/IP_
address
(config)>
```

8. Save the configuration and apply the change.

```
(config network interface my_wwan ipv4 surelink)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the device to reboot when a failure is detected

Using SureLink, you can configure the IX10 device to reboot when it has determined that an interface has failed.

Required configuration items

- By default, SureLink is enabled for the preconfigured **Modem** interface. The default configuration tests the DNS servers configured for the interface.

  When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the IX10 device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.
- Enable device reboot upon interface failure.
- The type of tests to be performed:
  - **Ping test**: Uses ICMP to determine connectivity. The default behavior is to ping the interface gateway, which means that an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
  - **DNS test**: Performs a DNS query to the named DNS server.
  - **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.
  - **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
  - **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.
  - **Custom test**: Tests the interface with custom commands.
  - **TCP connection test**: Tests that the interface can reach a destination port on the configured host.
  - **Test another interface's status**: Tests the status of another interface.

Additional configuration items

- See Configure SureLink active recovery to detect modem failures for optional SureLink configuration parameters.

To configure the IX10 device to reboot when an interface has failed:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

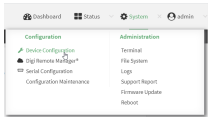
   b. Click the **Device ID**.

   c. Click **Settings**.

   d. Click to expand **Config**.

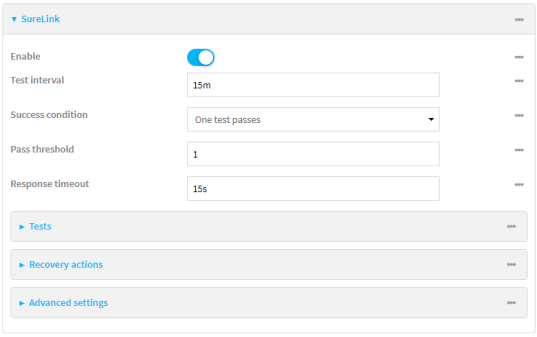
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Create a new interface or select an existing one:
   - To create a new interface, see Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing interface, click to expand the appropriate interface.
5. After creating or selecting the interface, click **SureLink**.



6. (Optional) Change the **Test interval** between connectivity tests.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Interval** to ten minutes, enter **10m** or **600s**.

   The default is 15 minutes.
7. (Optional) If more than one test target is configured, for **Success condition**, select either:
   - **One test passes**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **All test pass**: All tests need to pass for SureLink to consider the interface to be up.
8. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
9. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

   The default is 15 seconds.
10. Click to expand **Tests**.

By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

a. Click .

New tests are enabled by default. To disable, click to toggle off **Enable**.

b. Type a **Label** for the test.

c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.

d. Select the **Test type**.

Available test types:

- **Ping test**: Uses ICMP to determine connectivity.

  If **Ping test** is selected, complete the following:

  - **Ping target:** The type of target for the ping, one of:
    - **Hostname or IP address** of an external server.
      - **Ping host**: hostname or IP address of the server.
    - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - The **Interface address**.
    - The **Interface DNS** server.
  - **Ping payload size:** The number of bytes to send as part of the ping payload.
- **DNS test**: Performs a DNS query to the named DNS server.

  If **DNS test** is selected, complete the following:

  - **DNS server**: The IP address of the DNS server.
- **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **HTTP test** is selected, complete the following:

  - **Web server**: The URL of the web server.
- **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **Test the interface status** is selected, complete the following:

  - **Down time**: The amount of time that the interface is down before the test can be considered to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Down time** to ten minutes, enter **10m** or **600s**.

- **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

  Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

  For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test**: Tests the interface with custom commands.

  If **Custom test** is selected, complete the following:

  - The **Commands to run to test**.

- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

  If **TCP connection test** is selected, complete the following:

  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.

- **Test another interface's status**: Tests the status of another interface.

  If **Test another interface's status** is selected, complete the following:

  - **Test interface**: The interface to test.
  - **IP version**: The type of IP connection, one of:
    - **Any**: Either the IPv4 or IPv6 connection must be up.
    - **Both**: Both the IPv4 or IPv6 connection must be up.
    - **IPv4**: The IPv4 connection must be up.
    - **IPv6**: The IPv6 connection must be up.
  - **Expected status**: The status required for the test to past.
    - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

e. Repeat for each additional test.

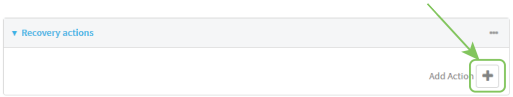
11. Add recovery actions:

a. Click to expand **Recovery actions**.

By default, there are two preconfigured recovery actions:

- **Update routing**: Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
- **Restart interface**.

b. Click



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

c. Type a **Label** for the recovery action.

d. For **Recovery type**, select **Reboot device**.

e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

- **Change default gateway**: Increases the interface's metric to change the default gateway.

  If **Change default gateway** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Increase metric to change active default gateway**: Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Restart interface**.

  If **Restart interface** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Reset modem**: This recovery action is available for WWAN interfaces only.

  If **Reset modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Switch to alternate SIM**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **Switch to alternate SIM** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Reboot device**.

  If **Reboot device** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.

- **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- Execute custom **Recovery commands**.

  If **Recovery commands** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - The **Commands to run to recovery connectivity**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Powercycle the modem**. This recovery action is available for WWAN interfaces only.

  If **Powercycle the modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

f. Repeat for each additional recovery action.

12. (Optional) Configure advanced SureLink parameters:
    a. Click to expand **Advanced settings**.
    b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

       Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

       For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

       The default is 300 seconds.
    c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

       Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

       For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

       The default is 300 seconds.
    d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.
13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new interface, or edit an existing one:
   - To create a new interface, see Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing interface, change to the interface's node in the configuration schema. For example, for a interface named **my_wwan**, change to the **my_wwan** node in the configuration schema:

```
(config)> network interface my_wwan
(config network interface my_wwan)>
```

4. Enable SureLink.

   By default, SureLink is enabled for the preconfigured WWAN (modem).

```
(config network interface my_wwan)> surelink enable true
(config network interface my_wwan)>
```

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

   To add additional tests:

   a. Add a test:

```
(config network interface my_wwan)> add surelink tests end
(config network interface my_wwan surelink tests 1)>
```

   b. New tests are enabled by default. To disable:

```
(config network interface my_wwan surelink tests 1)> enable false
(config network interface my_wwan surelink tests 1)>
```

   c. Create a label for the test:

```
(config network interface my_wwan surelink tests 1)> label string
(config network interface my_wwan surelink tests 1)>
```

   d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config network interface my_wwan surelink tests 1)> ipv6 true
(config network interface my_wwan surelink tests 1)>
```

   e. Set the test type:

```
(config network interface my_wwan surelink tests 1)> test value
(config network interface my_wwan surelink tests 1)>
```

   where *value* is one of:

- **ping**: Uses ICMP to determine connectivity.

  If **ping** is selected, complete the following:

  - Set the **ping_method**:

    ```
    (config network interface my_wwan surelink tests 1)> ping_method value
    (config network interface my_wwan surelink tests 1)>
    ```

    where *value* is one of:

    - **hostname**: The hostname or IP address of an external server.
      - Set **ping_host** to the hostname or IP address of the server:

        ```
        (config network interface my_wwan surelink tests 1)> ping_host hostname/IP_address
        (config network interface my_wwan surelink tests 1)>
        ```

    - **interface_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - **interface_address**.
    - **interface_dns**: The interface's DNS server.

  - Set the number of bytes to send as part of the ping payload:

    ```
    (config network interface my_wwan ipsec tunnel ipsec_example surelink tests 1)> ping_size int
    (config network interface my_wwan surelink tests 1)>
    ```

- **dns**: Performs a DNS query to the named DNS server.

  If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

  ```
  (config network interface my_wwan surelink tests 1)> dns_server IP_address
  (config network interface my_wwan surelink tests 1)>
  ```

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **http** is set, set the URL of the web server.

  ```
  (config network interface my_wwan surelink tests 1)> http url
  (config network interface my_wwan surelink tests 1)>
  ```

- **dns_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **interface_up** is set, complete the following:

  - Set the amount of time that the interface is down before the test can be considered to have failed.

```
(config network interface my_wwan surelink tests 1)> interface_down_time value
(config network interface my_wwan surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wwan surelink tests 1)> interface_down_time 600s
(config)>
```

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

```
(config network interface my_wwan surelink tests 1)> interface_timeout value
(config network interface my_wwan surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wwan surelink tests 1)> interface_timeout 600s
(config)>
```

- **custom_test**: Tests the interface with custom commands.

  If **custom_test** is set, set the commands to run to perform the test:

```
(config network interface my_wwan  surelink tests 1)> custom_test_commands "string"
(config network interface my_wwan surelink tests 1)>
```

- **tcp_connection**: Tests that the interface can reach a destination port on the configured host.

  If **tcp_connection** is selected, complete the following:

  - Set the hostname or IP address of the host to create a TCP connection to:

```
(config network interface my_wwan surelink tests 1)> tcp_host hostname/IP_
address
(config network interface my_wwan surelink tests 1)>
```

  - Set the TCP port to create a TCP connection to.

```
(config network interface my_wwan surelink tests 1)> tcp_port port
(config network interface my_wwan surelink tests 1)>
```

- **other**: Tests the status of another interface.

  If **other** is selected, complete the following:

- Set the interface to test.
  i. Use the **?** to determine available interfaces:
  ii. Set the interface. For example:

```
(config network interface my_wan surelink tests 1)> other_interface
/network/interface/eth1
(config network interface my_wan surelink tests 1)>
```

- Set the type of IP connection:

```
(config network interface my_wwan surelink tests 1)> other_ip_version value
(config network interface my_wwan surelink tests 1)>
```

  where *value* is one of:
  - **any**: Either the IPv4 or IPv6 connection must be up.
  - **both**: Both the IPv4 or IPv6 connection must be up.
  - **ipv4** The IPv4 connection must be up.
  - **ipv6**: The IPv6 connection must be up.
- The status required for the test to past.

```
(config network interface my_wwan surelink tests 1)> other_status value
(config network interface my_wwan surelink tests 1)>
```

  where *value* is one of:
  - **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
  - **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

6. Add recovery actions:
   a. Type **...** to return to the root of the configuration:

```
(config network interface my_wwan surelink tests 1)> ...
(config)>
```

   b. Add a recovery action:

```
(config)> add network interface my_wwan surelink actions end
(config network interface my_wwan surelink actions 0)>
```

   c. New actions are enabled by default. To disable:

```
(config network interface my_wwan surelink actions 0)> enable false
(config network interface my_wwan surelink actions 0)>
```

   d. Create a label for the action:

```
(config network interface my_wwan surelink actions 0)> label string
(config network interface my_wwan surelink actions 0)>
```

e. Set the type of recovery action to **reboot_device**:

```
(config network interface my_wwan surelink actions 0)> action reboot_device
(config network interface my_wwan surelink actions 0)>
```

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config network interface my_wwan surelink actions 0)> test_failures int
(config network interface my_wwan surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config network interface my_wwan surelink actions 0)> override_interval int
(config network interface my_wwan surelink actions 0)>
```

7. Optional SureLink configuration parameters:
   a. Type **...** to return to the root of the configuration:

```
(config network interface my_wwan surelink actions 0)> ...
(config)>
```

   b. Set the test interval between connectivity tests:

```
(config)> network interface my_wwan surelink interval value
(config)>
```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink interval 600s
(config)>
```

   The default is **15m**.

   c. If more than one test target is configured, set the success condition:

```
(config)> network interface my_wwan surelink success_condition value
(config)>
```

   where *value* is either:

   - **one**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **all**: All tests need to pass for SureLink to consider the interface to be up.

   d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

```
(config)> network interface my_wwan surelink pass_threshold int
(config)>
```

   The default is **1**.

e. Set the amount of time that the device should wait for a response to a test failure before considering it to have failed:

```
(config)> network interface my_wwan surelink timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink timeout 600s
(config)>
```

The default is **15s**.

f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

```
(config)> network interface my_wwan surelink advanced delayed_start value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **delayed_start** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink advanced delayed_start 600s
(config)>
```

The default is **300s**.

g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

```
(config)> network interface my_wwan surelink advanced backoff_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **backoff_interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink advanced backoff_interval 600s
(config)>
```

The default is 300 seconds.

h. The **interface_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

```
(config)> network interface my_wwan surelink advanced interface_gateway hostname/IP_
address
(config)>
```

8. Save the configuration and apply the change.

```
(config network interface my_wwan ipv4 surelink)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable SureLink

If your device uses a private APN with no Internet access or has a restricted WAN connection that doesn't allow DNS resolution, you can disable SureLink connectivity tests. You can also reconfigure SureLink to disable the DNS test and use one or more other tests.

Web

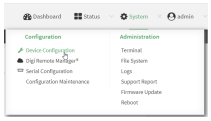
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

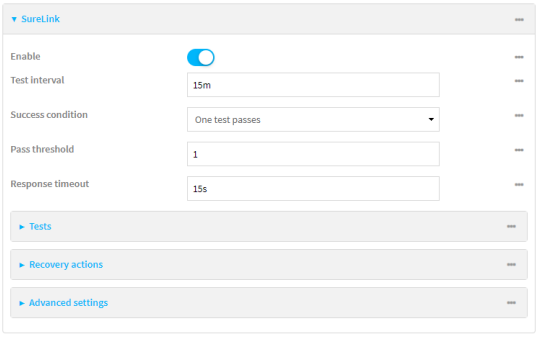
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Select the appropriate WAN or WWAN on which SureLink should be disabled..

5. After selecting the WAN or WWAN, click **SureLink**.



6. Toggle off **Enable** to disable SureLink.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Change to the WAN or WWAN's node in the configuration schema. For example, to disable SureLink for the Modem interface:

```
(config)> network interface modem
(config network interface modem)>
```

4. Disable SureLink:

```
(config network interface modem> surelink enable false
(config network interface modem)>
```

5. Save the configuration and apply the change.

```
(config network interface my_wwan surelink)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable the default DNS test

Alternatively, you can disable the default DNS test for devices that use a private APN with no Internet access, or that have restricted wired WAN connections that do not allow DNS resolution, and configure alternate test.

Web

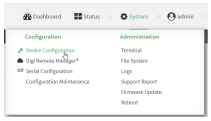
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

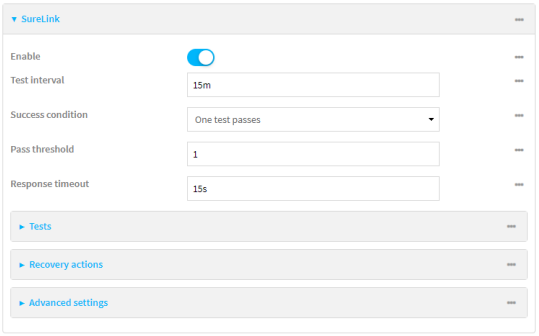
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

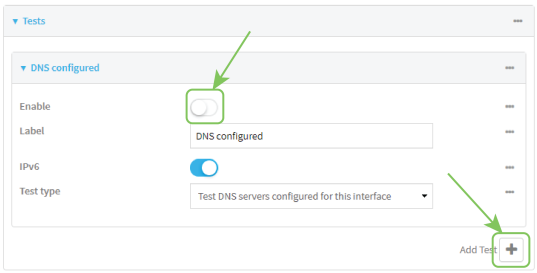
   

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Select the appropriate WAN or WWAN on which the default DNS test should be disabled..
5. After selecting the WAN or WWAN, click **SureLink**.



6. Click to expand **Tests**.
7. Click to expand the default **DNS configured** test.
8. Click to toggle off **Enable**.

9. Click to add a new test.



10. Type a **Label** for the test.
11. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.
12. Select the **Test type**.

    Available test types:

    - **Ping test**: Uses ICMP to determine connectivity.

      If **Ping test** is selected, complete the following:

      - **Ping target:** The type of target for the ping, one of:
        - **Hostname or IP address** of an external server.
          - **Ping host**: hostname or IP address of the server.
        - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
        - The **Interface address**.
        - The **Interface DNS** server.
      - **Ping payload size:** The number of bytes to send as part of the ping payload.
    - **DNS test**: Performs a DNS query to the named DNS server.

      If **DNS test** is selected, complete the following:

      - **DNS server**: The IP address of the DNS server.
    - **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

      If **HTTP test** is selected, complete the following:

      - **Web server**: The URL of the web server.
    - **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
    - **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

      If **Test the interface status** is selected, complete the following:

      - **Down time**: The amount of time that the interface is down before the test can be considered to have failed.

        Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

        For example, to set **Down time** to ten minutes, enter **10m** or **600s**.

- **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

  Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

  For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test**: Tests the interface with custom commands.

  If **Custom test** is selected, complete the following:

  - The **Commands to run to test**.

- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

  If **TCP connection test** is selected, complete the following:

  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.

- **Test another interface's status**: Tests the status of another interface.

  If **Test another interface's status** is selected, complete the following:

  - **Test interface**: The interface to test.
  - **IP version**: The type of IP connection, one of:
    - **Any**: Either the IPv4 or IPv6 connection must be up.
    - **Both**: Both the IPv4 or IPv6 connection must be up.
    - **IPv4**: The IPv4 connection must be up.
    - **IPv6**: The IPv6 connection must be up.
  - **Expected status**: The status required for the test to past.
    - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Change to WAN or WWAN's node in the configuration schema. For example, to disable the default DNS test for an interface named my_wan:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Disable the default DNS test:

```
(config network interface my_wan)> surelink tests 0 enable false
(config network interface my_wan)>
```

5. Add a new test:
   a. Add a test:

```
(config network interface my_wan)> add surelink tests end
(config network interface my_wan surelink tests 1)>
```

   b. Create a label for the test:

```
(config network interface my_wan surelink tests 1)> label string
(config network interface my_wan surelink tests 1)>
```

   c. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config network interface my_wan surelink tests 1)> ipv6 true
(config network interface my_wan surelink tests 1)>
```

   d. Set the test type:

```
(config network interface my_wan surelink tests 1)> test value
(config network interface my_wan surelink tests 1)>
```

   where *value* is one of:

   - **ping**: Uses ICMP to determine connectivity.

     If **ping** is selected, complete the following:

     - Set the **ping_method**:

```
(config network interface my_wan surelink tests 1)> ping_method value
(config network interface my_wan surelink tests 1)>
```

       where *value* is one of:

       - **hostname**: The hostname or IP address of an external server.
         - Set **ping_host** to the hostname or IP address of the server:

```
(config network interface my_wan surelink tests 1)> ping_host hostname/IP_address
(config network interface my_wan surelink tests 1)>
```

       - **interface_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
       - **interface_address**.
       - **interface_dns**: The interface's DNS server.

- Set the number of bytes to send as part of the ping payload:

```
(config network interface my_wan ipsec tunnel ipsec_example surelink tests 1)>
ping_size int
(config network interface my_wan surelink tests 1)>
```

- **dns**: Performs a DNS query to the named DNS server.

  If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

```
(config network interface my_wan surelink tests 1)> dns_server IP_address
(config network interface my_wan surelink tests 1)>
```

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **http** is set, set the URL of the web server.

```
(config network interface my_wan surelink tests 1)> http url
(config network interface my_wan surelink tests 1)>
```

- **dns_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **interface_up** is set, complete the following:

  - Set the amount of time that the interface is down before the test can be considered to have failed.

```
(config network interface my_wan surelink tests 1)> interface_down_time value
(config network interface my_wan surelink tests 1)>
```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

    For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wan surelink tests 1)> interface_down_time 600s
(config)>
```

  - Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

```
(config network interface my_wan surelink tests 1)> interface_timeout value
(config network interface my_wan surelink tests 1)>
```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

    For example, to set **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wan surelink tests 1)> interface_timeout 600s
(config)>
```

- **custom_test**: Tests the interface with custom commands.

  If **custom_test** is set, set the commands to run to perform the test:

  ```
  (config network interface my_wan  surelink tests 1)> custom_test_commands "string"
  (config network interface my_wan surelink tests 1)>
  ```

- **tcp_connection**: Tests that the interface can reach a destination port on the configured host.

  If **tcp_connection** is selected, complete the following:

  - Set the hostname or IP address of the host to create a TCP connection to:

    ```
    (config network interface my_wan surelink tests 1)> tcp_host hostname/IP_address
    (config network interface my_wan surelink tests 1)>
    ```

  - Set the TCP port to create a TCP connection to.

    ```
    (config network interface my_wan surelink tests 1)> tcp_port port
    (config network interface my_wan surelink tests 1)>
    ```

- **other**: Tests the status of another interface.

  If **other** is selected, complete the following:

  - Set the interface to test.
    i. Use the **?** to determine available interfaces:
    ii. Set the interface. For example:

    ```
    (config network interface my_wan surelink tests 1)> other_interface
    /network/interface/eth1
    (config network interface my_wan surelink tests 1)>
    ```

  - Set the type of IP connection:

    ```
    (config network interface my_wan surelink tests 1)> other_ip_version value
    (config network interface my_wan surelink tests 1)>
    ```

    where *value* is one of:

    - **any**: Either the IPv4 or IPv6 connection must be up.
    - **both**: Both the IPv4 or IPv6 connection must be up.
    - **ipv4** The IPv4 connection must be up.
    - **ipv6**: The IPv6 connection must be up.

  - The status required for the test to past.

    ```
    (config network interface my_wan surelink tests 1)> other_status value
    (config network interface my_wan surelink tests 1)>
    ```

    where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

6. Save the configuration and apply the change.

```
(config network interface my_wan ipv4 surelink)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Using cellular modems in a Wireless WAN (WWAN)

The IX10 supports one cellular modem, named **Modem**, which is included in a preconfigured Wireless WAN, also named **Modem**.

The cellular modem can have only one active SIM slot at any one time. For example, **Modem** can have either SIM1 or SIM2 up at one time.

Typically, you configure SIM1 of the cellular modem as the primary cellular interface, and SIM2 as the backup cellular interface. In this way, if the IX10 device cannot connect to the network using SIM1, it automatically fails over to SIM2. IX10 devices automatically use the correct cellular module firmware for each carrier when switching SIMs.

Configure cellular modem

To configure your IX10's cellular modem, you need to modify the network and SIM settings.

Required configuration items

- Enable the cellular modem.

  The cellular modem is enabled by default.
- Configure the criteria used to determine which modem this modem configuration applies to.
- Determine the SIM slot that will be used when connecting to the cellular network.
- Configure the maximum number of interfaces that can use the modem.
- Enable carrier switching, which allows the modem to automatically match the carrier for the active SIM.

  Carrier switching is enabled by default.
- Configure the access technology.
- Determine which cellular antennas to use.

Additional configuration items

- If **Active SIM slot** is set to **Any**, by default the device uses the SIM slot that was last used or was operational. As an alternative, you can specify a preferred SIM slot.

  In the event of a failover to a non-preferred SIM, or if manual SIM switching is used to switch to a non-preferred SIM, the modem will attempt to reconnect to the SIM in the preferred SIM slot.

To configure the modem:

Web

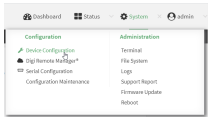
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

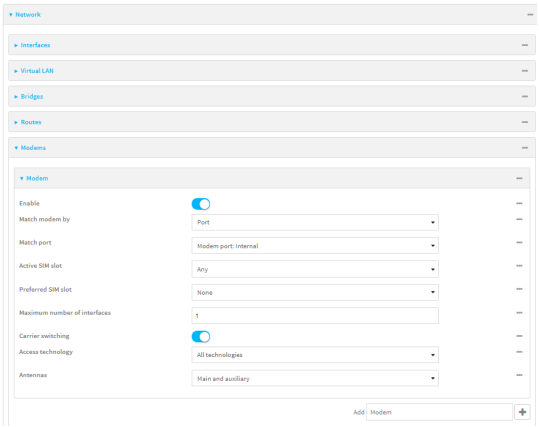
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. For single-cellular models, click **Network** > **Modems** > **WWAN cellular modem** or **Modem**.
4. Click **Network** > **Modems** > **Modem**.



5. Modem configurations are enabled by default. Click to toggle **Enable** to off to disable.
6. For **Match modem by**, select the matching criteria used to determine if this modem configuration applies to the currently attached modem:
   - **Any modem**: Applies this configuration to any modem that is attached.
   - **IMEI**: Applies this configuration only to a modem that matches the identified IMEI.
     - If **IMEI** is selected, for **Match IMEI**, type the IMEI of the modem that this configuration should be applied to.

- **Port**: Applies this configuration to a modem attached to the identified physical port.
  - If **Port** is selected, for **Match Port**, select the modem's port.

The default is **Any modem**.

7. The **Active SIM slot** selection is used to determine which SIM slot the modem will attempt to connect with. For **Active SIM slot**, select one of the following options:
   - **Any**: Use the SIM slot that was last used or was last operational. The default is **Any**.
   - **SIM1**: Only use SIM slot 1 with the modem
   - **SIM2**: Only use SIM slot 2 with the modem
8. If you set the **Active SIM slot** to **Any**, the **Preferred SIM slot** option displays. Options for **Preferred SIM slot** are:
   - **None**: The modem attempts to connect to the SIM in the SIM slot that was last used or was last operational. **None** is the default.
   - **SIM slot**: Select the SIM slot that should be considered the preferred slot for this modem. If a preferred SIM is configured, the **Preferred SIM slot check schedule** displays in the configuration settings. In the event of a SIM failover, or if manual SIM switching is used to switch SIM slots, the modem attempts to reconnect to the preferred SIM at the interval or schedule configured in the **Preferred SIM slot check schedule** settings. If a **Preferred SIM slot** is selected, you can choose the type of schedule:
     - **On boot** - Runs task when device starts.
     - **Interval** - Runs task once per hour.
     - **Set time** - Runs task at a set time.
     - **During system maintenance window** - Runs task only during the period of time designated for system maintenance.
     - **Manual** - Task is not performed automatically.
     - **After** - Task runs for a fixed time interval on a different SIM and then goes back to the preferred SIM.
9. For **Maximum number of interfaces**, type the number of interfaces that can be configured to use this modem. This is used when using dual-APN SIMs. The default is **1**.
10. For **Signal strength query interval**, type or select the amount of time the system waits before polling the modem for signal information.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Signal strength query interval** to ten minutes, enter **10m** or **600s**.

    The default is **10s**.
11. Enable **Carrier switching** to allow the modem to automatically match the carrier for the active SIM. **Carrier switching** is enabled by default.
12. For **Access technology**, select the type of cellular technology that this modem should use to access the cellular network, or select **All technologies** to configure the modem to use the best available technology. The default is **All technologies**.
13. For **Antennas**, select whether the modem should use the main antenna, the auxiliary antenna, or both the main and auxiliary antennas.

Note For **4G bands**, specify the frequency bands you want to include or exclude. By default, all bands are used. To only use certain bands, separate each band in the list with a space (for example, *B1 B3 B5*). To exclude certain bands, separate each band in the list with a space and precede each band with an exclamation point (for example, *!B1 !B5*).

CAUTION! Make sure to confirm with your service provider that the bands you want to include or exclude are accurate. Connection issues may occur if a service provider changed any of the frequency bands they use for their network and you have set limitations on the bands to which the IX10 can connect.

14. (Optional) For **4G bands**, specify the 4G bands.
15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Modem configurations are enabled by default. To disable:

```
(config)> network modem modem enable false
(config)>
```

4. Set the matching criteria used to determine if this modem configuration applies to the currently attached modem:

```
(config)> network modem modem match value
(config)>
```

   where *value* is one of the following:

   - **any**: Applies this configuration to any modem that is attached.
   - **imei**: Applies this configuration only to a modem that matches the identified IMEI.
     - If **imei** is used, set the IMEI of the modem that this configuration should be applied to:

```
(config)> network modem modem imei value
(config)>
```

       where *value* is the IMEI of the modem.

- **port**: Applies this configuration to a modem attached to the identified physical port.
  - If **port** is used, set modem's port:
    a. Determine available ports and correct syntax by using the **?**:

```
(config)> network modem modem port ?

Match port: The physical port that the modem device is attached to.
Format:
  /device/usb/modem/module
Default value: /device/usb/modem/module
Current value: /device/usb/modem/module

(config)> network modem modem port
```

    b. Set the port:

```
(config)> network modem modem port /device/usb/modem/module
(config)>
```

  The default is **any**.

5. Set the SIM slot that should be used by the modem:

```
(config)> network modem modem sim_slot value
(config)>
```

   where *value* is one of the following:
   - **any**: Uses either SIM slot.
   - **1**: Uses the first SIM slot.
   - **2**. Uses the second SIM slot.

   The default is **any**.

6. If **sim_slot** is set to **any**, set the SIM slot that should be considered the preferred slot for this modem:

```
(config)> network modem modem sim_slot_preference value
(config)>
```

   where *value* is one of the following:
   - **none**: Does not consider either SIM slot to be the preferred slot.
   - **1**: Configures the first SIM slot as the preferred SIM slot.
   - **2**. Configures the second SIM slot as the preferred SIM slot.

   In the event of a failover to a non-preferred SIM, or if manual SIM switching is used to switch to a non-preferred SIM, the modem will attempt to reconnect to the SIM in the preferred SIM slot. The default is **none**.

7. To set the preferred SIM slot check schedule:

```
(config)> network modem modem sim_slot_preference_value
```

where *value* is one of the following:

- **1**: SIM slot 1.
- **2**. SIM slot 2.

```
(config)> ...run-time when value
```

where *value* is one of the following:

- after
- boot
- interval
- maintenance_window
- manual
- set_time

The default is **set_time**.

8. Set the amount of time the system waits before polling the modem for signal information:

```
(config)> network modem modem query_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **query_interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network modem wan query_interval  600s
(config)>
```

The default is **10s**.

9. Set the maximum number of interfaces. This is used when using dual-APN SIMs. The default is **1**.

```
(config)> network modem modem max_intfs int
(config)>
```

10. Carrier switching allows the modem to automatically match the carrier for the active SIM. Carrier switching is enabled by default. To disable:

```
(config)> network modem modem carrier_switch false
(config)>
```

11. Set the type of cellular technology that this modem should use to access the cellular network:

```
(config)> network modem modem access_tech value
(config)>
```

Available options for *value* vary depending on the modem type. To determine available options:

```
(config)> network modem modem access_tech ?

Access technology: The cellular network technology that the modem may use.
Format:
  2G
  3G
  4G
  4GM
  4GT
  all
Default value: all
Current value: all

(config)>
```

The default is **all**, which uses the best available technology.

12. Set whether the modem should use the main antenna, the auxiliary antenna, or both the main and auxiliary antennas:

```
(config)> network modem modem antenna value
(config)>
```

where *value* is one of the following:

- **main**
- **aux**
- **both**

13. (Optional) To specify the 4G bands you want to include or exclude:

```
(config)> network modem modem 4g_bands
(config)>
```

14. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

15. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Cellular modem APNs

The IX10 device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. You can find the `serviceproviders-local.txt` and `serviceproviders.txt` files in the filesystem of the IX10. The order of the APNs for a specific carrier in these text files corresponds to the order in which the IX10 will try those APNS until it makes a successful connection. After the device has successfully connected, it will remember the correct APN. As a result, it is not necessary to configure APNs. However, you can configure the system to use a specified APN if you choose to do so.

Configure cellular modem APNs

To configure the APN:

Web

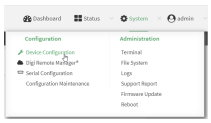
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

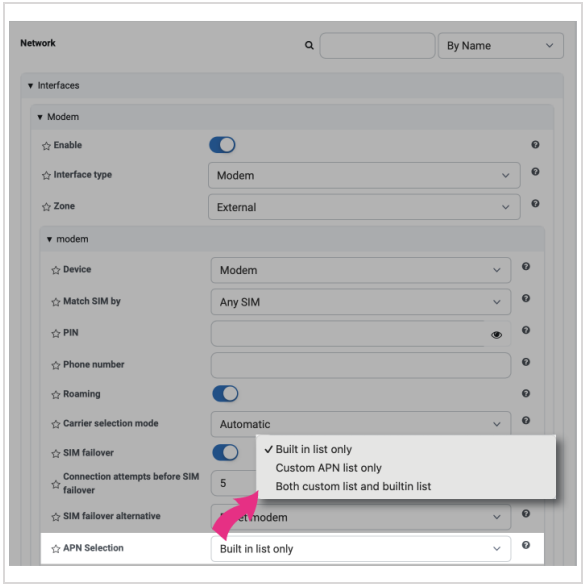
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. For your single-cellular IX10, click **Network** > **Interfaces** > **Modem** > **modem** > **APN Selection**.

4. For **APN Selection**, select whether you want your IX10 to use the preconfigured APNs, custom APNs, or both.

a. If you selected either the *Custom APN list only* or the *Both custom list and builtin list*, click to add an APN.
b. (Optional) For **APN**, add a name.
c. (Optional) For **IP version**, select one of the following settings:
   - **Automatic**: Requests both IPv4 and IPv6 address.
   - **IPv4**: Requests only an IPv4 address.
   - **IPv6**: Requests only an IPv6 address.

   The default is **Automatic**.
d. (Optional) For **Authentication method**, select one of the following settings:
   - **None**: No authentication is required.
   - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
   - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
   - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

   If **Automatic**, **CHAP**, or **PAP** is selected, enter the **Username** and **Password** required to authenticate.

   The default is **None**.
e. (Optional)For **PDP context index**, type the number for the index of the SIM card that the APN is programmed into. The default is **0** so the index is set automatically.
f. **Lightweight M2M support** is enabled by default. Disable if you are using an AT&T SIM that does not support AT&T lightweight M2M.
g. Repeat these steps to add additional APNs, if needed.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> network interface modem modem apn 0 apn value
(config)>
```

   where *value* is the APN for the SIM card.

4. (Optional) To add additional APNs:
   a. Use the **add** command to add a new APN entry. For example:

```
(config)> add network interface modem modem apn end
(config network interface modem modem apn 1)>
```

   b. Set the value of the APN:

```
(config network interface modem modem apn 1)> apn value
(config network interface modem modem apn 1)>
```

   where value is the APN for the SIM card.
5. (Optional) Set the IP version:

```
(config)> network interface modem modem apn 0 ip_version version
(config)>
```

   where *version* is one of the following:
   - **auto**: Requests both IPv4 and IPv6 address.
   - **ipv4**: Requests only an IPv4 address.
   - **ipv6**: Requests only an IPv6 address.

   The default is **auto**.
6. (Optional) Set the PDP context index:

```
(config network interface wwan1 modem apn 0) > cid value
(config network interface wwan1 modem apn 0) >
```

   where *value* is the index number of the SIM that the APN is programmed into. *0* means the index will be automatically set.
7. (Optional) Set the authentication method:

```
(config)> network interface modem modem apn 0 auth method
(config)>
```

   where *method* is one of the following:
   - **none**: No authentication is required.
   - **auto**: The device will attempt to connect using CHAP first, and then PAP.
   - **chap**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
   - **pap**: Uses the Password Authentication Profile (PAP) to authenticate.

   If **auto**, **chap**, or **pap** is selected, enter the **Username** and **Password** required to authenticate:

```
(config)> network interface modem modem apn 0 username name
(config)> network interface modem modem apn 0 password pwd
(config)>
```

   The default is **none**.
8. Disable Lightweight M2M support if you are using an AT&T SIM that does not support AT&T lightweight M2M:

```
(config)> network interface modem modem apn 0 attm2mglobal false
(config)>
```

9. (Optional) To configure the device to use either the preconfigured APNs, custom APNs, or both:

```
(config)> network interface modem modem apn_selection value
(config)>
```

Where *value* is one of the following:

- apn_list_only
- both_lists
- built-in-list-only

10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show cellular status and statistics

You can view a summary status for all cellular modems, or view detailed status and statistics for a specific modem.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **Status**.
2. Under **Connections**, click **Modems**.

The modem status window is displayed

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show modem command:
   - To view a status summary for the modem:

```
> show modem

Modem  SIM          Status     APN       Signal Strength
-----  ------------ ---------- --------- ---------------------
modem  1 (ready)    connected  1234      Good (-84 dBm)
```

```
>
```

- To view detailed status and statistics, use the show modem name *name* command:

```
> show modem name modem

 modem: [Telit] LM940
 ------------------------------------------------------------------------------
 IMEI              : 781154796325698
 Model             : LM940
 FW Version        : 24.01.541_ATT
 Revision          : 24.01.541

 Status
 ------
 State             : connected
 Signal Strength   : Good (-85 dBm)
 Bars              : 2/5
 Access Mode       : 4G
 Network Technology (CNTI): LTE
 Band              : B2
 Temperature       : 34C

 wwan1 Interface
 ---------------
 APN               : 1234
 IPv4 surelink     : passing
 IPv4 address      : 189.232.229.47
 IPv4 gateway      : 189.232.229.1
 IPv4 MTU          : 1500
 IPv4 DNS server(s)  : 245.144.162.207, 245.144.162.208

 IPv6 surelink     : passing
 IPv6 address      : 11f6:4680:0d67:59d2:552b:3429:81a8:f1ea
 IPv6 gateway      : ff50:d95d:7e98:abe8:3030:9138:4f25:f51b
 IPv6 MTU          : 1500

 TX bytes          : 127941
 RX bytes          : 61026
 Uptime            : 10 hrs, 56 mins (39360s)

 SIM
 ---
 SIM Slot          : 1
 SIM Status        : ready
 IMSI              : 61582122197895
 ICCID             : 26587628655003992180
 SIM Provider      : AT&T

 4G
```

```
--
RSRQ          : Good (-11.0 dB)
RSRP          : Good (-93.0 dBm)
RSSI          : Excellent (-64.0 dBm)
SNR           : Good (6.4 dB)

>
```

Unlock a SIM card

A SIM card can be locked if a user tries to set an invalid PIN for the SIM card too many times. In addition, some cellular carriers require a SIM PIN to be added before the SIM card can be used. If the SIM card is locked, the IX10 device cannot make a cellular connection.

Command line

To unlock a SIM card:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, use the modem puk unlock command to set a new PIN for the SIM card:

   ```
   > modem puk unlock puk_code new_pin modem_name
   >
   ```

   For example, to unlock a SIM card in the modem named **modem** with PUK code **12345678**, and set the new SIM PIN to **1234**:

   ```
   > modem puk unlock 12345678 1234 modem
   >
   ```
3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Note If the SIM remains in a locked state after using the unlock command, contact your cellular carrier.

Signal strength for 4G cellular connections

For 4G connections, the **RSRP** value determines signal strength.

- **Excellent**: > **-90 dBm**
- **Good**: **-90 dBm** to **-105 dBm**
- **Fair**: **-106 dBm** to **-115 dBm**
- **Poor**: **-116 dBm** to **-120 dBm**:
- **No service**: **< -120 dBm**

See Show cellular status and statistics for procedures to view this information.

Signal strength for 3G and 2G cellular connections

For 3G and 2G cellular connections, the current **RSSI** value determines signal strength.

- **Excellent**: > **-70 dBm**
- **Good**: **-70 dBm** to **-85 dBm**
- **Fair**: **-86 dBm** to **-100 dBm**
- **Poor**: **< -100 dBm** to **-109 dBm**
- **No service**: **-110 dBm**

See Show cellular status and statistics for procedures to view this information.

Tips for improving cellular signal strength

If the signal strength LEDs or the signal quality for your device indicate **Poor** or **No service**, try the following things to improve signal strength:

- Move the IX10 device to another location.
- Try connecting a different set of antennas, if available.
- Purchase a Digi Antenna Extender Kit:
  - Antenna Extender Kit, 1m

AT command access

To run AT commands from the IX10 command line:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **modem at-interactive** and press **Enter**. Type **n** if you do not want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the cellular network.
3. At the Admin CLI prompt, use the modem at-interactive command to begin an interactive AT command session:

```
> modem at-interactive


Do you want exclusive access to the modem?  (y/n) [y]:
```

4. Type **n** if you do not want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the cellular network.

   The following is an example interactive AT command:

```
> modem at-interactive
```

```
Do you want exclusive access to the modem? (y/n) [y]: n
Starting terminal access to modem AT commands.
Note that the modem is still in operation.

To quit enter '~.' ('~~.' if using an ssh client) and press ENTER

Connected
ati
Manufacturer: Sierra Wireless, Incorporated
Model: MC7455
Revision: SWI9X30C_02.24.03.00 r6978 CARMD-EV-FRMWR2 2017/03/02 13:36:45
MEID: 35907206045169
IMEI: 359072060451693
IMEI SV: 9
FSN: LQ650551070110
+GCAP: +CGSM
OK
```

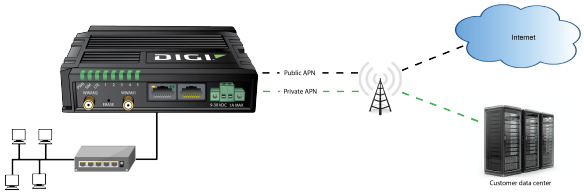
5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure dual APNs

Some cellular carriers offer a dual APN feature that allows a SIM card to be provisioned with two separate APNs that can be used simultaneously. For example, Verizon offers this service as its Split Data Routing feature. This feature provides two separate networking paths through a single cellular modem and SIM card, and allows for configurations such as:

- Segregating public and private traffic, including policy-based routes to ensure that your internal network traffic always goes through the private connection.
- Separation of untrusted Internet traffic from trusted internal network traffic.
- Secure connection to internal customer network without using a VPN.
- Separate billing structures for public and private traffic.
- Site-to-site networking, without the overhead of tunneling for each device.



To accomplish this, we will create separate WWAN interfaces that use the same modem but use different APNs, and then use routing roles to forward traffic to the appropriate WWAN interface.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

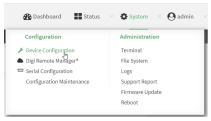
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

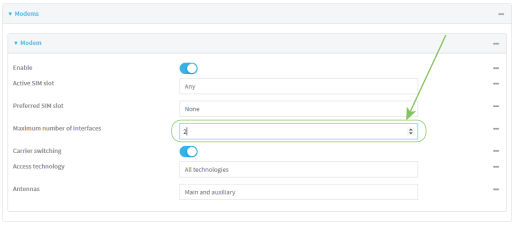
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

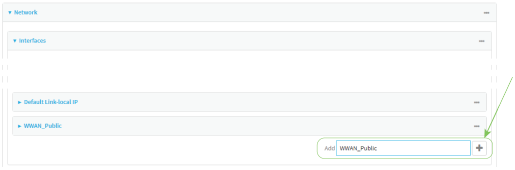
   

   The **Configuration** window is displayed.

3. Increase the maximum number of interfaces allowed for the modem:
   a. Click **Network** > **Modems** > **Modem**.
   b. For **Maximum number of interfaces**, type **2**.

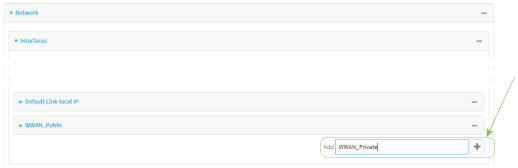
   

4. Create the WWAN interfaces:
   In this example, we will create two interfaces named **WWAN_Public** and **WWAN_Private**.
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface**, type **WWAN_Public** and click .

   c. For **Interface type**, select **Modem**.
   d. For **Zone**, select **External**.
   e. For **Device**, select **Modem** .
   f. (Optional) For **APN selection**, select whether you want to configure the device to use the preconfigured APNs, custom APNs, or both.

g. For **Add Interface**, type **WWAN_Private** and click .



h. For **Interface type**, select **Modem**.

i. For **Zone**, select **External**.

j. For **Device**, select **Modem** .

This should be the same modem selected for the **WWAN_Public** WWAN.

k. For **APN selection**, select whether you want to configure the device to use the preconfigured APNs, custom APNs, or both.

5. Create the routing policies. For example, to route all traffic from a device with the IP address of 192.168.2.101 through the private APN:

a. Click **Network** > **Routes** > **Policy-based routing**.

b. Click the to add a new route policy.

c. For **Label**, enter **Route through private APN**.

d. For **Interface**, select **Interface: WWAN_Private**.

e. Configure the source address:

i. Click to expand **Source address**.

ii. For **Type**, select **IPv4 address**.

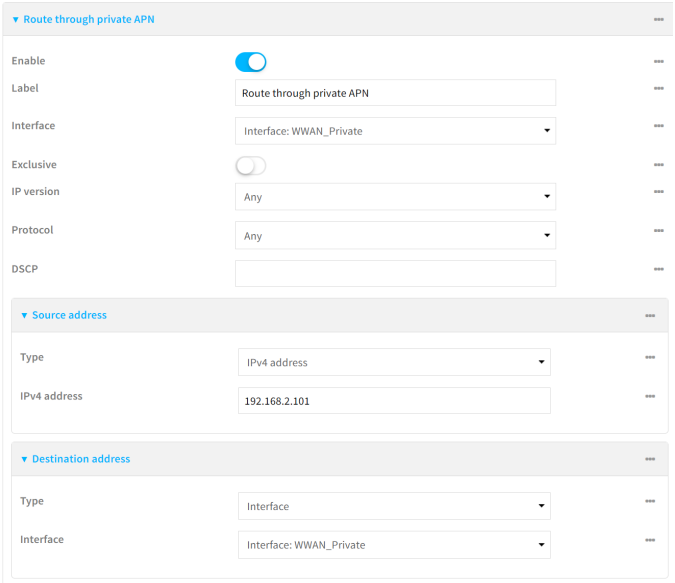
iii. For **Address**, type **192.168.2.101**.

f. Configure the destination address:

i. Click to expand **Destination address**.

ii. For **Type**, select **Interface**.

iii. For **Interface**, select **Interface: WWAN_Private**.



6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set the maximum number of interfaces for the modem:

```
(config)> network modem modem max_intfs 2
(config)>
```

4. Create the WWAN interfaces:
   a. Create the **WWANPublic** interface:

```
(config)> add network interface WWANPublic
(config network interface WWANPublic)>
```

   b. Set the interface type to modem:

```
(config network interface WWANPublic)> type modem
(config network interface WWANPublic)>
```

   c. Set the modem device:

```
(config network interface WWANPublic)> modem device modem
(config network interface WWANPublic)>
```

d. Configure whether you want the device to use the preconfigured APNs, custom APNs, or both. For more information, see Cellular modem APNs.

```
(config network interface WWANPublic)> modem apn public_apn
(config network interface WWANPublic)>
```

e. Use to periods (**..**) to move back one level in the configuration:

```
(config network interface WWANPublic)> ..
(config network interface)>
```

f. Create the **WWANPrivate** interface:

```
(config network interface)> add WWANPrivate
(config network interface WWANPrivate)>
```

g. Set the interface type to modem:

```
(config network interface WWANPrivate)> type modem
(config network interface WWANPrivate)>
```

h. Set the modem device:

```
(config network interface WWANPrivate)> modem device modem
(config network interface WWANPrivate)>
```

i. Enable **APN list only**:

```
(config network interface WWANPrivate)> modem apn_selection apn_list_only
(config network interface WWANPrivate)>
```

j. Set the private APN:

```
(config network interface WWANPublic)> modem apn private_apn
(config network interface WWANPublic)>
```

5. Create the routing policies. For example, to route all traffic from a device with the IP address of 192.168.2.101 through the private APN:
   a. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

   b. Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "Route through private apn"
(config network route policy 0)>
```

c. Set the interface:

```
(config network route policy 0)> interface /network/interface/WWANPrivate
(config network route policy 0)>
```

d. Configure the source address:

i. Set the source type to **address**:

```
(config network route policy 0)> src type address
(config network route policy 0)>
```

ii. Set the IP address to **192.168.2.101**:

```
(config network route policy 0)> src address 192.168.2.101
(config network route policy 0)>
```

e. Configure the destination address:

i. Set the type to **interface**:

```
(config network route policy 1)> dst type interface
(config network route policy 1)>
```

ii. Set the interface to **WWANPrivate** :

```
(config network route policy 1)> interface /network/interface/WWANPrivate
(config network route policy 1)>
```

6. Save the configuration and apply the change.

```
(config network route policy 1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure a Wireless Wide Area Network (WWAN)

Configuring a Wireless Wide Area Network (WWAN) involves configuring the following items:

Required configuration items

- The interface type: **Modem**.
- The firewall zone: **External**.
- The cellular modem that is used by the WWAN.

Additional configuration items

- SIM selection for this WWAN.
- The SIM PIN.
- The SIM phone number for SMS connections.

- Enable or disable roaming.
- SIM failover configuration.
- APN configuration.
- The custom gateway/netmask.
- IPv4 configuration:
  - The type being the way to control how the modem in the Digi device obtains an IP address from the cellular network.
  - The metric for IPv4 routes associated with the WAN.
  - The relative weight for IPv4 routes associated with the WAN.
  - The IPv4 management priority of the WAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
  - The IPv4 Maximum Transmission Unit (MTU) of the WAN.
  - Whether to assign a static IPv4 address to the WAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect modem failures for further information.
- IPv6 configuration:
  - The type being the way to control how the modem in the Digi device obtains an IP address from the cellular network.
  - The metric for IPv6 routes associated with the WAN.
  - The relative weight for IPv6 routes associated with the WAN.
  - The IPv6 management priority of the WAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
  - The IPv6 Maximum Transmission Unit (MTU) of the WAN.
  - Whether to assign a static IPv6 address to the WAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect modem failures for further information.

Web

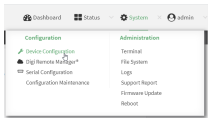
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

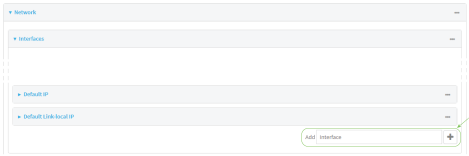
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

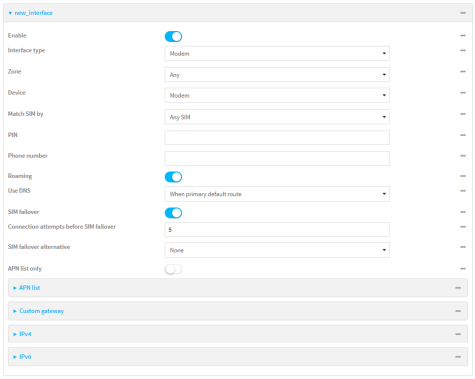


The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Create the WWAN or select an existing WWAN:
   - To create a new WWAN:
     a. For **Add interface**, type a name for the WWAN and click **Add**.



     b. For **Interface type**, select **Modem**.



     New WWANs are enabled by default. To disable, toggle off **Enable**.
   - To edit an existing WWAN, click to expand the WWAN.
5. For **Zone**, select **External**.
6. For **Device**, select the cellular modem.
7. For **Match SIM by**, select a SIM matching criteria to determine when this WWAN should be used:
   - If **SIM slot** is selected, for **Match SIM slot**, select which SIM slot must be in active for this WWAN to be used.
   - If **Carrier** is selected, for **Match SIM carrier**, select which cellular carrier must be in active for this WWAN to be used.
   - If **PLMN identifier** is selected, for **Match PLMN identifier**, type the PLMN id that must be in active for this WWAN to be used.

- If **IMSI** is selected, for **Match IMSI**, type the International Mobile Subscriber Identity (IMSI) that must be in active for this WWAN to be used.
- If **ICCID** is selected, for **Match ICCID**, type the unique SIM card ICCID that must be in active for this WWAN to be used.

8. Type the **PIN** for the SIM. Leave blank if no PIN is required.
9. Type the **Phone number** for the SIM, for SMS connections.

   Normally, this should be left blank. It is only necessary to complete this field if the SIM does not have a phone number or if the phone number is incorrect.
10. **Roaming** is enabled by default. Click to disable.
11. For **Carrier selection mode**, select one of the following:
    - **Automatic**: The cellular carrier is selected automatically by the device.
    - **Manual**: The cellular carrier must be manually configured. If the configured network is not available, no cellular connection will be established.
    - **Manual/Automatic**: The carrier is manually configured. If the configured network is not available, automatic carrier selection is used.

    If **Manual** or **Manual/Automatic** is selected:

    a. For **Network PLMN ID**, type the PLMN ID for the cellular network.

    b. For **Network technology**, select the technology that should be used. The default is **All technologies**, which means that the best available technology will be used.

    > Note If **Manual** is configured for **Carrier selection mode** and a specific network technology is selected for the **Network technology**, your modem must support the selected technology or no cellular connection will be established. If you are using a cellular connection to perform this procedure, you may lose your connection and the device will no longer be accessible.

12. **SIM failover** is enabled by default, which means that the modem will automatically fail over from the active SIM to the next available SIM when the active SIM fails to connect. If enabled:

    a. For **Connection attempts before SIM failover**, type the number of times that the device should attempt to connect to the active SIM before failing over to the next available SIM.

    b. For **SIM failover alternative**, configure how SIM failover will function if automatic SIM switching is unavailable:
       - **None**: The device will perform no alternative action if automatic SIM switching is unavailable.
       - **Reset modem**: The device will reset the modem if automatic SIM switching is unavailable.
       - **Reboot device**: The device will reboot if automatic SIM switching is unavailable.
13. For **APN Selection**, select whether you want to configure the IX10 to use the preconfigured APNs, custom APNs, or both. See Cellular modem APNs for information and instructions for setting an APN.
14. (Optional) To configure the IP address of a custom gateway or a custom netmask:

    a. Click **Custom gateway** to expand.

    b. Click **Enable**.

c. For **Gateway/Netmask**, enter the IP address and netmask of the custom gateway. To override only the gateway netmask, but not the gateway IP address, use all zeros for the IP address. For example, **0.0.0.0./32** will use the network-provided gateway, but with a /32 netmask.

15. Optional IPv4 configuration items:
    a. Click **IPv4** to expand.
    b. IPv4 support is **Enabled** by default. Click to disable.
    c. Set the **Type**.
    - Static IP address - Digi device obtains the static IP address from the cellular network.
    - DHCP address - Digi device obtains IP address through a DHCP server on the cellular network.

    a. Set the **MTU**.
    b. For **Use DNS**:
    - **Always**: DNS will always be used for this WWAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
    - **When primary default route**: Only use the DNS servers provided for this WWAN when the WWAN is the primary route.
    - **Never**: Never use DNS servers for this WWAN.

    The default setting is **When primary default route**.
16. Optional IPv6 configuration items:
    a. Click **IPv6** to expand.
    b. IPv6 support is **Enabled** by default. Click to disable.
    c. Set the **Type**.
    - Static IP address - Digi device obtains the static IP address from the cellular network.
    - DHCP address - Digi device obtains IP address through a DHCP server on the cellular network.

    a. Set the **MTU**.
    b. For **Use DNS**:
    - **Always**: DNS will always be used for this WWAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
    - **When primary default route**: Only use the DNS servers provided for this WWAN when the WWAN is the primary route.
    - **Never**: Never use DNS servers for this WWAN.

    The default setting is **When primary default route**.
1. See Configure SureLink active recovery to detect modem failures for information about configuring **SureLink**.
17. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new WWAN or edit an existing one:
   - To create a new WWAN named **my_wwan**:

```
(config)> add network interface my_wwan
(config network interface my_wwan)>
```

   - To edit an existing WWAN named **my_wwan**, change to the my_wwan node in the configuration schema:

```
(config)> network interface my_wwan
(config network interface my_wwan)>
```

4. Set the appropriate firewall zone:

```
(config network interface my_wwan)> zone zone
(config network interface my_wwan)>
```

   See Firewall configuration for further information.

5. Select a cellular modem:
   a. Enter **modem device ?** to view available modems and the proper syntax.

```
(config network interface my_wwan)> modem device ?

Device: The modem used by this network interface.
Format:
  modem
Current value:

(config network interface my_wwan)> device
```

   b. Set the device:

```
(config network interface my_wwan)> modem device modem
(config network interface my_wwan)>
```

6. Set the SIM matching criteria to determine when this WWAN should be used:

```
(config network interface my_wwan)> modem match value
(config network interface my_wwan)>
```

   Where *value* is one of:

- **any**
- **carrier**

  Set the cellular carrier must be in active for this WWAN to be used:

  a. Use **?** to determine available carriers:

```
(config network interface my_wwan)> modem carrier

Match SIM carrier: The SIM carrier match criteria. This interface is applied when the SIM
card is
provisioned from the carrier.
Format:
  AT&T
  Rogers
  Sprint
  T-Mobile
  Telstra
  Verizon
  Vodafone
  other
Default value: AT&T
Current value: AT&T

(config network interface my_wwan)>
```

  b. Set the carrier:

```
(config network interface my_wwan)> modem carrier value
(config network interface my_wwan)>
```

- **iccid**

  Set the unique SIM card ICCID that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem iccid ICCID
(config network interface my_wwan)>
```

- **imsi**

  Set the International Mobile Subscriber Identity (IMSI) that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem imsi IMSI
(config network interface my_wwan)>
```

- **plmn_id**

  Set the PLMN id that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem plmn_id PLMN_ID
(config network interface my_wwan)>
```

- **sim_slot**

  Set which SIM slot must be in active for this WWAN to be used:

  ```
  (config network interface my_wwan)> modem sim_slot value
  (config network interface my_wwan)>
  ```

  where *value* is either **1** or **2**.

7. Set the PIN for the SIM. Leave blank if no PIN is required.

   ```
   (config network interface my_wwan)> modem pin value
   (config network interface my_wwan)>
   ```

8. Set the phone number for the SIM, for SMS connections:

   ```
   (config network interface my_wwan)> modem phone num
   (config network interface my_wwan)>
   ```

   Normally, this should be left blank. It is only necessary to complete this field if the SIM does not have a phone number or if the phone number is incorrect.

9. Roaming is enabled by default. To disable:

   ```
   (config network interface my_wwan)> modem roaming false
   (config network interface my_wwan)>
   ```

10. Set the carrier selection mode:

    ```
    (config network interface my_wwan)> modem operator_mode value
    (config network interface my_wwan)>
    ```

    where *value* is one of:

    - **automatic**: The cellular carrier is selected automatically by the device.
    - **manual**: The cellular carrier must be manually configured. If the configured network is not available, no cellular connection will be established.
    - **manual_automatic**: The carrier is manually configured. If the configured network is not available, automatic carrier selection is used.

    If **manual** or **manual_automatic** is set:

    a. Set the Network PLMN ID:

       ```
       (config network interface my_wwan)> modem operator PLMN_ID
       (config network interface my_wwan)>
       ```

    b. Set the cellular network technology:

       ```
       (config network interface my_wwan)> modem operator_technology value
       (config network interface my_wwan)>
       ```

       where *value* is one of:

       - **all**: The best available technology will be used.
       - **2G**: Only 2G technology will be used.
       - **3G**: Only 3G technology will be used.

- **4G**: Only 4G technology will be used.
- **NR5G-NSA**: Only 5G non-standalone technology will be used.
- **NR5G-SA**: Only 5G standalone technology will be used.

The default is **all**.

> **Note** If **manual** is configured for the carrier selection mode and a specific network technology is selected for the cellular network technology, your modem must support the selected technology or no cellular connection will be established. If you are using a cellular connection to perform this procedure, you may lose your connection and the device will no longer be accessible.

11. SIM failover is enabled by default, which means that the modem will automatically fail over from the active SIM to the next available SIM when the active SIM fails to connect. To disable:

```
(config network interface my_wwan)> modem sim_failover false
(config network interface my_wwan)>
```

If enabled:

a. Set the number of times that the device should attempt to connect to the active SIM before failing over to the next available SIM:

```
(config network interface my_wwan)> modem sim_failover_retries num
(config network interface my_wwan)>
```

The default setting is **5**.

b. Configure how SIM failover will function if automatic SIM switching is unavailable:

```
(config network interface my_wwan)> modem sim_failover_alt value
(config network interface my_wwan)>
```

where *value* is one of:

- **none**: The device will perform no alternative action if automatic SIM switching is unavailable.
- **reset**: The device will reset the modem if automatic SIM switching is unavailable.
- **reboot**: The device will reboot if automatic SIM switching is unavailable.

12. (Optional) To configure the device to use either the preconfigured APNs, custom APNs, or both:

```
(config)> network interface modem modem apn_selection value
(config)>
```

Where *value* is one of the following:

- apn_list_only
- both_lists
- built-in-list-only

13. (Optional) To configure the IP address of a custom gateway or a custom netmask:
    a. Enable the custom gateway:

```
(config network interface my_wwan)> modem custom_gw enable true
(config network interface my_wwan)>
```

    b. Set the IP address and netmask of the custom gateway:

```
(config network interface my_wwan)> modem custom_gw gateway ip_address/netmask
(config network interface my_wwan)> modem custom_gw
```

    To override only the gateway netmask, but not the gateway IP address, use all zeros for the IP address. For example, **0.0.0.0./32** will use the network-provided gateway, but with a /32 netmask.
14. Optional IPv4 configuration items:
    a. IPv4 support is enabled by default. To disable:

```
(config network interface my_wwan)> ipv4 enable false
(config network interface my_wwan)>
```

    b. Set the type, which determines how the modem in the device obtains an IP address from the cellular network.

```
(config network interface my_wwan)> ipv4 modem_type value
(config network interface my_wwan)>
```

    Where *value* is one of:
    - **static**: Digi device obtains the static IP address from the cellular network.
    - **dhcp**: Digi device obtains IP address via a DHCP server on the cellular network.

    c. Set the MTU:

```
(config network interface my_wwan)> ipv4 mtu num
(config network interface my_wwan)>
```

    d. Configure when the WWAN's DNS servers will be used:

```
(config network interface my_wwan)> ipv4  dns value
(config network interface my_wwan)>
```

    Where *value* is one of:
    - **always**: DNS will always be used for this WWAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
    - **never**: Never use DNS servers for this WWAN.
    - **primary**: Only use the DNS servers provided for this WWAN when the WWAN is the primary route.

    The default setting is **primary**.
15. Optional IPv6 configuration items:

a. IPv6 support is enabled by default. To disable:

```
(config network interface my_wwan)> ipv4 enable false
(config network interface my_wwan)>
```

b. Set the type, which determines how the modem in the device obtains an IP address from the cellular network.

```
(config network interface my_wwan)> ipv4 modem_type value
(config network interface my_wwan)>
```

Where *value* is one of:

- **static**: Digi device obtains the static IP address from the cellular network.
- **dhcp**: Digi device obtains IP address via a DHCP server on the cellular network.

c. Set the MTU:

```
(config network interface my_wwan)> ipv4 mtu num
(config network interface my_wwan)>
```

d. Configure when the WWAN's DNS servers will be used:

```
(config network interface my_wwan)> ipv4  dns value
(config network interface my_wwan)>
```

Where *value* is one of:

- **always**: DNS will always be used for this WWAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
- **never**: Never use DNS servers for this WWAN.
- **primary**: Only use the DNS servers provided for this WWAN when the WWAN is the primary route.

The default setting is **primary**.

16. See Configure SureLink active recovery to detect modem failures for information about configuring active recovery.
17. Save the configuration and apply the change.

```
(config network interface my_wan)> save
Configuration saved.
>
```

18. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show WWAN status and statistics

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. From the menu, click **Status**.
2. Under **Networking**, click **Interfaces**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the show network command at the Admin CLI prompt:

```
> show network

Interface       Proto  Status   Address
--------------- -----  -------  ------------------------------
setupip         IPv4   up       192.168.210.1/24
setuplinklocalip IPv4  up       169.254.100.100/16
eth             IPv4   up       192.168.2.1/24
eth             IPv6   up       fd00:2704::1/48
loopback        IPv4   up       127.0.0.1/8
modem           IPv4   up       10.200.1.101/30
modem           IPv6   down

>
```

3. Additional information can be displayed by using the show network verbose command:

```
> show network verbose

Interface       Proto  Status  Type    Zone     Device    Metric  Weight
--------------- -----  ------- ------  -------- --------  ------  ------
setupip         IPv4   up      static  setup    eth       10      10
setuplinklocalip IPv4  up      static  setup    eth       0       10
eth             IPv4   up      static  internal eth       5       10
eth             IPv6   up      static  internal eth       5       10
loopback        IPv4   up      static  loopback loopback  0       10
modem           IPv4   up      modem   external wwan1     3       10
modem           IPv6   down    modem   external wwan1     3       10

>
```

4. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific WAN. For example, to display information about ETH1, enter **show network interface *eth1***:

```
> show network interface eth1

wan1 Interface Status
---------------------
Device          : eth1
```

```
Zone            : external

IPv4 Status     : up
IPv4 Type       : dhcp
IPv4 Address(es)   : 10.10.10.10/24
IPv4 Gateway    : 10.10.10.1
IPv4 MTU        : 1500
IPv4 Metric     : 1
IPv4 Weight     : 10
IPv4 DNS Server(s)  : 10.10.10.2, 10.10.10.3

IPv6 Status     : up
IPv6 Type       : dhcpv6
IPv6 Address(es)   : fe00:2404::240:f4ff:fe80:120/64
IPv6 Gateway    : ff80::234:f3ff:ff0e:4320
IPv6 MTU        : 1500
IPv6 Metric     : 1
IPv6 Weight     : 10
IPv6 DNS Server(s)  : fd00:244::1, fe80::234:f3f4:fe0e:4320

>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a WWAN.

Follow this procedure to delete any WANs and WWANs that have been added to the system. You cannot delete the preconfigured WAN, **ETH1**, or the preconfigured WWAN, **Modem**.

Web

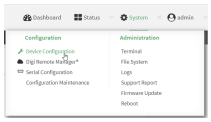
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Click the menu icon (**...**) next to the name of the WAN or WWAN to be deleted and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **del** command to delete the WAN or WWAN. For example, to delete a WWAN named my_wwan:

```
(config)> del network interface my_wwan
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Local Area Networks (LANs)

The IX10 device is preconfigured with the following Local Area Networks (LANs):

Interface type	Preconfigured interfaces	Devices	Default configuration
Local Area Network (LAN)	▪ **ETH**	▪ Ethernet: **ETH**	▪ Firewall zone: Internal ▪ IP Address: 192.168.2.1/24 ▪ DHCP server enabled ▪ LAN priority: Metric=5 ▪ Ethernet port Type: Hybrid IP address Note The new default **Type** setting for the Ethernet port is now **Hybrid IP Address** (Interfaces > ETH > IPv4 > Type). The Ethernet port acts as a WAN (DHCP client) but automatically changes to LAN DHCP server if no WAN connections occurs within one minute of reboot. The benefit is for customers provisioning or staging these routers. There is no need to insert a SIM card in each device or make local UI changes for every device if you just want to get it online to upgrade device or modem firmware and apply some basic configuration settings for provisioning or staging purposes.

Interface type	Preconfigured interfaces	Devices	Default configuration
	▪ **Loopback**	▪ Ethernet: **Loopback**	▪ Firewall zone: Loopback ▪ IP address: 127.0.0.1/8
	▪ **Setup IP**	▪ Ethernet: **ETH**	▪ Firewall zone: Setup ▪ IP address 192.168.210.1/24
	▪ **Setup Link-local IP**	▪ Ethernet: **ETH**	▪ Firewall zone: Setup ▪ IP address 169.254.100.100/16

You can modify configuration settings for **ETH**, and you can create new LANs.

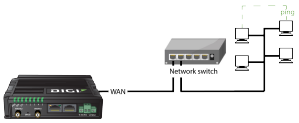
This section contains the following topics:

About Local Area Networks (LANs) 159
Configure a LAN 159
Change the default LAN subnet 166
Change the LAN address type 167
Show LAN status and statistics 168
Delete a LAN 170
Configure an interface to operate in passthrough mode 171
DHCP servers 177

About Local Area Networks (LANs)

A Local Area Network (LAN) connects network devices together in a logical Layer-2 network.

The following diagram shows a LAN connected to the **ETH** Ethernet device. Once the LAN is configured and enabled, the devices connected to the network interfaces can communicate with each other, as demonstrated by the **ping** commands.



Configure a LAN

Configuring a Local Area Network (LAN) involves configuring the following items:

Required configuration items

- A name for the interface.

  Note If the interface name is more than eight characters, the name will be truncated in the underlying network interface to the first six characters followed by three digits, incrementing from 000. This affects any custom scripts or firewall rules that may be trying to adjust the interface or routing table entries.

- The interface type: either **Ethernet**, **IP Passthrough**, or **PPPoE**.
- The firewall zone: **Internal**.
- The network device that is used by the LAN.
- The IPv4 address and subnet mask for the LAN. While it is not strictly necessary for a LAN to have an IP address, if you want to send traffic from other networks to the LAN, you must configure an IP address.

  Note By default, **ETH** is set to an IP address of 192.168.2.1 and uses the IP subnet of 192.168.2.0/24. If the **WAN/ETH1** Ethernet device is being used by a WAN with the same IP subnet, you should change the Setup IP address and subnet of LAN1.

Additional configuration items

- Additional IPv4 configuration:
  - The type being the way to control how the modem in the Digi device obtains an IP address from the cellular network.
  - The metric for IPv4 routes associated with the LAN.
  - The relative weight for IPv4 routes associated with the LAN.
  - The IPv4 management priority of the LAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
  - The IPv4 Maximum Transmission Unit (MTU) of the LAN.
  - Whether to assign a static IPv4 address to the LAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.

    - IPv4 DHCP server configuration. See DHCP servers for more information.
- IPv6 configuration:
    - The type being the way to control how the modem in the Digi device obtains an IP address from the cellular network.
    - The metric for IPv6 routes associated with the LAN.
    - The relative weight for IPv6 routes associated with the LAN.
    - The IPv6 management priority of the LAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
    - The IPv6 Maximum Transmission Unit (MTU) of the LAN.
    - Whether to assign a static IPv6 address to the LAN.
    - When to use DNS: always, never, or only when this interface is the primary default route.
    - The IPv6 prefix length and ID.
    - IPv6 DHCP server configuration. See DHCP servers for more information.
- MAC address denylist and allowlist.

To create a new LAN or edit an existing LAN:

Web

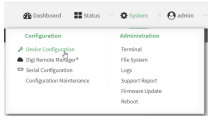
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

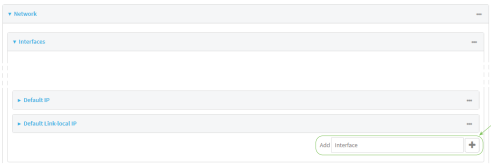
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

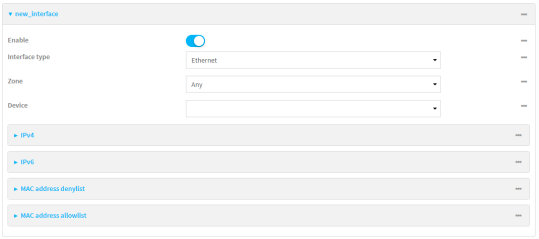
   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.

4. Create the LAN or select an existing LAN:
   - To create a new LAN, for **Add interface**, type a name for the LAN and click .



   - To edit an existing LAN, click to expand the LAN.

   The Interface configuration window is displayed.



   New LANs are enabled by default. To disable, toggle off **Enable**.
5. For **Interface type**, leave at the default setting of **Ethernet**.
6. For **Zone**, select the appropriate firewall zone. See Firewall configuration for further information.
7. For **Device**, select an Ethernet device.
8. (Optional) Click to expand **802.1x** to configure 802.1x port based network access control.

   The IX10 can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.
   a. Click to expand **Authentication**.
   b. Click **Enable server** to enable the 802.1x authenticator on the IX10 device.
   c. Set the **Reauth** period.
9. Configure IPv4 settings:
   a. Click to expand **IPv4**.

      IPv4 support is enabled by default.
   b. For **Type**, select **Static IP address**.
   c. For **Address**, type the IP address and subnet of the LAN interface. Use the format *IPv4_address/netmask*, for example, 192.168.2.1/24.
   d. Optional IPv4 configuration items:
      i. Set the **MTU**.
   e. Enable the DHCP server:
      i. Click to expand **DHCP server**.
      ii. Click **Enable**.

      See DHCP servers for information about configuring the DHCP server.
   f. Enable **Force link** to keep the network interface active even when the device link is down.
10. See Configure DHCP relay for information about configuring **DHCP relay**.

11. (Optional) Configure IPv6 settings:
    a. Click to expand **IPv6**.
    b. **Enable** IPv6 support.
    c. For **Type**, select **IPv6 prefix delegration**.
    d. For **Prefix length**, type the minimum length of the prefix to assign to this LAN. If the minimum length is not available, then a longer prefix will be used.
    e. For **Prefix ID**, type the identifier used to extend the prefix to the assigned length. Leave blank to use a random identifier.
    f. Set the **MTU**.
    g. (Optional) To assign a static address to a network interface, click to expand **Static address**.
        i. Click the slider to enable.
        ii. For **Address**, type the name of the static address you want to use (for example, *tree::squirrel:tail/64*).
12. (Optional) Click to expand **MAC address denylist**.

    Incoming packets will be dropped from any devices whose MAC addresses is included in the **MAC address denylist**.
    a. Click to expand **MAC address denylist**.
    b. For **Add MAC address**, click ⍾.
    c. Type the **MAC address**.
13. (Optional) Click to expand **MAC address allowlist**.

    If allowlist entries are specified, incoming packets will only be accepted from the listed MAC addresses.
    a. Click to expand **MAC address allowlist**.
    b. For **Add MAC address**, click ⍾.
    c. Type the **MAC address**.
14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new LAN or edit an existing one:
   - To create a new LAN named **my_lan**:

```
(config)> add network interface my_lan
(config network interface my_lan)>
```

- To edit an existing LAN named **my_lan**, change to the **my_lan** node in the configuration schema:

```
(config)> network interface my_lan
(config network interface my_lan)>
```

4. Set the appropriate firewall zone:

```
(config network interface my_lan)> zone zone
(config network interface my_lan)>
```

See Firewall configuration for further information.

5. Select an Ethernet device.
   a. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface my_lan)> device ?

Device: The network device used by this network interface.
Format:
 /network/device/eth
 /network/device/loopback
Current value:

(config network interface my_lan)> device
```

   b. Set the device for the LAN:

```
(config network interface my_lan)> device device
(config network interface my_lan)>
```

6. Configure IPv4 settings:
   - IPv4 support is enabled by default. To disable:

```
(config network interface my_lan)> ipv4 enable false
(config network interface my_lan)>
```

   - The LAN is configured by default to use a static IP address for its IPv4 configuration. To configure the LAN to be a DHCP client, rather than using a static IP addres:

```
(config network interface my_lan)> ipv4 type dhcp
(config network interface my_lan)>
```

     These instructions assume that the LAN will use a static IP address for its IPv4 configuration.

   a. Set the IPv4 address and subnet of the LAN interface. Use the format *IPv4_address/netmask*, for example, 192.168.2.1/24.

```
(config network interface my_lan)> ipv4 address ip_address/netmask
(config network interface my_lan)>
```

   b. Optional IPv4 configuration items:

i. Set the MTU:

```
(config network interface my_lan)> ipv4 mtu num
(config network interface my_lan)>
```

c. Enable the DHCP server:

```
(config network interface my_lan)> ipv4 dhcp_server enable true
```

See DHCP servers for information about configuring the DHCP server.

d. See Configure WAN priority and default route metrics for further information about metrics.

7. (Optional) Configure IPv6 settings:

a. Enable IPv6 support:

```
(config network interface my_lan)> ipv6 enable true
(config network interface my_lan)>
```

b. Set the IPv6 type to DHCP:

```
(config network interface my_lan)> ipv6 type dhcpv6
(config network interface my_lan)>
```

c. Generally, the default settings for IPv6 support are sufficient. You can view the default IPv6 settings by using the question mark (**?**):

```
(config network interface my_lan)> ipv6 ?

IPv6

 Parameters            Current Value
 ------------------------------------------------------------------------------
 enable                 true          Enable
 metric                 0             Metric
 mgmt                   0             Management priority
 mtu                    1500          MTU
 prefix_id              1             Prefix ID
 prefix_length          48            Prefix length
 type                   prefix_delegation  Type
 weight                 10            Weight

 Additional Configuration
 ------------------------------------------------------------------------------
 connection_monitor     Active recovery
 dhcpv6_server          DHCPv6 server

(config network interface my_lan)>
```

View default settings for the IPv6 DHCP server:

```
(config network interface my_lan)> ipv6 dhcpv6_server ?
```

```
DHCPv6 server: The DHCPv6 server settings for this network interface.

 Parameters            Current Value
 ------------------------------------------------------------------------------
 enable                true        Enable

(config network interface my_lan)>
```

d. Modify any of the remaining default settings as appropriate.

e. (Optional) To assign a static address to a network interface:

```
>config
(config)> network interfacemy_lan ipv6 static ?

Static address: IPv6 static address.


 Parameters       Current value
 ------------------------------------------------------------------------
 address                        Address
 enable               false     Enable

(config)> network interface my_lan ipv6 static address ?

Address: The IPv6 address to use.

Format: IPv6_address/prefix_length

Current value:

(config)>
```

8. (Optional) To configure 802.1x port based network access control:

Note The IX10 can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

a. Enable the 802.1x authenticator on the IX10 device:

```
(config network interface my_lan)> 802_1x authentication enable true
(config network interface my_lan)>
```

b. Set the frequency period for reauthorization:

```
(config network interface my_lan)> 802_1x authentication reauth_period value
(config network interface my_lan)>
```

where *value* is an integer between **0** and **86400**. The default is **3600**.

9. (Optional) Configure the MAC address deny list.

Incoming packets will be dropped from any devices whose MAC addresses is included in the MAC address denylist.

a. Add a MAC address to the denylist:

```
(config network interface my_lan)> add mac_denylist end mac_address
(config network interface my_lan)>
```

where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

b. Repeat for each additional MAC address.

10. (Optional) Configure the MAC address allowlist.

If allowlist entries are specified, incoming packets will only be accepted from the listed MAC addresses.

a. Add a MAC address to the allowlist:

```
(config network interface my_lan)> add mac_allowlist end mac_address
(config network interface my_lan)>
```

where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

b. Repeat for each additional MAC address.

11. Save the configuration and apply the change.

```
(config network interface my_lan)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Change the default LAN subnet

You can change the IX10 default LAN subnet—192.168.2.1/24—to any range of private IPs. The local DHCP server range will also change to the range of the LAN subnet.

To change the LAN subnet:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

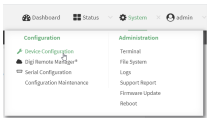
b. Click the **Device ID**.

c. Click **Settings**.

d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces** > **LAN** > **IPv4**.
4. For **Address**, change the IP address to an alternate private IP. You must also specify the subnet mask. It must have the syntax of *IPv4_address*/*netmask*.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, set the IP address to an alternate private IP:

```
(config)> network interface lan ipv4 address IPv4_address/netmask
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Change the LAN address type

By default, the LAN interface uses a static IP address. To configure it to use a DHCP address instead:

Web

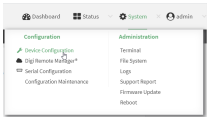
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces** > **LAN** > **IPv4**.
4. For the **Type** option, select **DHCP address**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, set the LAN to use a DHCP address:

```
(config)> network interface lan ipv4 type dhcp
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show LAN status and statistics

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. From the menu, click **Status**.
2. Under **Networking**, click **Interfaces**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the show network command at the Admin CLI prompt:

```
> show network

Interface       Proto  Status   Address
--------------- -----  -------  ------------------------------
setupip         IPv4   up       192.168.210.1/24
setuplinklocalip IPv4  up       169.254.100.100/16
eth             IPv4   up       192.168.2.1/24
eth             IPv6   up       fd00:2704::1/48
loopback        IPv4   up       127.0.0.1/8
modem           IPv4   up       10.200.1.101/30
modem           IPv6   down

>
```

3. Additional information can be displayed by using the show network verbose command:

```
> show network verbose

Interface       Proto  Status  Type    Zone     Device    Metric  Weight
--------------- -----  ------- ------  -------- --------  ------  ------
setupip         IPv4   up      static  setup    eth       10      10
setuplinklocalip IPv4  up      static  setup    eth       0       10
eth             IPv4   up      static  internal eth       5       10
eth             IPv6   up      static  internal eth       5       10
loopback        IPv4   up      static  loopback loopback  0       10
modem           IPv4   up      modem   external wwan1     3       10
modem           IPv6   down    modem   external wwan1     3       10

>
```

4. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific LAN. For example, to display information about ETH, enter **show network interface *eth***:

```
> show network interface eth

lan1 Interface Status
---------------------
Device          : eth
```

```
Zone            : internal

IPv4 Status     : up
IPv4 Type       : static
IPv4 Address(es)   : 192.168.2.1/24
IPv4 Gateway    :
IPv4 MTU        : 1500
IPv4 Metric     : 5
IPv4 Weight     : 10
IPv4 DNS Server(s) :

IPv6 Status     : up
IPv6 Type       : prefix
IPv6 Address(es)   : fd00:2704::1/48
IPv6 Gateway    :
IPv6 MTU        : 1500
IPv6 Metric     : 5
IPv6 Weight     : 10
IPv6 DNS Server(s) :

>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a LAN

Follow this procedure to delete any LANs that have been added to the system. You cannot delete the preconfigured LAN, **LAN1**.

Web

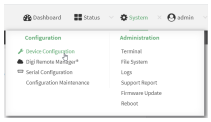
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Click the menu icon (**...**) next to the name of the LAN to be deleted and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **del** command to delete the LAN. For example, to delete a LAN named my_lan:

```
(config)> del network interface my_lan
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure an interface to operate in passthrough mode

You can configure interfaces on your IX10 device to operate in passthrough mode, which means that the device passes the IP address assigned to it on a WAN or cellular modem interface, to a client connected to a LAN interface.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

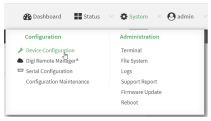
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

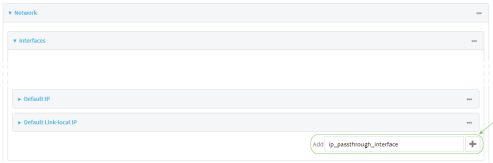
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

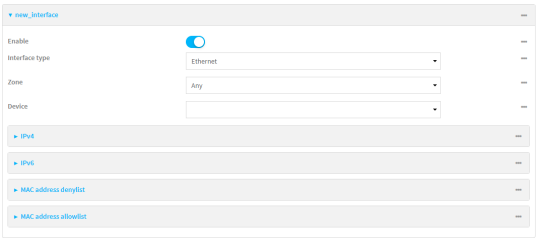
   The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Create the interface or select an existing interface:
   - To create a new interface, for **Add interface**, type a name for the interface and click ⊕

   - To edit an existing interface, click to expand the interface.

   The Interface configuration window is displayed.

   New Interfaces are enabled by default. To disable, toggle off **Enable**.
5. For **Interface type**, select **IP Passthrough**.
6. For **Zone**, select **Internal**.
7. For Device, select an Ethernet device or a Wi-Fi access point.
8. Add one or more interface that will be the source of the passed-through IP address:
   a. Click to expand **Source interfaces**.
   b. Click ⊕ to add a source interface.

c. Select the appropriate **Interface**.

d. Repeat for additional interfaces.

9. (Optional) **Packet filtering** is disabled by default. Toggle on to enable.

   If packet filtering is disabled, traffic is allowed in both directions and it is the responsibility of the external device to provide its own firewall.

10. (Optional) **Allow all addresses** is disabled by default. Toggle on to enable.

    When enabled, this option allows forwarding between the source interface and devices connected to this interface, which allows connected devices to forward and receive packets without network address translation (NAT). This should normally be disabled unless it is required for modem passthrough, because some cellular will disconnect modems that send packets that are not from the carrier-assigned IP address.

11. **Ancillary addressing** is enabled by default, which provides an IPv4 address to the connected device when the source address is not available.

    a. For **Ancillary address/netmask**, type the IPv4 address and netmask to provide to the connected device when the source address is not available.

    b. For **Ancillary gateway**, type the IPv4 address of the network gateway to be used when the connected device when the source address is not available.

    c. **Ancillary DNS redirect** is enabled by default, which means resolves all DNS requests to the connected device and redirects HTTP traffic to the device's web administration page.

12. For **Server type**, select the type of server to use to pass the IP address through to the client.

13. If **PPPoE server** is selected for **Server type**:

    a. Click to expand **PPPoE server**.

    b. For **Service name**, type the name of service to offer to the client.

    c. For **Access concentrator name**, type the name of the access concentrator to report to the client. If no name is provided, the host name is used.

    d. For **Authentication method**, select the authentication method used to connect to the remote peer.

       If an authentication method is selected, type the **Username** and **Password** required to authenticate the remote peer.

    e. (Optional) Click to expand **Custom PPP configuration**.

    f. Custom PPP configuration is disabled by default. Click toggle on **Enable**.

    g. Enable **Override** to override the default configuration and use only the custom configuration file.

    h. For **Configuration** file, type or paste configuration data using the format of a pppd options file.

14. (Optional) Click to expand **802.1x** to configure 802.1x port based network access control.

    The IX10 can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

    a. Click to expand **Authentication**.

    b. Click **Enable server** to enable the 802.1x authenticator on the IX10 device.

    c. Set the **Reauth** period.

15. Configure IPv4 settings:
    a. Click to expand **IPv4**.

       IPv4 support is enabled by default.
    b. Set the **Metric**.
    c. For **Weight**, type the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, **Weight** is used to load balance traffic to the interfaces.
    d. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
    e. Set the **MTU**.
    f. For **Use DNS**, select one of the following:
       - **Always**: DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
       - **When primary default route**: Only use the DNS servers provided for this interface when the interface is the primary route.
       - **Never**: Never use DNS servers for this interface.
    g. See Configure SureLink active recovery to detect modem failures for information about configuring **SureLink** for active recovery.
16. (Optional) Configure IPv6 settings:
    a. Click to expand **IPv6**.
    b. **Enable** IPv6 support.
    c. Set the **Metric**.
    d. For **Weight**, type the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, **Weight** is used to load balance traffic to the interfaces.
    e. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
    f. Set the **MTU**.
    g. For **Use DNS**, select one of the following:
       - **Always**: DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
       - **When primary default route**: Only use the DNS servers provided for this interface when the interface is the primary route.
       - **Never**: Never use DNS servers for this interface.
    h. See Configure SureLink active recovery to detect modem failures for information about configuring **SureLink** for active recovery.
17. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new interface or edit an existing one:
   - To create a new interface named **ip_passthrough_interface**:

```
(config)> add network interface ip_passthrough_interface
(config network interface ip_passthrough_interface)>
```

   - To edit an existing interface named **ip_passthrough_interface**, change to the IP-passthrough-interface node in the configuration schema:

```
(config)> network interface ip_passthrough_interface
(config network interface ip_passthrough_interface)>
```

4. Set the interface type to passthrough:

```
(config network interface ip_passthrough_interface)> type passthrough
(config network interface ip_passthrough_interface)>
```

5. Set the firewall zone to internal:

```
(config network interface ip_passthrough_interface)> zone internal
(config network interface ip_passthrough_interface)>
```

6. Select an Ethernet device or a Wi-Fi access point for this interface:
   a. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface my_wan)> device ?


Device: The network device used by this network interface.
Format:
  /network/device/eth
  /network/device/loopback
Current value:

(config network interface ip_passthrough_interface)> device
```

   b. Set the device for the interface:

```
(config network interface ip_passthrough_interface)> device device
(config network interface my_wan)>
```

7. Set passthrough options

8. Configure IPv4 settings:
   - IPv4 support is enabled by default. To disable:

     ```
     (config network interface ip_passthrough_interface)> ipv4 enable false
     (config network interface ip_passthrough_interface)>
     ```

   a. Set the IP metric:

      ```
      (config network interface ip_passthrough_interface)> ipv4 metric num
      (config network interface ip_passthrough_interface)>
      ```

   b. Set the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, the weight is used to load balance traffic to the interfaces.

      ```
      (config network interface ip_passthrough_interface)> ipv4 weight num
      (config network interface ip_passthrough_interface)>
      ```

   c. Set the management priority. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

      ```
      (config network interface ip_passthrough_interface)> ipv4 mgmt num
      (config network interface ip_passthrough_interface)>
      ```

   d. Set the MTU:

      ```
      (config network interface ip_passthrough_interface)> ipv4 mtu num
      (config network interface ip_passthrough_interface)>
      ```

   e. Configure how to use DNS:

      ```
      (config network interface ip_passthrough_interface)> ipv4 use_dns value
      (config network interface ip_passthrough_interface)>
      ```

      where *value* is one of:
      - **always**: DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
      - **primary**: Only use the DNS servers provided for this interface when the interface is the primary route.
      - **never**: Never use DNS servers for this interface.

   f. See Configure SureLink active recovery to detect modem failures for information about configuring **SureLink** for active recovery.

9. (Optional) Configure IPv6 settings:

   a. Enable IPv6 support:

      ```
      (config network interface ip_passthrough_interface)> ipv6 enable true
      (config network interface ip_passthrough_interface)>
      ```

   b. Generally, the default settings for IPv6 support are sufficient. You can view the default IPv6 settings by using the question mark (**?**):

```
(config network interface ip_passthrough_interface)> ipv6 ?

IPv6

 Parameters            Current Value
-------------------------------------------------------------------------------
 enable                 true          Enable
 metric                 0             Metric
 mgmt                   0             Management priority
 mtu                    1500          MTU
 use_dns                always        Use DNS
 weight                 10            Weight

(config network interface ip_passthrough_interface)>
```

c. Modify any of the remaining default settings as appropriate.

10. (Optional) To configure 802.1x port based network access control:

> **Note** The IX10 can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

a. Enable the 802.1x authenticator on the IX10 device:

```
(config network interface ip_passthrough_interface)> 802_1x authentication enable true
(config network interface ip_passthrough_interface)>
```

b. Set the frequency period for reauthorization:

```
(config network interface ip_passthrough_interface)> 802_1x authentication reauth_period value
(config network interface ip_passthrough_interface)>
```

where *value* is an integer between **0** and **86400**. The default is **3600**.

11. Save the configuration and apply the change.

```
(config network interface ip_passthrough_interface)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

DHCP servers

You can enable DHCP on your IX10 device to assign IP addresses to clients, using either:

- The DHCP server for the device's local network, which assigns IP addresses to clients on the device's local network. Addresses are assigned from a specified pool of IP addresses. For a local network, the device uses the DHCP server that has the IP address pool in the same IP subnet as the local network.

When a host receives an IP configuration, the configuration is valid for a particular amount of time, known as the lease time. After this lease time expires, the configuration must be renewed. The host renews the lease time automatically.

- A DHCP relay server, which forwards DHCP requests from clients to a DHCP server that is running on a separate device.

Configure a DHCP server

Note These instructions assume you are configuring the device to use its local DHCP server. For instructions about configuring the device to use a DHCP relay server, see Configure DHCP relay.

Required configuration items

- Enable the DHCP server.

Additional configuration items

- The lease address pool: the range of IP addresses issued by the DHCP server to clients.
- Lease time: The length, in minutes, of the leases issued by the DHCP server.
- The Maximum Transmission Units (MTU).
- The domain name suffix appended to host names.
- The IP gateway address given to clients.
- The IP addresses of the preferred and alternate Domain Name Server (DNS), NTP servers, and WINS severs that are given to clients.
- The TFTP server name.
- The filepath and name of the bootfile on the TFTP server.
- Custom DHCP options. See Configure DHCP options for information about custom DHCP options.
- Static leases. See Map static IP addresses to hosts for information about static leases.

Web

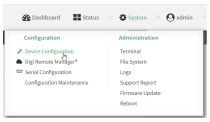
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Click to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server**.
6. **Enable** the DHCP server.
7. (Optional) For **Lease time**, type the amount of time that a DHCP lease is valid.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Lease time** to ten minutes, enter **10m** or **600s**.

   The default is 12 hours.

   - By default, DHCP leases are persistent across reboots. You can disable persistent leases:
     a. Click **Network** > **Advanced**.
     b. Click to toggle off **DHCP persistent leases**.
8. (Optional) For **Lease range start** and **Lease range end**, type the lowest and highest IP address that the DHCP server will assign to a client. This value represents the low order byte of the address (the final triplet in an IPv4 address, for example, 192.168.2.**xxx**). The remainder of the IP address will be based on the LAN's static IP address as defined in the **Address** field.

   Allowed values are between **1** and **254**, and the default is **100** for **Lease range start** and **250** for **Lease range end**.

   - Sequential DHCP address allocation:

     By default, DHCP addresses are assigned psuedo-randomly, using a hash of the client's MAC address to determine the IP address that gets assigned. You can configure the device to use sequential IP addresses instead:

     a. Click **Network** > **Advanced**.
     b. Click to enable **Sequential DHCP address allocation**.

     Because sequential mode does not use a hash based on the client's MAC address, when DHCP lease expires, the client is not likely to get the same IP address assigned to it. Therefore, sentential DHCP address allocation generally should not be used.
9. Optional DHCP server settings:
   a. Click to expand **Advanced settings**.
   b. For **Gateway**, select either:
      - **None**: No gateway is broadcast by the DHCP server. Client destinations must be resolvable without a gateway.
      - **Automatic**: Broadcasts the IX10 device's gateway.
      - **Custom**: Allows you to identify the IP address of a **Custom gateway** to be broadcast.

The default is **Automatic**.

c. For **MTU**,
   - **None**: An MTU of length **0** is broadcast. This is not recommended.
   - **Automatic**: No MTU is broadcast and clients will determine their own MTU.
   - **Custom**: Allows you to identify a **Custom MTU** to be broadcast.

   The default is **Automatic**.

d. For **Domain name suffix**, type the domain name that should be appended to host names.

e. For **Primary** and **Secondary DNS**, **Primary** and **Secondary NTP server**, and **Primary** and **Secondary WINS server**, select either:
   - **None**: No server is broadcast.
   - **Automatic**: Broadcasts the IX10 device's server.
   - **Custom**: Allows you to identify the IP address of the server.

f. Enable **BOOTP dynamic allocation** to automatically assign an IP address to a device on the server.

CAUTION! The IP address assigned to the device is leased forever and becomes permanently unavailable for other hosts to use.

g. For **Bootfile name**, type the relative path and file name of the bootfile on the TFTP server.

h. For **TFTP server** name, type the IP address or host name of the TFTP server.

i. Enable

10. See Configure DHCP options for information about **Custom DHCP options**.
11. See Map static IP addresses to hosts for information about **Static leases**.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the DHCP server for an existing LAN. For example, to enable the DHCP server for a LAN named **my_lan**:

```
(config)> network interface my_lan ipv4 dhcp_server enable true
(config)>
```

See Configure a LAN for information about creating a LAN.

4. (Optional) Set the amount of time that a DHCP lease is valid:

```
(config)> network interface my_lan ipv4 dhcp_server lease_time value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **network interface my_lan ipv4 dhcp_server lease_time** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_lan ipv4 dhcp_server lease_time 600s
(config)>
```

- By default, DHCP leases are persistent across reboots. You can disable persistent leases:

```
(config)> network advanced dhcp_persistent_lease false
(config)>
```

5. (Optional) Set the lowest IP address that the DHCP server will assign to a client. This value represents the low order byte of the address (the final triplet in an IPv4 address, for example, 192.168.2.**xxx**). The remainder of the IP address will be based on the LAN's static IP address as defined in the **address** parameter.

```
(config)> network interface my_lan ipv4 dhcp_server lease_start num
(config)>
```

Allowed values are between **1** and **254**, and the default is **100**.

6. (Optional) Set the highest IP address that the DHCP server will assign to a client:

```
(config)> network interface my_lan ipv4 dhcp_server lease_end num
(config)>
```

Allowed values are between **1** and **254**, and the default is **250**.

7. Sequential DHCP address allocation

By default, DHCP addresses are assigned psuedo-randomly, using a hash of the client's MAC address to determine the IP address that gets assigned. You can configure the device to use sequential IP addresses instead:

```
(config)> network advanced sequential_dhcp_allocation true
(config)>
```

Because sequential mode does not use a hash based on the client's MAC address, when DHCP lease expires, the client is not likely to get the same IP address assigned to it. Therefore, sentential DHCP address allocation generally should not be used.

8. Optional DHCP server settings:

a. Click to expand **Advanced settings**.

b. Determine how the DHCP server should broadcast the gateway server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced gateway value
(config)>
```

where **value** is one of:

- **none**: No gateway is broadcast by the DHCP server. Client destinations must be resolvable without a gateway.
- **auto**: Broadcasts the IX10 device's gateway.
- **custom**: Allows you to identify the IP address of a custom gateway to be broadcast:

```
(config)> network interface my_lan ipv4 dhcp_server advanced gateway_custom ip_
address
(config)>
```

The default is **auto**.

c. Determine how the DHCP server should broadcast the the MTU:

```
(config)> network interface my_lan ipv4 dhcp_server advanced mtu value
(config)>
```

where **value** is one of:

- **none**: An MTU of length **0** is broadcast. This is not recommended.
- **auto**: No MTU is broadcast and clients will determine their own MTU.
- **custom**: Allows you to identify a custom MTU to be broadcast:

```
(config)> network interface my_lan ipv4 dhcp_server advanced mtu_custom mtu
(config)>
```

The default is **auto**.

d. Set the domain name that should be appended to host names:

```
(config)> network interface my_lan ipv4 dhcp_server advanced domain_suffix name
(config)>
```

e. Set the IP address or host name of the primary and secondary DNS, the primary and secondary NTP server, and the primary and secondary WINS servers:

```
(config)> network interface my_lan ipv4 dhcp_server advanced primary_dns value
(config)> network interface my_lan ipv4 dhcp_server advanced secondary_dns value
(config)> network interface my_lan ipv4 dhcp_server advanced primary_ntp value
(config)> network interface my_lan ipv4 dhcp_server advanced secondary_ntp value
(config)> network interface my_lan ipv4 dhcp_server advanced primary_wins value
(config)> network interface my_lan ipv4 dhcp_server advanced secondary_wins value
(config)>
```

where **value** is one of:

- **none**: No server is broadcast.
- **auto**: Broadcasts the IX10 device's server.
- **custom**: Allows you to identify the IP address of the server. For example:

```
(config)> network interface my_lan ipv4 dhcp_server advanced primary_dns_custom ip_
address
(config)>
```

The default is **auto**.

f. Set the IP address or host name of the TFTP server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced nftp_server ip_address
(config)>
```

g. Set the relative path and file name of the bootfile on the TFTP server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced bootfile filename
(config)>
```

h. Enable **BOOTP dynamic allocation** to automatically assign an IP address to a device on the server:

CAUTION! The IP address assigned to the device is leased forever and becomes permanently unavailable for other hosts to use.

```
(config)> network interface my_lan ipv4 dhcp_server advanced bootp_dynamic true
(config)>
```

9. See Configure DHCP options for information about custom DHCP options.
10. See Map static IP addresses to hosts for information about static leases.
11. Save the configuration and apply the change.

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Map static IP addresses to hosts

You can configure the DHCP server to assign static IP addresses to specific hosts.

Required configuration items

- IP address that will be mapped to the device.
- MAC address of the device.

Additional configuration items

- A label for this instance of the static lease.

To map static IP addresses:

Web

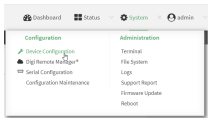
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Click to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Static leases**.
6. For **Add Static lease**, click .
7. Type the **MAC address** of the device associated with this static lease.
8. Type the **IP address** for the static lease.

   Note The IP address here should be outside of the DHCP server's configured lease range. See Configure a DHCP server for further information about the lease range.
9. (Optional) For **Hostname**, type a label for the static lease. This does not have to be the device's actual hostname.
10. Repeat for each additional DHCP static lease.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a static lease to the DHCP server configuration for an existing LAN. For example, to add static lease to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_server advanced static_lease end
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)>
```

See Configure a LAN for information about creating a LAN.

4. Set the MAC address of the device associated with this static lease, using the colon-separated format:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)> mac
00:40:D0:13:35:36
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)>
```

5. Set the IP address for the static lease:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)> ip 10.01.01.10
(network interface my_lan ipv4 dhcp_server advanced static_lease 0)>
```

Note The IP address here should be outside of the DHCP server's configured lease range. See Configure a DHCP server for further information about the lease range.

6. (Optional) Set a label for this static lease:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)> name label
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)>
```

7. Save the configuration and apply the change.

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 0)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show current static IP mapping

To view your current static IP mapping:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**
2. Under **Networking**, click **DHCP Leases**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Show the static lease configuration. For example, to show the static leases for a lan named **my_lan**:

```
(config)> show network interface my_lan ipv4 dhcp_server advanced static_lease
0
   ip 192.168.2.10
   mac BF:C3:46:24:0E:D9
   no name
1
   ip 192.168.2.11
   mac E3:C1:1F:65:C3:0E
   no name
(config)>
```

4. Type **cancel** to exit configuration mode:

```
(config)> cancel
>
```

5. Type exit to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete static IP mapping entries

To delete a static IP entry:

Web

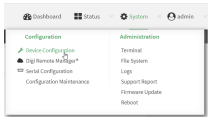
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

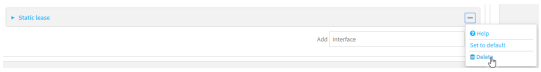
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Click to expand an existing LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Static leases**.
6. Click the menu icon (**...**) next to the name of the static lease to be deleted and select **Delete**.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Show the static lease configuration. For example, to show the static leases for a lan named **my_lan**:

```
(config)> show network interface my_lan ipv4 dhcp_server advanced static_lease
0
   ip 192.168.2.10
   mac BF:C3:46:24:0E:D9
   no name
1
   ip 192.168.2.11
   mac E3:C1:1F:65:C3:0E
   no name
(config)>
```

4. Use the **del *index_number*** command to delete a static lease. For example, to delete the static lease for the device listed in the above output with a mac address of BF:C3:46:24:0E:D9 (index number **0**):

```
(config)> del network interface lan1 ipv4 dhcp_server advanced static_lease 0
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure DHCP options

You can configure DHCP servers running on your IX10 device to send certain specified DHCP options to DHCP clients. You can also set the user class, which enables you to specify which specific DHCP clients will receive the option. You can also force the command to be sent to the clients.

DHCP options can be set on a per-LAN basis, or can be set for all LANs. A total of 32 DHCP options can be configured.

Required configuration items

- DHCP option number.
- Value for the DHCP option.

Additional configuration items

- The data type of the value.
- Force the option to be sent to the DHCP clients.
- A label for the custom option.

Web

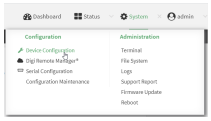
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Click to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Custom DHCP option**.
6. For **Add Custom option**, click .

   Custom options are enabled by default. To disable, toggle off **Enable**.
7. For **Option number**, type the DHCP option number.
8. For **Value**, type the value of the DHCP option.
9. (Optional) For **Label**, type a label for the custom option.
10. (Optional) If **Forced send** is enabled, the DHCP option will always be sent to the client, even if the client does not ask for it.
11. (Optional) For **Data type**, select the data type that the option uses. If the incorrect data type is selected, the device will send the value as a string.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a custom DHCP option to the DHCP server configuration for an existing LAN. For example, to add static lease to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_server advanced custom_option end
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

   See Configure a LAN for information about creating a LAN.
4. Custom options are enabled by default. To disable:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> enable false
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

5. Set the option number for the DHCP option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> option 210
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

6. Set the value for the DHCP option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> value_str value
(network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

7. (Optional) Set a label for this custom option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> name label
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

8. (Optional) To force the DHCP option to always be sent to the client, even if the client does not ask for it:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> force true
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

9. (Optional) Set the data type that the option uses.

   If the incorrect data type is selected, the device will send the value as a string.

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> datatype value
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

   where *value* is one of:

   - **1byte**
   - **2byte**
   - **4byte**
   - **hex**
   - **ipv4**
   - **str**

   The default is **str**.

10. Save the configuration and apply the change.

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option 0)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure DHCP relay

DHCP relay allows a router to forward DHCP requests from one LAN to a separate DHCP server, typically connected to a different LAN.

For the IX10 device, DHCP relay is configured by providing the IP address of a DHCP relay server, rather than an IP address range. If both the DHCP relay server and an IP address range are specified, DHCP relay is used, and the specified IP address range is ignored.

Multiple DHCP relay servers can be provided for each LAN. If multiple relay servers are provided, DHCP requests are forwarded to all servers without waiting for a response. Clients will typically use the IP address from the first DHCP response received.

Configuring DHCP relay involves the following items:

Required configuration items

- Disable the DHCP server, if it is enabled.
- IP address of the primary DHCP relay server, to define the relay server that will respond to DHCP requests.

Additional configuration items

- IP address of additional DHCP relay servers.

Web

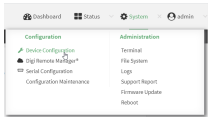
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Click to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Disable the DHCP server, if it is enabled:
   a. Click to expand **IPv4** > **DHCP server**.
   b. Click **Enable** to toggle off the DHCP server.
6. Click to expand **DHCP relay**.
7. For **Add DHCP Server:**, click .
8. For **DHCP server address**, type the IP address of the relay server.
9. Repeat for each additional DHCP relay server.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a DHCP relay server to an existing LAN. For example, to add a server to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_relay end
(config network interface lan1 my_lan dhcp_relay 0)>
```

   See Configure a LAN for information about creating a LAN.
4. Set the IP address of the DHCP relay server:

```
(config network interface my_lan ipv4 dhcp_relay 0)> address 10.10.10.10
(config network interface my_lan ipv4 dhcp_relay 0)>
```

5. (Optional) Add additional DHCP relay servers:
   a. Move back one step in the configuration schema by typing two periods (**..**):

```
(config network interface my_lan ipv4 dhcp_relay 0)> ..
(config network interface my_lan ipv4 dhcp_relay)>
```

   b. Add the next server:

```
(config network interface lan1 ipv4 dhcp_relay)> add end
(config network interface lan1 ipv4 dhcp_relay 1)>
```

   c. Set the IP address of the DHCP relay server:

```
(config network interface my_lan ipv4 dhcp_relay 1)> address 10.10.10.11
(config network interface my_lan ipv4 dhcp_relay 1)>
```

   d. Repeat for each additional relay server.

1. Disable the DHCP server, if it is enabled:

```
(config network interface my_lan ipv4 dhcp_relay 1)> .. .. dhcp_server enable false
(config network interface my_lan ipv4 dhcp_relay 1)>
```

6. Save the configuration and apply the change.

```
(config network interface lan1 ipv4 dhcp_relay 1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show DHCP server status and settings

View DHCP status to monitor which devices have been given IP configuration by the IX10 device and to diagnose DHCP issues.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**
2. Under **Networking**, click **DHCP Leases**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the show dhcp-lease command at the Admn CLI prompt:

```
> show dhcp-lease

 IP Address    Hostname       Expires
 ------------- ---------------- -------
 192.168.2.194  MTK-ENG-USER1
 192.168.2.195  MTK-ENG-USER2

 >
```

3. Additional information can be returned by using the show dhcp-lease verbose command:

```
> show dhcp-lease verbose

 IP Address    Hostname     Expires                Type    Active  MAC Address
 ------------- --------     ------------------------ ------- ------ -----------------
 192.168.2.194  MTK-ENG-USER1 May 19 08:25:11 UTC 2021  Dynamic  Yes    ba:ba:2c:13:8c:71
 192.168.2.195  MTK-ENG-USER2 May 20 11:32:12 UTC 2021  Dynamic  Yes    09:eb:10:f0:bc:16

 >
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Virtual LANs (VLANs)

Virtual LANs (VLANs) allow splitting a single physical LAN into separate Virtual LANs. Each device on a VLAN can only access other devices on the same VLAN and each device is unaware of any other

VLAN, which isolates networks from one another, even though they run over the same physical network.

Your IX10 device supports two VLANs modes:

- Trunking: Supports multiple VLANs per Ethernet port, which enables you to extend your VLAN across multiple switches through your entire network.
- Switchport: Each Ethernet port can have one or more VLAN IDs associated to it. Any un-tagged VLAN packets that come into a network interface are automatically tagged with the primary VLAN ID for that switchport. This allows devices on the network that aren't configured with a VLAN to act as if they are directly connected to the VLAN.

This section contains the following topics:

Create a trunked VLAN route 195
Create a VLAN using switchport mode 196

Create a trunked VLAN route

Required configuration items

- Device to be assigned to the VLAN.
- The VLAN ID. The TCP header uses the VLAN ID to identify the destination VLAN for the packet.

To create a VLAN:

Web

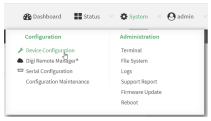
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Virtual LAN**.
4. Type a name for the VLAN and click ♈.
5. Select the **Device**.
6. Type or select a unique numeric **ID** for the VLAN ID.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the VLAN:

```
(config)> add network vlan name
(config)>
```

4. Set the device to be used by the VLAN:
   a. View a list of available devices:

```
(config network vlan vlan1)> device ?

Device: The Ethernet device to use for this virtual LAN
Format:

 /network/device/loopback
 /network/vlan/vlan1
Current value:

(config network vlan vlan1)>
```

   b. Add the device:

```
(config network vlan vlan1)> device /network/device/
(config network vlan vlan1)>
```

5. Set the VLAN ID:

```
(config network vlan vlan1)> id value
```

   where *value* is an integer between **1** and **4095**.

6. Save the configuration and apply the change.

```
(config network vlan vlan1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Create a VLAN using switchport mode

Required configuration items

- Device to be assigned to the VLAN.
- The VLAN ID. The TCP header uses the VLAN ID to identify the destination VLAN for the packet.

To create a VLAN using switchport mode:

Web

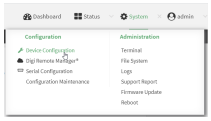
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Bridges**.
4. For **Add Bridge**, type a name for the bridge and click .
5. Bridges are enabled by default. To disable, toggle off **Enable**.
6. For **Bridge type**, select **Switchport**.
7. (Optional) Enable Spanning Tree Protocol (STP).

   STP is used when using multiple LANs on the same device, to prevent bridge loops and other routing conflicts.

   a. Click **STP**.
   b. Click **Enable**.
   c. For **Forwarding delay**, enter the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data. The default is **2** seconds.
8. For **Port**, type a name for the VLAN port and click . Generally, numbers are used for VLAN ports.
9. Select the **Device** that the port uses.
10. Configure Vlan IDs:

    a. Click to expand **Vlan IDs**.
    b. Click for **Add Vlan ID**.
    c. Type or select a unique numeric **Vlan ID**.
    d. Click for **Add Vlan ID** again to add additional VLAN IDs.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the VLAN:

```
(config)> add network vlan name
(config)>
```

4. Set the device to be used by the VLAN:
   a. View a list of available devices:

```
(config network vlan vlan1)> device ?

Device: The Ethernet device to use for this virtual LAN
Format:

 /network/device/loopback
 /network/vlan/vlan1
Current value:

(config network vlan vlan1)>
```

   b. Add the device:

```
(config network vlan vlan1)> device /network/device/
(config network vlan vlan1)>
```

5. Set the VLAN ID:

```
(config network vlan vlan1)> id value
```

   where *value* is an integer between **1** and **4095**.
6. Save the configuration and apply the change.

```
(config network vlan vlan1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status and statistics

You can show SureLink status for all interfaces, or for an individual interface. You can also show Surelink status for ipsec tunnels and OpenVPN clients.

SureLink status is only available from the Admin CLI.

Command line

Show SureLink State

To show the current state of SureLink for the IX10 device, use the show surelink state command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type:

```
> show surelink state

Test on network.interface.eth1.ipv6 with condition: one
dns_configured (n);

network.interface.eth1.ipv6;  -> update_routing_table
 ACTION           ATTEMPTS    STATUS
 restart_interface    00/01     [FAILED]
 update_routing_table 00/01

Test on network.interface.modem.ipv4 with condition: all
dns_configured (n);

network.interface.modem.ipv4;  -> restart_interface
 ACTION           ATTEMPTS    STATUS
 update_routing_table 00/03     [ BUSY ]
 restart_interface    00/03
 reset_modem          00/03
 switch_sim           00/03
 modem_power_cycle    00/03
 restart_interface    00/03

>
```

Show SureLink status for all interfaces

To show the SureLink status all interfaces, use the show surelink interface all command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type :

```
> show surelink interface all

Interface  Test                        Proto  Last Response  Status
---------  ----------------------------- -----  -------------  -------
eth1       Interface is up             IPv4   32 seconds     Passing
eth1       Interface's DNS servers (DNS)  IPv4   28 seconds     Passing
eth        Interface is up             IPv4   21 seconds     Passing
eth        Interface's DNS servers (DNS)  IPv4   20 seconds     Passing
modem      Interface is up             IPv4   115 seconds    Passing
modem      Interface's DNS servers (DNS)  IPv4   114 seconds    Passing

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status for a specific interface

To show the SureLink status a specific interface, use the show surelink interface name *name* command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show surelink interface name *name* command to show the Surelink status of a specific interface, for example:

```
> show surelink interface name eth1

wan1 Surelink Status
--------------------
IPv4 Status : Passing
IPv6 Status : Failed

Test                        Proto  Last Response  Status
----------------------------- -----  -------------  ------
Interface's DNS servers (DNS)  IPv6   15 seconds     Failed

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status for all IPsec tunnels

To show the SureLink status all IPsec tunnels, use the show surelink ipsec all command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type :

```
> show surelink ipsec all

IPsec  Test               Last Response  Status
------ ------------------- ------------- ------------------
test   194.43.79.74 (Ping)  29 seconds    Passed
test   194.43.79.75 (Ping)  5 seconds     Passed
test1  194.43.79.74 (Ping)  21 seconds    Failed
test2  194.43.79.75 (Ping)  21 seconds    Waiting for result

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status for a specific IPsec tunnel

To show the SureLink status a specific IPsec tunnel, use the show surelink ipsec tunnel *name* command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show surelink ipsec tunnel *name* command to show the Surelink status of a specific tunnel, for example:

```
> show surelink ipsec tunnel test

IPsec  Test               Last Response  Status
------ ------------------- ------------- ------------------
test   194.43.79.74 (Ping)  29 seconds    Passed
test   194.43.79.75 (Ping)  5 seconds     Passed

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status for all OpenVPN clients

To show the SureLink status all OpenVPN clients, use the show surelink openvpn client all command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type :

```
> show surelink openvpn all

 OpenVPN Client   Test               Last Response  Status
 --------------- -------------------- ------------- ------------------
 test_client1    194.43.79.74 (Ping)  29 seconds    Passed
 test_client1    194.43.79.75 (Ping)  5 seconds     Passed
 test_client2    194.43.79.74 (Ping)  21 seconds    Failed
 test_client2    194.43.79.75 (Ping)  21 seconds    Waiting for result

 >
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SureLink status for a specific OpenVPN client

To show the SureLink status a specific OpenVPN client, use the show surelink openvpn client *name* command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show surelink openvpn client *name* command to show the Surelink status of a specific OpenVPN client, for example:

```
> show surelink openvpn client test_client1

 OpenVPN Client   Test               Last Response  Status
 --------------- -------------------- ------------- ------------------
 test_client1    194.43.79.74 (Ping)  29 seconds    Passed
 test_client1    194.43.79.75 (Ping)  5 seconds     Passed

 >
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Serial port

IX10 devices have a single serial port that provides access to different features, depending on the serial port mode selection.

Default serial port configuration

You can review the default serial port configuration for your device.

Serial mode options

You can choose a serial mode option for each serial port, depending on the feature that you want to use.

- Login: Allows the port to be used to log into the CLI.
- Remote Access: Provides socket level access to ports.
- Application: Provides access to the serial device from Python applications.
- PPP dial-in: Allows the device to answer Point-to-Point Protocol (PPP) connections over serial ports.
- RealPort: Used in conjunction with the Digi RealPort driver.
- UDP serial: Provides access to the serial port using UDP.
- Modem emulator: Allows the device to act as a dial-up modem emulator for handling incoming AT dial-ins.
- Modbus: Allows the device to function as a Modbus protocol gateway.

View serial port information

- Show serial port status and statistics
- Review the serial port message log

Default serial port configuration

The IX10 default serial port configuration is:

- **Enabled**
- **Serial mode**: Remote Access
- **Label**: None
- **Baud rate**: 9600

- **Data bits**: 8
- **Parity**: None
- **Stop bits**: 1
- **Flow control**: None

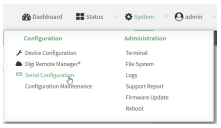
Configure Login mode for a serial port

Login mode allows the user to log into the device through the serial port.

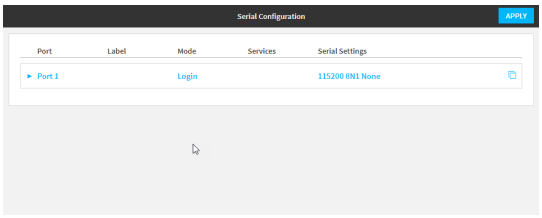
To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

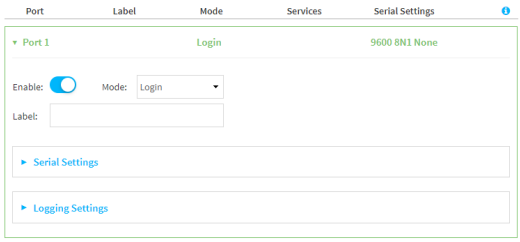


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **Login**. This is the default.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:

- **RS-232**
- **RS-485**
  - Enable **Termination** if you want to enable electrical termination on this serial port.

The default is **RS-232**.

7. Expand **Serial Settings**.

   The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

   a. **Baud rate**: For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.

   b. **Data bits**: For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.

   c. **Parity**: For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.

   d. **Stop bits**: For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.

   e. **Flow control**: For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.

8. Expand **Logging Settings** to configure logging for this serial port.

   a. To enable logging, click to toggle on **Enable**.

   b. In the **Log file name** field, enter a descriptive name for the log file.

   c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.

   d. From the **Type of data to log** list box, specify the type of data that should be saved.

      - **Received**
      - **Transmitted**
      - **Both**
      - **Both with arrows**. This is the default.

   e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.

   f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

   > **Note** You can review the message log in the **Serial Port Log** page. See Review the serial port message log.

9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode login
(config)>
```

5. Set the signaling interface type used on this serial port:
   - **rs-232**
   - **rs-485**
     - Enable **termination** if you want to enable electrical termination on this serial port:

```
(config)> serial port1 termination true
(config)>
```

   The default is **rs-232**.
6. (Optional) Set a label that will be used when referring to this port.

```
(config)>path-paramlabel label
(config)>
```

7. Set the baud rate used by the device to which you want to connect:

```
(config)> serial port1 baudrate rate
(config)>
```

8. Set the number of data bits used by the device to which you want to connect:

```
(config)> serial port1 databits bits
(config)>
```

9. Set the type of parity used by the device to which you want to connect:

```
(config)> serial port1 parity parity
(config)>
```

   Allowed values are:
   - **even**
   - **odd**
   - **none**

   The default is **none**.

10. Set the stop bits used by the device to which you want to connect:

```
(config)> serial port1 stopbits bits
(config)>
```

11. Set the type of flow control used by the device to which you want to connect:

```
(config)> serial port1 flow value
(config)>
```

where value is one of:

- **none**
- **rts/cts**
- **xon/xoff**

12. Configure serial port logging:
    a. Enable serial port logging:

```
(config)>serial port1 logging enable true
(config)>
```

    b. Set the file name:

```
(config)>serial port1 logging filename string
(config)>
```

    c. Set the maximum allowed log size for the serial port log when starting the log:

```
(config)>serial port1 logging size value
(config)>
```

    where *value* is the size of the log file in bytes. The default is **65536**.
    d. Specify the data type:

```
(config)>serial port1 logging type value
(config)>
```

    where *value* is one of:
    - received
    - transmitted
    - both
    - arrows. This is the default.

    e. Log the time at which date was received or transmitted:

```
(config)>serial port1 logging hex true
(config)>
```

    f. Log data as hexadecimal values:

```
(config)>serial port1 logging timestamp true
(config)>
```

13. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

14. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

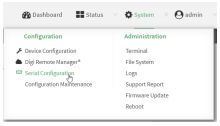
Configure Remote Access mode for a serial port

Remote Access mode allows for remote access to another device that is connected to the serial port.

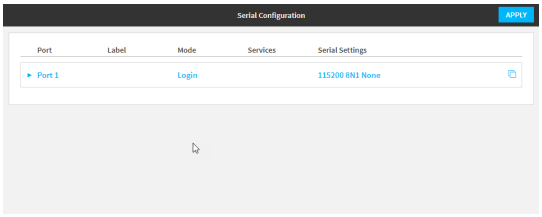
To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

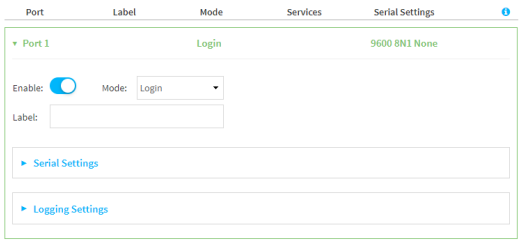


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Serial mode**, select **Remote access (TCP)**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
   - **RS-485**
     - Enable **Termination** if you want to enable electrical termination on this serial port.

   The default is **RS-232**.
7. Expand **Serial Settings**.

   The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

   a. **Baud rate**: For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.

   b. **Data bits**: For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.

   c. **Parity**: For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.

   d. **Stop bits**: For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.

   e. **Flow control**: For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
8. Click to expand **Data Framing**.

   a. Click **Enable** to enable the data framing feature.

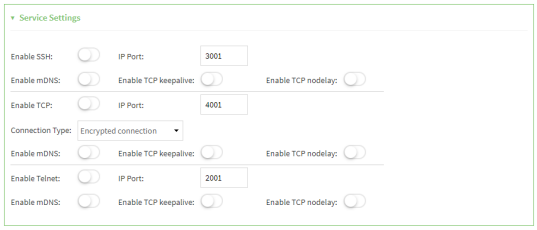
   b. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.

   c. For **Idle Time**, enter the length of time the device should wait before sending the packet.

   d. For **End Pattern**, enter the end pattern. The packet is sent when this pattern is received from the serial port.

   e. Click **Strip End Pattern** if you want to remove the end pattern from the packet before it is sent.
9. Expand **Service Settings**.

   All service settings are disabled by default. Click available options to toggle them to enabled, and set the IP ports as appropriate.



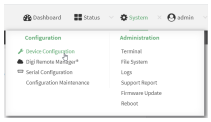
Note If the Telnet service is enabled for the serial port, note that the **Telnet Login** option, when enabled, prompts the user to enter Telnet login credentials when accessing the serial

port via Telnet. The **Telnet Login** option is enabled by default. To disable this option, navigate to **System** > **Device Configuration** > **Authentication** > **Serial** and disable **Telnet Login**.

For each type of service, you can also configure the access control.

To do this, you need to go to **Device Configuration**:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

b. Access the configuration for the appropriate type of service:

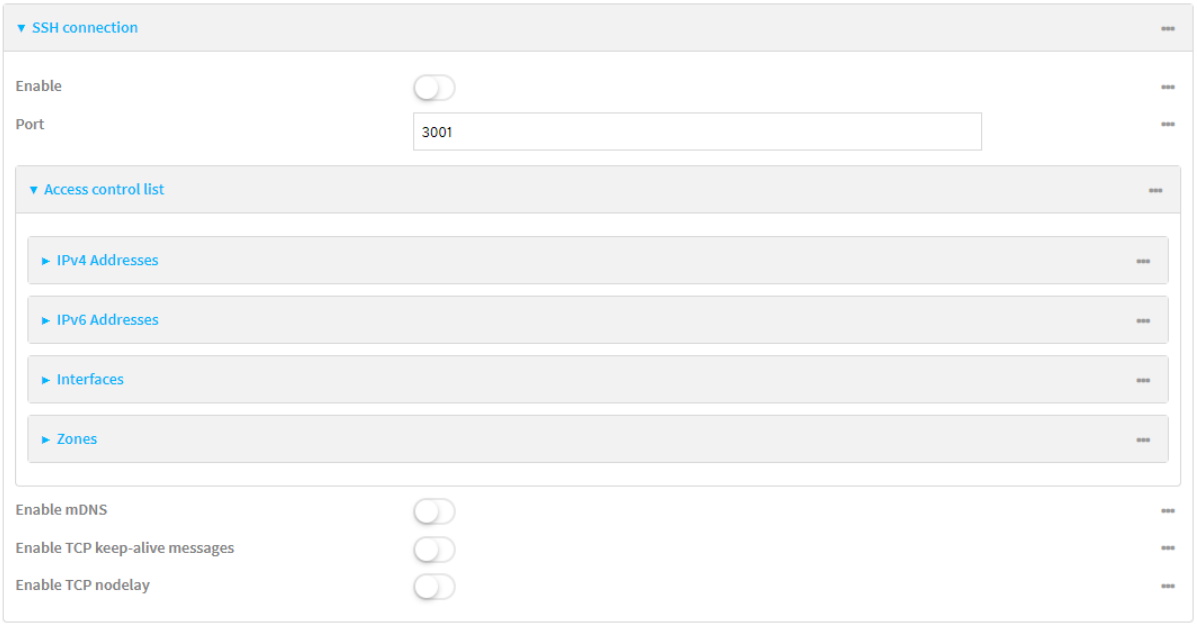
i. Click to expand **Serial**.

ii. Click to expand the appropriate serial port.

iii. Click to expand the appropriate type of service.

iv. Click to expand **Access Control List**.

For example, to set the Access Control List for the SSH connection for serial port 1, click to expand **Serial** > **Port 1** > **SSH connection** > **Access Control List**:



- To limit access to specified IPv4 addresses and networks:

i. Click **IPv4 Addresses**.

ii. For **Add Address**, click ♈.

iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

iv. Click again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
  i. Click **IPv6 Addresses**.
  ii. For **Add Address**, click .
  iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
    - A single IP address or host name.
    - A network designation in CIDR notation, for example, 2001:db8::/48.
    - **any**: No limit to IPv6 addresses that can access the service-type.

  iv. Click again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  i. Click **Interfaces**.
  ii. For **Add Interface**, click .
  iii. For **Interface**, select the appropriate interface from the dropdown.
  iv. Click again to allow access through additional interfaces.
- To limit access based on firewall zones:
  i. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  ii. For **Add Zone**, click .
  iii. For **Zone**, select the appropriate firewall zone from the dropdown.

  See Firewall configuration for information about firewall zones.
  iv. Click again to allow access through additional firewall zones.

10. Expand **Autoconnect Settings**. The autoconnect feature is used to initiate a connection to a remote server to directly access the serial port.
    a. Click **Enable** to enable the autoconnect feature.
    b. For **Connection Trigger**, select the option that describes the type of event that should trigger the connection.

    If you select the **Data received matches a string** option, additional fields display.
      a. In the **Data Match String** field, enter the received data string that should trigger the connection. The syntax is: *backslash escaped string*
      b. The **Flush String** option determines whether the match string data sent from the remote server is discarded.
        - **Enable**: Discard the match string data. This is the default.
        - **Disable**: Do not discard the match string data.

    c. For **Outbound Connection Type**, select the option that describes the method used to initiate the connection.
    d. For **Destination**, enter the host name or IP address of the remote server. When using SSH, this should be prefixed with the user name and followed by @, for example,

admin@192.168.1.1.

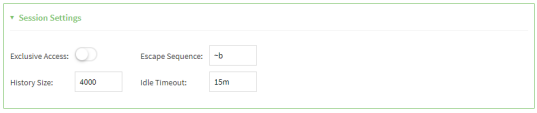
e. For **IP port**, enter the TCP port of the remote server (1-65535).

f. Click **Enable TCP keep-alive** to enable TCP keepalive on the connection.

g. Click **Enable TCP nodelay** to enable TCP nodelay on the connection.

h. For **Socket ID string**, type text to be transmitted to the remote server when the socket connects.

11. Expand **Session Settings**.



a. Enable **Exclusive access** to limit access to the serial port to a single active session. This option is disabled by default. When it is disabled, multiple users can connect using Telnet, TCP, and SSH.

b. For **Escape sequence**, type the characters used to start an escape sequence. If no characters are defined, the escape sequence is disabled. The default is **~b**.

c. For **History size**, type or select the number of bytes of output from the serial port that are written to buffer. These bytes are redisplayed when a user connects to the serial port. The default is **4000** bytes.

d. For **Idle timeout**, type the amount of time to wait before disconnecting due to user inactivity.

12. Expand **Monitor Settings**.

a. Enable **CTS** to monitor CTS (Clear to Send) changes on this port.

b. Enable **DCD** to monitor DCD (Data Carrier Detect) changes on this port.

13. Expand **Logging Settings** to configure logging for this serial port.

a. To enable logging, click to toggle on **Enable**.

b. In the **Log file name** field, enter a descriptive name for the log file.

c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.

d. From the **Type of data to log** list box, specify the type of data that should be saved.

- **Received**
- **Transmitted**
- **Both**
- **Both with arrows**. This is the default.

e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.

f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

> **Note** You can review the message log in the **Serial Port Log** page. See Review the serial port message log.

14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```
3. Serial ports is enabled by default. To disable:

   ```
   (config)> serial port_number enable false
   (config)>
   ```

   Command line examples in this section will use port1 for the serial port. However, any port number can be used.
4. Set the mode:

   ```
   (config)> serial port1 mode remoteaccess
   (config)>
   ```
5. Set the signaling interface type used on this serial port:
   - **rs-232**
   - **rs-485**
     - Enable **termination** if you want to enable electrical termination on this serial port:

       ```
       (config)> serial port1 termination true
       (config)>
       ```

   The default is **rs-232**.
6. (Optional) Set a label that will be used when referring to this port.

   ```
   (config)>serial port1 label label
   (config)>
   ```
7. Set the baud rate used by the device to which you want to connect:

   ```
   (config)> serial port1 baudrate rate
   (config)>
   ```
8. Set the number of data bits used by the device to which you want to connect:

   ```
   (config)> serial port1 databits bits
   (config)>
   ```
9. Set the type of parity used by the device to which you want to connect:

   ```
   (config)> serial port1 parity parity
   (config)>
   ```

Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

10. Set the stop bits used by the device to which you want to connect:

```
(config)> serial port1 stopbits bits
(config)>
```

11. Set the type of flow control used by the device to which you want to connect:

```
(config)> serial port1 flow value
(config)>
```

where value is one of:

- **none**
- **rts/cts**
- **xon/xoff**

12. Configure the session settings.
    a. Set the characters used to start an escape sequence:

```
(config)>serial port1 escape string
(config)
```

If no characters are defined, the escape sequence is disabled. The default is **~b**.

    b. Limit access to the serial port to a single active session:

```
(config)>serial port1 exclusive true
(config)
```

    c. Set the number of bytes of output from the serial port that are written to buffer. These bytes are redisplayed when a user connects to the serial port.

```
(config)>serial port1 history bytes
(config)
```

The default is **4000** bytes.

    d. Set the amount of time to wait before disconnecting due to user inactivity:

```
(config)>serial port1 idle_timeout value
(config)
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **idle_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)>serial port1 idle_timeout 600s
(config)
```

The default is **15m**.

13. Configure monitor settings.
    a. (Optional) Enable monitoring of CTS (Clear to Send) changes on this port:

```
(config)>serial port1 monitor cts true
(config)
```

    b. (Optional) Enable monitoring of DCD (Data Carrier Detect) changes on this port:

```
(config)>serial port1 monitor dcd true
(config)
```

14. (Optional) Configure autoconnect:
    a. Enable autoconnect:

```
(config)>serial port1 autoconnect enable true
(config)>
```

    b. Set the option that will trigger the connection:

```
(config)>serial port1 autoconnect trigger value
(config)>
```

    where *value* is one of:
    - **always**
    - **data**
    - **dcd**
    - **destination**
    - **dsr**
    - **match**

      If **match** is selected:
      i. Set the string that, when received, will trigger the connection:

```
(config)>serial port1 autoconnect match_string string
(config)>
```

      ii. **flush_string** is enabled by default, which will discard the matched string from data sent to the server. To disable:

```
(config)>serial port1 autoconnect flush_string false
(config)>
```

    The default is **always**.
    c. Set the option that initiates the connection:

```
(config)>serial port1 autoconnect conn_type value
(config)>
```

where *value* is one of:

- **ssh**
- **tcp**
- **telnet**
- **tls**
- **tls_auth**

The default is **tls**.

d. Set the host name or IP address of the destination server:

```
(config)>serial port1 autoconnect destination hostname/IP_address
(config)>
```

When using SSH, this should be prefixed with the user name and followed by @, for example:

```
(config)>serial port1 autoconnect destination admin@192.168.1.1
(config)>
```

e. Set the TCP port of the destination server:

```
(config)>serial port1 autoconnect port int
(config)>
```

where *int* is any integer between **1** and **65535**.

f. To enable TCP keepalive:

```
(config)>serial port1 autoconnect keepalive true
(config)>
```

g. To enable TCP nodelay:

```
(config)>serial port1 autoconnect nodely true
(config)>
```

h. Set the text to be transmitted to the remote server when the socket connects:

```
(config)>serial port1 socketid string
(config)>
```

15. (Optional) Configure data framing:

a. Enable data framing:

```
(config)>serial port1 framing enable true
(config)
```

b. Set the maximum size of the packet:

```
(config)>serial port1 framing max_count int
(config)
```

The default is **1024**.

c. Set the length of time the device should wait before sending the packet:

```
(config)>serial port1 framing idle_time value
(config)
```

where *value* is in milliseconds (ms) or seconds (s). The maximum value is **60s**.

d. Set the end pattern. The packet is sent when this pattern is received from the serial port:

```
(config)>serial port1 framing end_pattern backslash-escaped-string
(config)
```

e. Set the strip end pattern if you want to remove the end pattern from the packet before it is sent:

```
(config)>serial port1 framing strip_pattern true
(config)
```

16. (Optional) Configure service settings:
    a. Configure SSH settings:
        i. Enable SSH:

```
(config)>serial port1 service ssh enable true
(config)>
```

        ii. Set the port to be used for ssh communications:

```
(config)>serial port1 service ssh port int
(config)>
```

where *int* is any integer between **1** and **65535**. The default is **3001**.

        iii. Enable TCP keep-alive messages:

```
(config)>serial port1 service ssh keepalive true
(config)>
```

        iv. Enable TCP nodelay messages:

```
(config)>serial port1 service ssh nodelay true
(config)>
```

        v. (Optional) Configure access control:
            - To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 service ssh acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 service ssh acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add serial port1 service ssh acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add serial port1 service ssh acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to
```

```
by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

vi. (Optional) Enable Multicast DNS (mDNS):

```
(config)>serial port1 service ssh mdns enable true
(config)>
```

b. Configure TCP settings:

i. Enable TCP:

```
(config)>serial port1 service tcp enable true
(config)>
```

ii. Set the port to be used for ssh communications:

```
(config)>serial port1 service tcp port int
(config)>
```

where *int* is any integer between **1** and **65535**. The default is **4001**.

iii. Enable TCP keep-alive messages:

```
(config)>serial port1 service tcp keepalive true
(config)>
```

iv. Set the option that initiates the connection:

```
(config)>serial port1 service tcp conn_type value
(config)>
```

where *value* is one of:

- **tcp**
- **tls**
- **tls_auth**

The default is **tls**.

v. Enable TCP nodelay messages:

```
(config)>serial port1 service tcp nodelay true
(config)>
```

vi. (Optional) Configure access control:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 service tcp acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 service tcp acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add serial port1 service tcp acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add serial port1 service tcp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to
by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

vii. (Optional) Enable Multicast DNS (mDNS):

```
(config)>serial port1 service tcp mdns enable true
(config)>
```

c. Configure telnet settings:

i. Enable Telnet:

```
(config)>serial port1 service telnet enable true
(config)>
```

ii. Set the port to be used for Telnet communications:

```
(config)>serial port1 service telnet port int
(config)>
```

where *int* is any integer between **1** and **65535**. The default is **3001**.

iii. Enable TCP keep-alive messages:

```
(config)>serial port1 service telnet keepalive true
(config)>
```

iv. Enable TCP nodelay messages:

```
(config)>serial port1 service telnet nodelay true
(config)>
```

v. (Optional) Configure access control:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 service telnet acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 service telnet acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add serial port1 service telnet acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
----------------------------------------
setupip          Setup IP
setuplinklocalip      Setup Link-local IP
```

```
eth             ETH
loopback        Loopback
modem           Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add serial port1 service telnet acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to
by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

vi. (Optional) Enable Multicast DNS (mDNS):

```
(config)>serial port1 service telnet mdns enable true
(config)>
```

17. Configure serial port logging:
    a. Enable serial port logging:

```
(config)>serial port1 logging enable true
(config)>
```

    b. Set the file name:

```
(config)>serial port1 logging filename string
(config)>
```

c. Set the maximum allowed log size for the serial port log when starting the log:

```
(config)>serial port1 logging size value
(config)>
```

where *value* is the size of the log file in bytes. The default is **65536**.

d. Specify the data type:

```
(config)>serial port1 logging type value
(config)>
```

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

e. Log the time at which date was received or transmitted:

```
(config)>serial port1 logging hex true
(config)>
```

f. Log data as hexadecimal values:

```
(config)>serial port1 logging timestamp true
(config)>
```

18. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

19. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

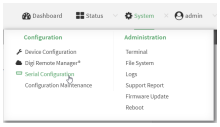
Configure Application mode for a serial port

Application mode provides access to the serial device from Python applications.

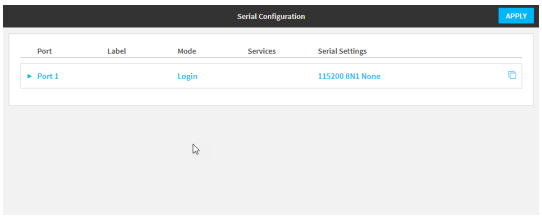
To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

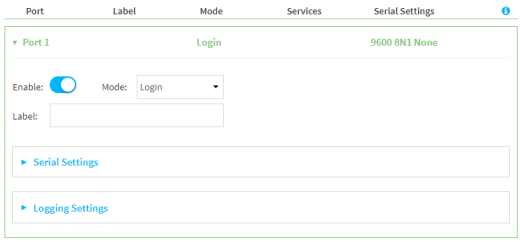


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **Application**. The default is **Remote Access**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
   - **RS-485**
     - Enable **Termination** if you want to enable electrical termination on this serial port.

   The default is **RS-232**.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode application
(config)>
```

5. Set the signaling interface type used on this serial port:
   - **rs-232**
   - **rs-485**
     - Enable **termination** if you want to enable electrical termination on this serial port:

```
(config)> serial port1 termination true
(config)>
```

   The default is **rs-232**.

6. (Optional) Set a label that will be used when referring to this port.

```
(config)>path-paramlabel label
(config)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure PPP dial-in mode for a serial port

PPP dial-in allows the device to answer Point-to-Point Protocol (PPP) connections over serial ports.

To change the configuration to match the serial configuration of the device to which you want to connect:

Web

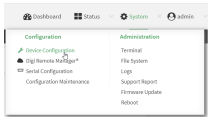
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

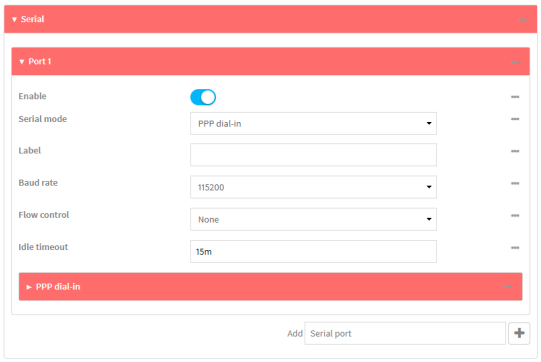


The **Configuration** window is displayed.

3. Click to expand the name of the port that you want to configure, for example, **Port 1**.

   The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **PPP-Dial-in**. The default is **Remote Access**.



5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
7. For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
8. For **Idle timeout**, type the amount of time that the active session can be idle before the session is disconnected.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.
9. Click to expand **PPP dial-in**.
10. For **Local IP address**, type the IP address assigned to this interface.
11. For **Remote IP address**, type the IP address assigned to the remote peer.
12. For **Metric**, set the priority of routes associated with this interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used.

13. For **Default route**, toggle to control whether a default route gets added for the PPP interface. This feature is disabled by default.
14. For **Zone**, select the firewall zone for this interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface.
15. For **Authentication method**, select the method used to authenticate the remote peer. Allowed values are:
    - **None**: No authentication is required.
    - **Automatic**: Attempt to authenticate using CHAP first, and then PAP.
    - **CHAP**: Use Challenge Handshake Authentication Protocol (CHAP) to authenticate.
    - **PAP**: Use Password Authentication Protocol (PAP) to authenticate.

    If Automatic, CHAP, or PAP are selected, type the **Username** and **Password** used to authenticate the remote peer.
16. (Optional) Configure the serial port to use a custom PPP configuration file:
    a. Click to expand **Custom PPP configuration**.
    b. Click **Enable** to enable the use of a custom PPP configuration file.
    c. Click **Override** to override the default PPP configuration and only use the custom configuration file.

    If **Override** is not enabled, the custom PPP configuration file is used in addition to the default configuration.
    d. For **Configuration file**, paste or type the configuration data in the format of a pppd options file. Because the options are passed directly to the pppd command line, they should all be entered on a single line. For example:

```
debug lcp-echo-interval 10 lcp-echo-failure 2
```

17. (Optional) Configure a script that will be run to prepare the link before PPP negotiations are started:
    a. Click to expand **Connect script**.
    b. Click **Enable** to enable the use of a connection script.
    c. For **Connect script filename**, type the name of the script. Scripts are located in the /etc/config/serial directory. An example script, windows_dun.sh is provided.

    Example windows_dun.sh file:

```
#!/bin/sh

# Example connect script for connecting from a PC using a Windows dial-up
# networking connection with built-in standard 33600 bps modem driver and phone
# number 123.

# The shell's 'read' builtin breaks on newline, so translate incoming carriage-
# return to newline, and outgoing newline to carriage-return-newline.
stty icrnl onlcr opost

# Read input from the serial port, one line at a time.
while read -r line; do
  case "$line" in
```

```
    ATDT123)
      echo "CONNECT" # instruct the peer to start PPP
      exit 0 # start up the local PPP session
      ;;
    AT*)
      echo "OK" # passively accept any other AT command
      ;;
  esac
done
```

18. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode ppp_dialin
(config)>
```

5. (Optional) Set a label that will be used when referring to this port.

```
(config)> serial port1  label label
(config)>
```

6. Set the baud rate used by the device to which you want to connect:

```
(config)> serial port1 baudrate rate
(config)>
```

7. Set the type of flow control used by the device to which you want to connect:

```
(config)> serial port1 flow value
(config)>
```

   where value is one of:

   - **none**
   - **rts/cts**
   - **xon/xoff**

8. Set the amount of time that the active session can be idle before the session is disconnected:

```
(config)> serial port1 idle_timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **idle_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> serial port1 idle_timeout 600s
(config)>
```

9. Set the local IP address assigned to this interface:

```
(config)> serial port1 ppp_dialin local_address IPv4_address
(config)>
```

10. Set the IP address assigned to the remote peer:

```
(config)> serial port1 ppp_dialin remote_address IPv4_address
(config)>
```

11. The default route is added for the PPP interface is disabled by default. To enable:

```
(config)> serial port1 ppp_dialin default_route true
config)>
```

12. Set the authentication method used to authenticate the remote peer:

```
(config)> serial port1 ppp_dialin auth value
(config)>
```

where *value* is one of:

- **none**: No authentication is required.
- **auto**: Attempt to authenticate using CHAP first, and then PAP.
- **chap**: Use Challenge Handshake Authentication Protocol (CHAP) to authenticate.
- **pap**: Use Password Authentication Protocol (PAP) to authenticate.

The default is **none**.

If auto, chap, or pap are set, set the username and password used to authenticate the remote peer:

```
(config)> serial port1 ppp_dialin username username
(config)> serial port1 ppp_dialin password password
(config)>
```

13. Set the priority of routes associated with this interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used.

```
(config)> serial port1 ppp_dialin metric int
(config)>
```

The default is **10**.

14. Set the firewall zone for this interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface.
    a. Use the **?** to determine available zones:

```
(config)> serial port1 ppp_dialin zone ?

Zone: The firewall zone assigned to this interface. This can be used by packet
filtering rules and access control lists to restrict network traffic on this
interface.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Default value: internal
Current value: internal

(config)>
```

    b. Set the zone:

```
(config)> serial port1 ppp_dialin zone zone
(config)>
```

15. (Optional) Configure the serial port to use a custom PPP configuration file:
    a. Enable the use of a custom PPP configuration file:

```
(config)> serial port1 ppp_dialin custom enable true
(config)>
```

    b. Enable **override** to override the default PPP configuration and only use the custom configuration file:

```
(config)> serial port1 ppp_dialin custom override true
(config)>
```

    If **override** is not enabled, the custom PPP configuration file is used in addition to the default configuration.
    c. Paste or type the configuration data in the format of a pppd options file:

```
(config)> serial port1 ppp_dialin custom config_file data
(config)>
```

    where *data* are one or more pppd command line options. Because the options are passed directly to the pppd command line, they should all be entered on a single line. For example:

```
(config)> serial port1 ppp_dialin custom config_file "debug lcp-echo-interval 10 lcp-echo-failure
2"
(config)>
```

16. (Optional) Configure a script that will be run to prepare the link before PPP negotiations are started:
    a. Enable the use of a connection script.

```
(config)> serial port1 ppp_dialin connect enable true
(config)>
```

    b. Set the name of the script:

```
(config)> serial port1 ppp_dialin connect script filename
(config)>
```

    Scripts are located in the /etc/config/serial directory. An example script, windows_dun.sh is provided.

    Example windows_dun.sh file:

```
#!/bin/sh

# Example connect script for connecting from a PC using a Windows dial-up
# networking connection with built-in standard 33600 bps modem driver and phone
# number 123.

# The shell's 'read' builtin breaks on newline, so translate incoming carriage-
# return to newline, and outgoing newline to carriage-return-newline.
stty icrnl onlcr opost

# Read input from the serial port, one line at a time.
while read -r line; do
  case "$line" in
    ATDT123)
      echo "CONNECT" # instruct the peer to start PPP
      exit 0 # start up the local PPP session
      ;;
    AT*)
      echo "OK" # passively accept any other AT command
      ;;
  esac
done
```

17. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

18. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

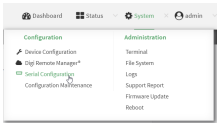
Configure UDP serial mode for a serial port

The **UDP** serial mode option in the serial port configuration provides access to the serial port using UDP.

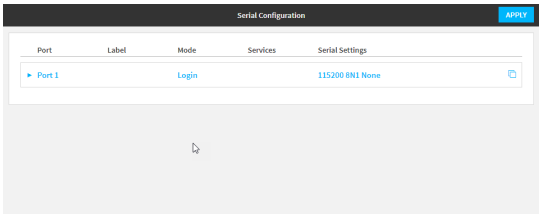
To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

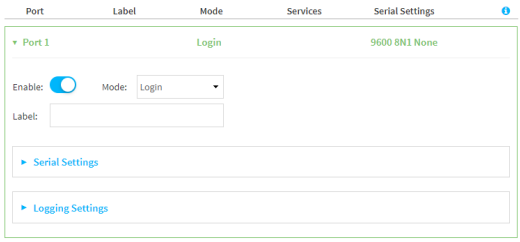


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click to expand the port that you want to configure for UDP serial mode.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **UDP serial**.

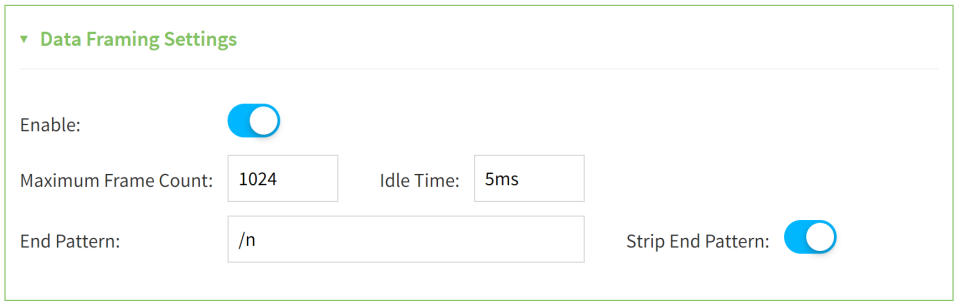
   The default is **Remote Access**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
   - **RS-485**
     - Enable **Termination** if you want to enable electrical termination on this serial port.

   The default is **RS-232**.

7. Expand **Serial Settings**.

   a. For **Baud rate**, select the baud rate used by the device to which you want to connect.
   b. For **Data bits**, select the number of data bits used by the device to which you want to connect.
   c. For **Parity**, select the type of parity used by the device to which you want to connect.
   d. For **Stop bits**, select the number of stop bits used by the device to which you want to connect.
   e. For **Flow control**, select the type of flow control used by the device to which you want to connect.

8. Expand **Data Framing Settings**.



   a. Click to expand **Data Framing**.
      i. Click **Enable** to enable the data framing feature.
      ii. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.
      iii. For **Idle Time**, enter the length of time the device should wait before sending the packet.
      iv. For **End Pattern**, enter the end pattern. The packet is sent when this pattern is received from the serial port.
      v. Click **Strip End Pattern** if you want to remove the end pattern from the packet before it is sent.

9. Expand **UDP Serial Settings**.

a. For **Local port**, enter the UDP port. The default is 4001 or serial port 1, 4002 for serial port 2, etc.

b. (Optional) For **Socket String ID**, enter a string that should be added at the beginning of each packet.

c. For **Destinations**, you can configure the remote sites to which you want to send data. If you do not specify any destinations, the IX10 sends new data from the last IP address and port from which data was received. To add a destination:

   i. Click **Add Destination**. A destination row is added.

   ii. (Optional) For **Description**, enter a description of the destination.

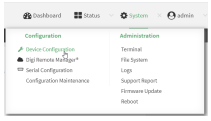
   iii. For **Hostname**, enter the host name or IP address of the remote site to which data should be sent.

   iv. For **Port**, enter the port number of the remote site to which data should be sent.

You can also configure access control for the serial port.

To do this, you need to go to **Device Configuration**:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

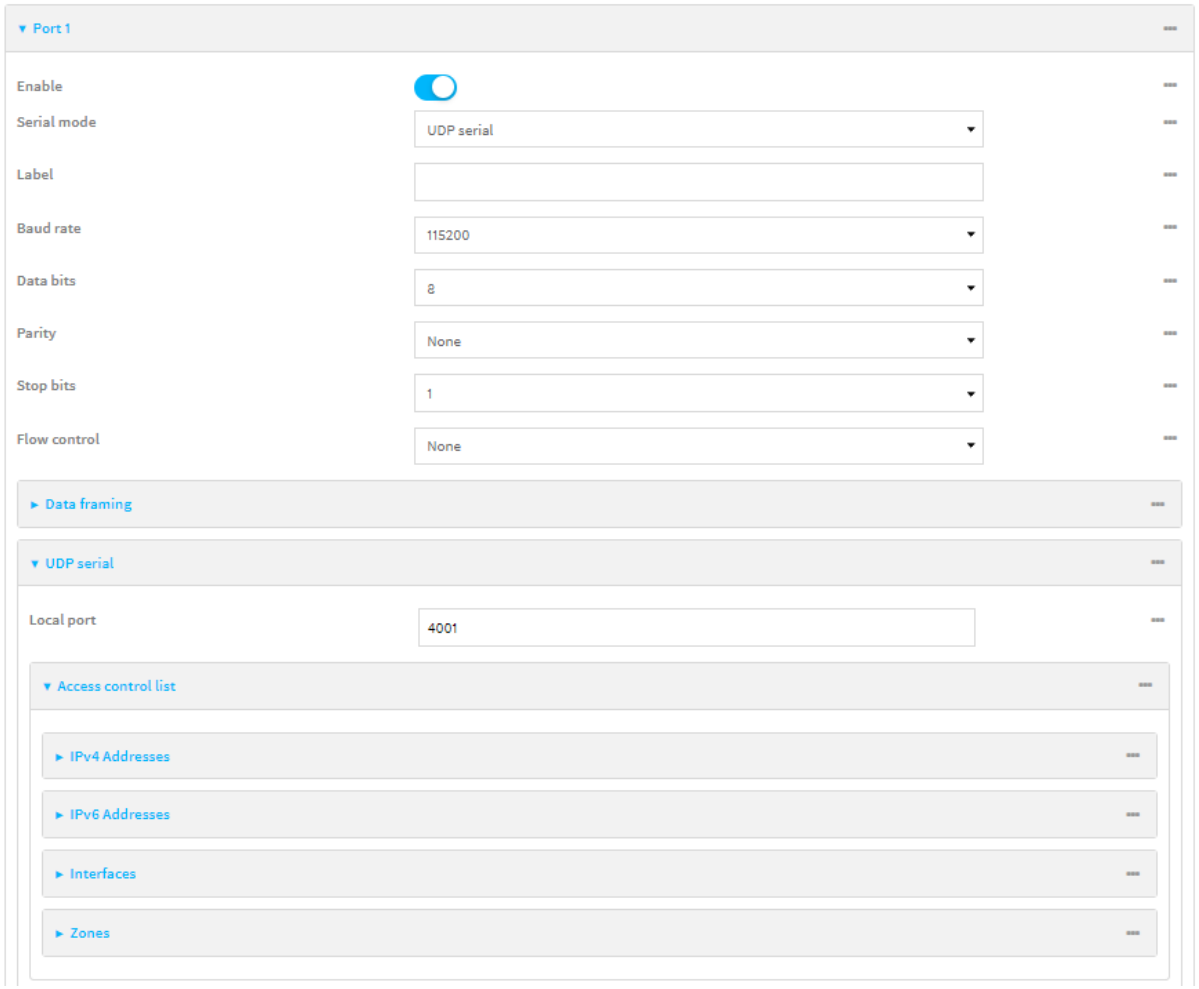
b. Access the configuration for the appropriate type of service:

   i. Click to expand **Serial**.

   ii. Click to expand the appropriate serial port.

   iii. Click to expand **UDP serial**.

   iv. Click to expand **Access Control List**.



- To limit access to specified IPv4 addresses and networks:
  i. Click **IPv4 Addresses**.
  ii. For **Add Address**, click ⋎.
  iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
    - A single IP address or host name.
    - A network designation in CIDR notation, for example, 192.168.1.0/24.
    - **any**: No limit to IPv4 addresses that can access the service-type.
  iv. Click ⋎ again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
  i. Click **IPv6 Addresses**.
  ii. For **Add Address**, click ⋎.
  iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

iv. Click again to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the device:
  i. Click **Interfaces**.
  ii. For **Add Interface**, click .
  iii. For **Interface**, select the appropriate interface from the dropdown.
  iv. Click again to allow access through additional interfaces.
- To limit access based on firewall zones:
  i. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  ii. For **Add Zone**, click .
  iii. For **Zone**, select the appropriate firewall zone from the dropdown.
  See Firewall configuration for information about firewall zones.
  iv. Click again to allow access through additional firewall zones.

10. Expand **Logging Settings** to configure logging for this serial port.
    a. To enable logging, click to toggle on **Enable**.
    b. In the **Log file name** field, enter a descriptive name for the log file.
    c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
    d. From the **Type of data to log** list box, specify the type of data that should be saved.
       - **Received**
       - **Transmitted**
       - **Both**
       - **Both with arrows**. This is the default.
    e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
    f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

    Note You can review the message log in the **Serial Port Log** page. See Review the serial port message log.

11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode udp
(config)>
```

5. Set the signaling interface type used on this serial port:
   - **rs-232**
   - **rs-485**
     - Enable **termination** if you want to enable electrical termination on this serial port:

```
(config)> serial port1 termination true
(config)>
```

   The default is **rs-232**.
6. (Optional) Set a label that will be used when referring to this port.

```
(config)>serial port1 label label
(config)>
```

7. Set the baud rate used by the device to which you want to connect:

```
(config)>serial port1 label baudrate rate
(config)>
```

8. Set the number of data bits used by the device to which you want to connect:

```
(config)>serial port1 label databits bits
(config)>
```

9. Set the type of parity used by the device to which you want to connect:

```
(config)>serial port1 label parity parity
(config)>
```

   Allowed values are:
   - **even**
   - **odd**
   - **none**

   The default is **none**.

10. Set the stop bits used by the device to which you want to connect:

```
(config)>serial port1 label stopbits bits
(config)>
```

11. Set the type of flow control used by the device to which you want to connect:

```
(config)>serial port1 label flow type
(config)
```

Allowed values are:

- **none**
- **rts/cts**
- **xon/xoff**

The default is **none**.

12. (Optional) Configure data framing:
    a. Enable data framing:

```
(config)>serial port1 framing enable true
(config)
```

    b. Set the maximum size of the packet:

```
(config)>serial port1 framing max_count int
(config)
```

    The default is **1024**.
    c. Set the length of time the device should wait before sending the packet:

```
(config)>serial port1 framing idle_time value
(config)
```

    where *value* is in milliseconds (ms) or seconds (s). The maximum value is **60s**.
    d. Set the end pattern. The packet is sent when this pattern is received from the serial port:

```
(config)>serial port1 framing end_pattern backslash-escaped-string
(config)
```

    e. Set the strip end pattern if you want to remove the end pattern from the packet before it is sent:

```
(config)>serial port1 framing strip_pattern true
(config)
```

13. Set the UDP port:

```
(config)> serial port1 udp port port
(config)>
```

The default is **4001**.

14. (Optional) Enter a string that should be added at the beginning of each packet:

```
(config)> serial port1 udp socketid backslash-escaped-string
(config)>
```

15. Configure the remote sites to which you want to send data. If you do not specify any destinations, the IX10 send new data to the last hostname and port from which data was received. To add a destination:
    i. Add a destination:

```
(config)> add serial port1 upd destination end
(config serial port1 udp destination 0)>
```

    ii. (Optional) Enter a description of the destination:

```
(config serial port1 udp destination 0)> description string
(config serial port1 udp destination 0)>
```

    iii. Set the host name or IP address of the remote site to which data should be sent:

```
(config serial port1 udp destination 0)>hostname hostanme-or-IP-address
(config serial port1 udp destination 0)>
```

    iv. Set the port number of the remote site to which data should be sent:

```
(config serial port1 udp destination 0)> port port
(config serial port1 udp destination 0)>
```

16. (Optional) Configure access control:
    a. Return to the root configuration prompt by typing **...**:

```
(config serial port1 udp destination 0)> ...
(config)>
```

    b. Set the Access Control List:
        - To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 udp acl address end value
(config)>
```

          Where *value* can be:
          - A single IP address or host name.
          - A network designation in CIDR notation, for example, 192.168.1.0/24.
          - **any**: No limit to IPv4 addresses that can access the service-type.

          Repeat this step to list additional IP addresses or networks.
        - To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 udp acl address6 end value
(config)>
```

          Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add serial port1 udp acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add serial port1 udp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by
packet
filtering rules and access control lists.

Additional Configuration
-------------------------------------------------------------------------------
any
```

```
dynamic_routes
edge
external
internal
ipsec
loopback
setup

(config)>
```

Repeat this step to include additional firewall zones.

- To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 udp acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 udp acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add serial port1 udp acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------------
setupip         Setup IP
```

```
setuplinklocalip     Setup Link-local IP
eth                  ETH
loopback             Loopback
modem                Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add serial port1 udp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

17. Configure serial port logging:
    a. Enable serial port logging:

```
(config)>serial port1 logging enable true
(config)>
```

    b. Set the file name:

```
(config)>serial port1 logging filename string
(config)>
```

    c. Set the maximum allowed log size for the serial port log when starting the log:

```
(config)>serial port1 logging size value
(config)>
```

where *value* is the size of the log file in bytes. The default is **65536**.

d. Specify the data type:

```
(config)>serial port1 logging type value
(config)>
```

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

e. Log the time at which date was received or transmitted:

```
(config)>serial port1 logging hex true
(config)>
```

f. Log data as hexadecimal values:

```
(config)>serial port1 logging timestamp true
(config)>
```

18. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

19. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure Modem emulator mode for a serial port

Modem emulator mode allows the device to act as a dial-up modem emulator for handling incoming AT dial-ins.

To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

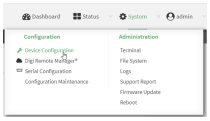
   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click to expand the name of the port that you want to configure, for example, **Port 1**.

   The serial port is enabled by default. To disable, toggle off **Enable**.
4. For **Mode**, select **Modem emulator**. The default is **Remote Access**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
7. For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.
8. For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.
9. For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**
10. For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
11. For **Idle timeout**, type the amount of time that the active session can be idle before the session is disconnected.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.
12. For **Escape character**, type the character to use in the escape sequence. Enter this character three times, followed by the escape delay and then an AT command to switch from data mode to command mode. The default is the plus sign (**+**).
13. For **Escape delay**, type the delay between the escape sequence and an AT command to switch from data mode to command mode. The default is **1s**.
14. For **Auto-answer rings**, type the number of rings to wait before auto-answering. Enter **0** (zero) to disable auto-answering.
15. **Command echo** is enabled by default. Commands sent to the port are echoed back to the user. Select to disable this feature.
16. For **Result codes**, select the type of result code that are displayed as responses to commands. Options are:

- **None**: No result codes are displayed.
- **Numeric**: Numeric result codes are displayed.
- **Verbose**: Result codes are displayed in English, for example: OK, ERROR, CONNECT. This is the default.

17. (Optional) Click to expand **Phonebook** and create dial strings that can be used to connect to remote servers.
    a. Click to add a phone book entry.
    b. For **Label**, type a descriptive name for the phone book entry.
    c. (Required) For **Dialstring**, type the string to dial to connect to the remote server.
    d. (Required) For **Connection destination**, type the hostname or IP address of the remote server.
    e. (Required) For **Connection port**, type the TCP port of the remote server. Minimum is 1 and maximum is 65535.
18. Expand **TCP connection** to configure TCP connection for this serial port.
    a. To enable a TCP connection, click to toggle on **Enable**.
    b. For **Port**, type the TCP port for this service. The default is **4001**.
    c. Expand **Access control list** to create a list of IP addresses, interfaces, and firewall zones from which this service may be accessed.
        - To limit access to specified IPv4 addresses and networks:
            i. Click **IPv4 Addresses**.
            ii. For **Add Address**, click .
            iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
                - A single IP address or host name.
                - A network designation in CIDR notation, for example, 192.168.1.0/24.
                - **any**: No limit to IPv4 addresses that can access the service-type.
            iv. Click again to list additional IP addresses or networks.
        - To limit access to specified IPv6 addresses and networks:
            i. Click **IPv6 Addresses**.
            ii. For **Add Address**, click .
            iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
                - A single IP address or host name.
                - A network designation in CIDR notation, for example, 2001:db8::/48.
                - **any**: No limit to IPv6 addresses that can access the service-type.
            iv. Click again to list additional IP addresses or networks.
        - To limit access to hosts connected through a specified interface on the device:
            i. Click **Interfaces**.
            ii. For **Add Interface**, click .
            iii. For **Interface**, select the appropriate interface from the dropdown.
            iv. Click again to allow access through additional interfaces.

- To limit access based on firewall zones:
  i. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  ii. For **Add Zone**, click .
  iii. For **Zone**, select the appropriate firewall zone from the dropdown.
  See Firewall configuration for information about firewall zones.
  iv. Click again to allow access through additional firewall zones.

d. Toggle on **Enable mDNS** to enable Multicast DNS (mDNS) reporting for this service. This feature is disabled by default.

19. Expand **Logging Settings** to configure logging for this serial port.
    a. To enable logging, click to toggle on **Enable**.
    b. In the **Log file name** field, enter a descriptive name for the log file.
    c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
    d. From the **Type of data to log** list box, specify the type of data that should be saved.
       - **Received**
       - **Transmitted**
       - **Both**
       - **Both with arrows**. This is the default.
    e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
    f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

    Note You can review the message log in the **Serial Port Log** page. See Review the serial port message log.

20. Click **Apply** to save the configuration and apply the change.

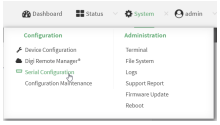
Configure Modbus mode for a serial port

Modbus mode allows you to use the serial port for Modbus. See Modbus gateway.

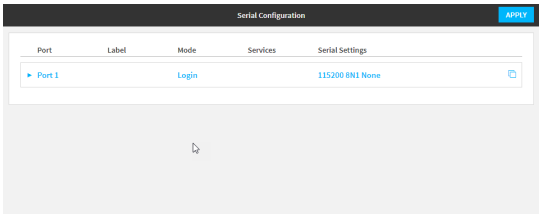
To change the configuration to match the serial configuration of the device to which you want to connect:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

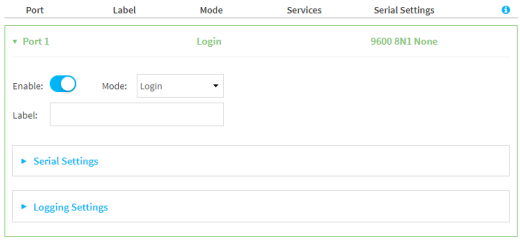


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **Modbus**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
   - **RS-485**
     - Enable **Termination** if you want to enable electrical termination on this serial port.

   The default is **RS-232**.
7. Expand **Serial Settings**.

   The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

   a. **Baud rate**: For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.

   b. **Data bits**: For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.

   c. **Parity**: For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.

   d. **Stop bits**: For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.

   e. **Flow control**: For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```
3. The serial port is enabled by default. To disable:

   ```
   (config)> serial port1 enable false
   (config)>
   ```
4. Set the mode:

   ```
   (config)> serial port1 mode modbus
   (config)>
   ```
5. Set the signaling interface type used on this serial port:
   - **rs-232**
   - **rs-485**
     - Enable **termination** if you want to enable electrical termination on this serial port:

       ```
       (config)> serial port1 termination true
       (config)>
       ```

   The default is **rs-232**.
6. (Optional) Set a label that will be used when referring to this port.

   ```
   (config)>path-paramlabel label
   (config)>
   ```
7. Set the baud rate used by the device to which you want to connect:

   ```
   (config)> serial port1 baudrate rate
   (config)>
   ```
8. Set the number of data bits used by the device to which you want to connect:

   ```
   (config)> serial port1 databits bits
   (config)>
   ```
9. Set the type of parity used by the device to which you want to connect:

   ```
   (config)> serial port1 parity parity
   (config)>
   ```

   Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

10. Set the stop bits used by the device to which you want to connect:

```
(config)> serial port1 stopbits bits
(config)>
```

11. Set the type of flow control used by the device to which you want to connect:

```
(config)> serial port1 flow value
(config)>
```

where value is one of:

- **none**
- **rts/cts**
- **xon/xoff**

12. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

13. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure RealPort mode using the Digi Navigator

You can use RealPort mode to enable communication between a device and your computer. From the **Digi Navigator**, you can easily configure your device for RealPort, and then install and configure RealPort on your computer.

With Digi Navigator, you can set serial ports on the device to RealPort mode as needed, and then also enable the RealPort service. The COM ports on your laptop are also configured. These processes ensure that RealPort is configured on the device and on your computer.

Note You must configure the device for RealPort before you install and configure RealPort on your computer. The RealPort configuration on the device includes enabling RealPort service on the device. When you configure RealPort on your computer, it must connect to the RealPort service on the device.

Digi Navigator installation

The **Digi Navigator** can only be installed on a computer with a Windows OS. If you are using Linux, you can manually install and configure RealPort without **Digi Navigator**. For the Linux installation process, refer to the Get started: Install RealPort for LINUX in the **RealPort Installation User's Guide**.

Installation and configuration process

These steps explain how to install and configure the **Digi Navigator**.

Step 1: Install the Digi Navigator

Step 2: Configure RealPort on a Digi device from the Digi Navigator

Step 3: Install and configure RealPort on your computer

Note If you have Digi Navigator 1.0 already installed, Digi recommends that you uninstall it, as both versions of the Digi Navigator are not needed. See Uninstall Digi Navigator 1.0.

Digi Navigator features

- Digi Navigator application features
- Filter devices for display in the Digi Navigator
  - Filter the device list by service option
  - Filter the device list for auto-discovered devices
  - Filter the device list by RealPort configuration status
- Specify the IP address to discover a Digi device
- Set an IP address for a device
- Access a device's web UI from the Digi Navigator
- Manage the list of devices configured for RealPort
  - Refresh the RealPort device list
  - Review the COM ports configured for RealPort
  - Uninstall the RealPort device configuration from your computer
- Reconfigure RealPort on a device
- Generate a device setup script
- Review Digi Navigator version information
- Uninstall Digi Navigator 1.0

Install the Digi Navigator

This section explains how to download and install the **Digi Navigator** application.

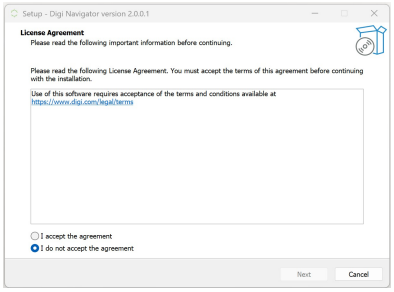
Note Microsoft Visual C++ is required for RealPort and is installed by default during the Digi Navigator install process.

1. Navigate to the Digi Navigator support page.

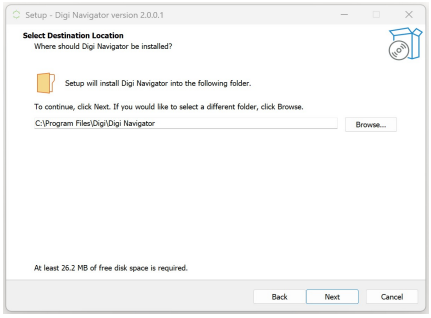
   Note The **Digi Navigator** application can also be downloaded from your device's product support page.

2. Scroll down to the **Product Resources** tab, and in the **Drivers & Patches** section, click **Digi Navigator**.
3. From the list box, select the appropriate Microsoft Windows option from the list of driver options.
4. Click the **download** link to download the **Digi Navigator** application.

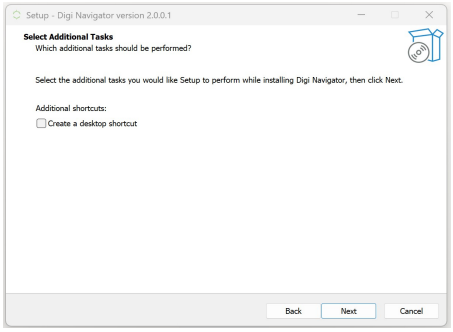
5. When the download is complete, click on the downloaded .exe file. The **Digi Navigator Setup** wizard displays.
6. In the **License Agreement** page, review the agreement and select the **I accept the agreement** option.



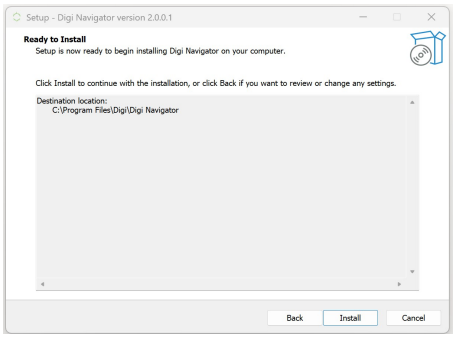
7. Click **Next**. The **Select Destination Location** page displays.
   - You can leave the installation location as the default, or click **Browse** to select a different location.



8. Click **Next**. The **Select Additional Tasks** page displays.
   - If you want to create a shortcut for the Digi Navigator, select the **Create a desktop shortcut** option.

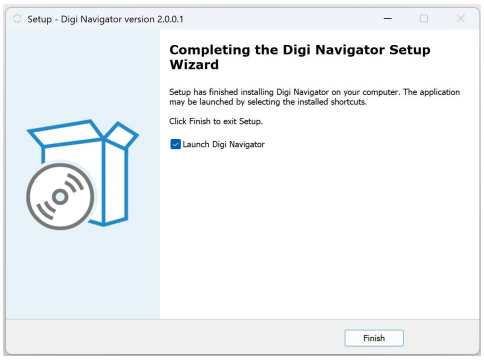


9. Click **Next**. The **Ready to Install** page displays.



10. Click **Install** to start the installation. When complete, the **Completing the Digi Navigator Setup Wizard** page displays.

    The **Launch Digi Navigator** option is selected by default. De-select this option if you don't want the **Digi Navigator** to automatically launch each time you boot your computer.



11. Click **Finish** to complete the installation process. If the **Launch Digi Navigator** option was selected, the Digi Navigator launches.

NEXT STEP: Configure RealPort on a device. See Configure RealPort on a Digi device from the Digi Navigator.

Configure RealPort on a Digi device from the Digi Navigator

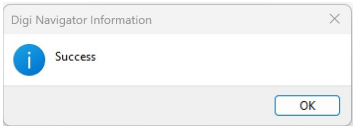
You can configure the IX10 to communicate with your computer using RealPort. In this step, you can select which serial ports on the device should be set to RealPort mode, and the RealPort service is enabled for the device.

Configuring RealPort on your device is the first step in a two-step process. To ensure communication between the device and your laptop, you must also configure your computer for RealPort after the first step is completed.

Note You can also manually configure the device for RealPort by logging into the device's web UI. See Advanced RealPort configuration without using the Digi Navigator.

1. Make sure the IX10 is powered and connected your local network or computer with an Ethernet cable.

2. Launch the **Digi Navigator**.
3. A list of the devices you have manually added displays. You can add additional devices if needed.
4. Find the device that you want to configure and expand it to display the IP addresses for the device.
5. Use one of the following methods to begin configuring RealPort on the device:
   - **Configuration pane**: Click on the IP address to display options in the Configuration pane. Click **Configure Device for RealPort**. The **Enter Device Credentials** page displays.
   - **Shortcut menu**: Right-click on an IP address to display the shortcut menu, and click **Configure Device For RealPort**. The **Enter Device Credentials** page displays.
6. In the **Enter Device Credentials** page, enter the device's default user name and password in the **Username** and **Password** fields. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device. If the defaults do not work, they may have been changed. Verify with your system administrator.
7. Click **OK**.
8. When RealPort configuration is complete, the **Success** message displays.



9. Click **OK** to close the message.
10. (Optional) If desired, you can verify the RealPort configuration. See Configure the serial port for RealPort mode and Configure the RealPort service.

NEXT STEP: Install and configure RealPort on your computer. See Install and configure RealPort on your computer.

Install and configure RealPort on your computer

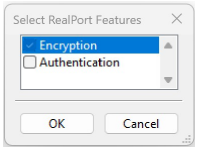
You can configure your computer to communicate with the IX10 using RealPort. In this step, RealPort is installed on your computer and communication with the device is configured.

Configuring RealPort on your device is the second step in a two-step process. To ensure communication between the device and your laptop, you must also have configured your device for RealPort. See Configure RealPort on a Digi device from the Digi Navigator.

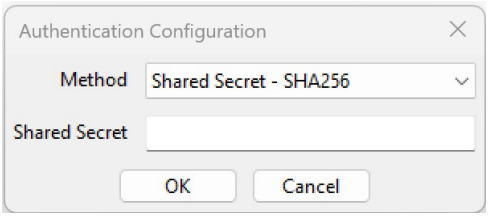
Note You can also manually install and configure RealPort on your computer. See Advanced RealPort configuration without using the Digi Navigator.

1. Make sure the IX10 is powered and connected your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. A list of the devices you have manually added displays. You can add additional devices if needed.
4. Find the device that you want to access and expand it to display the IP addresses for the device.

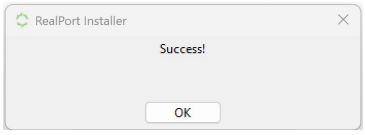
5. Use one of the following methods to begin configuring RealPort on your computer:
   - **Configuration pane**: Click on the IP address to display options in the Configuration pane. Click **Configure this PC for RealPort**. The **Select RealPort Features** dialog displays.
   - **Shortcut menu**: Right-click on an IP address to display the shortcut menu, and click **Configure this PC for RealPort**. The **Select RealPort Features** dialog displays.
6. Configure features in the **Select RealPort Features** dialog.



   a. Enable **Encryption** to enable encryption of data. This is enabled by default.
   b. Enable **Authentication** to configure the authentication method the RealPort server uses to authenticate clients. The **Authentication Configuration** dialog displays.
      - From the **Method** list box, select the **Shared Secret - SHA256** option.
      - For **Shared Secret**, enter the authentication password to ensure secure communication. Leave this field blank to disable authentication.



   c. Click **OK**.
7. The **Select Ports** dialog displays. By default, all of the ports on the device are selected to be configured for RealPort. De-select the ports that you don't want to configure for RealPort.
8. Click **OK**. The **COM Selection** dialog displays.
9. From the **Select starting COM** list box, select the first COM port that should be configured for RealPort. The first available COM port is selected by default. The number of COM ports configured matches the number of serial ports on the device.
10. Click **OK**. A series of progress messages displays.
11. When the configuration is complete, a message displays.



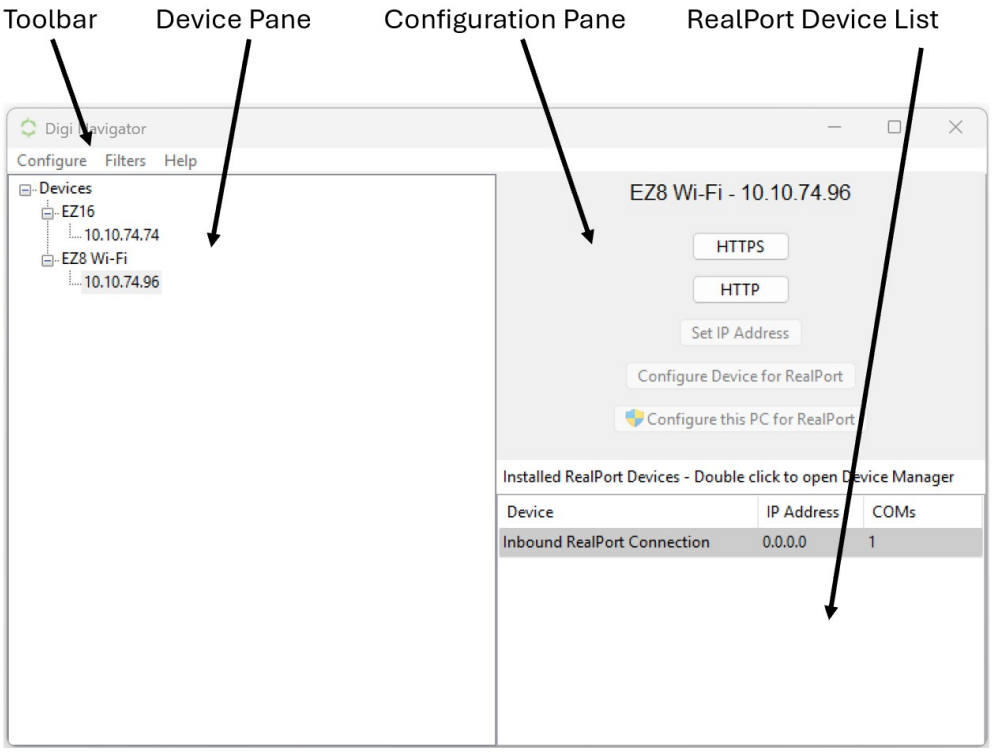
12. Click **OK** to close the message.
13. (Optional) After RealPort configuration on your laptop is complete, you can open the Windows **Properties** dialog for your computer.
    a. Launch the **Digi Navigator** if it is not currently open. A list of devices that have RealPort enabled and configured displays in the **Installed RealPort Devices** section at the bottom

of the screen.

b. Double-click on a device name. The Windows **Properties** dialog for your computer displays. and display the COM ports on your computer that are configured for RealPort. For more information, see Review the COM ports configured for RealPort.

Digi Navigator application features

All features of the **Digi Navigator** are available from the main application screen.



Toolbar

The toolbar menus are used to configure Digi Navigator.

Menu item	Sub-menu item	Description
Configure	**Known Devices**	If a Digi device is not on the same network as your computer or the device is undiscoverable, you can manually add the device using that device's IP address. ■ Specify the IP address to discover a Digi device
	Refresh Installed RealPort Device List	Use the **Refresh Installed RealPort Device List** feature to update the list of the Digi devices that have RealPort enabled and configured. The list displays in the RealPort Device List pane in the Digi Navigator.

Menu item	Sub-menu item	Description
		▪ Refresh the RealPort device list
	Generate Device Setup Script	Use the **Generate Device Setup Script** feature to generate a script of the RealPort configuration of the local PC. The script can be saved and used as a backup.The script is generated as a .cmd file. ▪ Generate a device setup script
Filters	**Services**	You can limit the service options that display in the Configuration pane in the **Digi Navigator**. You can click on a service option in the Configuration pane to use that service to log in to the device. ▪ Filter the device list by service option
	IP Addresses	Not applicable for devices that do not support autodiscovery with Digi Navigator.
	Devices > Supported Services > RealPort	You can use the **RealPort** option to filter which devices are included in the device list, depending on the RealPort configuration status. ▪ Filter the device list by RealPort configuration status
	Devices > Discovered Devices	You can use the **Discovered Devices** option to filter which devices are included in the device list, depending on whether the device was auto-discovered. ▪ Filter the device list for auto-discovered devices
Help	**About**	Review the Digi Navigator version information. ▪ Review Digi Navigator version information

Device pane

A list of the discovered devices and those added to the known device list display in the Device pane. Expand each device to display the IP addresses associated with each device.

Filter the device list

You can apply filters to limit which devices display in the pane.

- Filter the device list by service option
- Filter the device list for auto-discovered devices
- Filter the device list by RealPort configuration status

Display configuration options for a device in the Configuration page

Expand a device and click on an IP address for the device to display related configurations options in the Configuration pane.

Shortcut menu

You can right-click on the IP address for a device to display the shortcut menu options. The options are an easy way to use the features from the toolbar.

Item	Description
Add to Known Devices	If a Digi device is not on the same network as your computer or the device is undiscoverable, you can manually add the device using that device's IP address. ■ Specify the IP address to discover a Digi device
HTTPS	You can use the **HTTPS** menu option to access the device's web UI using the HTTPS service. ■ Access a device's web UI from the Digi Navigator
HTTP	You can choose the **HTTP** menu option to access the device's web UI using the HTTP service. ■ Access a device's web UI from the Digi Navigator
SSH	You can use the **SSH** menu option to access the device's web UI using the SSH service. ■ Access a device's web UI from the Digi Navigator
Set IP Address	You can reconfigure the IP address of a device to a DHCP address or a specified static address. ■ Set an IP address for a device
Configure Device for RealPort	You can use the **Configure Device for RealPort** menu option to configure RealPort on the device. ■ Configure RealPort on a Digi device from the Digi Navigator ■ Reconfigure RealPort on a device
Configure this PC for RealPort	Use the **Configure this PC for RealPort** menu option to configure RealPort on your computer so that it can communicate with the device. ■ Install and configure RealPort on your computer

Configuration pane

You can use the buttons in the Configuration pane to connect to a device's web UI, and configure RealPort on your device and on your computer.

Item	Description
HTTPS	You can click **HTTPS** to access the device's web UI using the HTTPS service. ■ Access a device's web UI from the Digi Navigator
HTTP	You can click **HTTP** to access the device's web UI using the HTTP service. ■ Access a device's web UI from the Digi Navigator
SSH	You can click **SSH** to access the device's web UI using the SSH service. ■ Access a device's web UI from the Digi Navigator

Item	Description
Set IP Address	You can reconfigure the IP address of a device to a DHCP address or a specified static address. ■ Set an IP address for a device
Configure Device for RealPort	Click **Configure Device for RealPort** to configure RealPort on the device. ■ Configure RealPort on a Digi device from the Digi Navigator ■ Reconfigure RealPort on a device
Configure this PC for RealPort	Click **Configure this PC for RealPort** to configure RealPort on your computer so that it can communicate with the device. ■ Install and configure RealPort on your computer

RealPort device list pane

The RealPort device list displays all of the devices in Digi Navigator that are configured for RealPort.

Item	Description
Open Device Manager	Click a name in the RealPort device list to open the Windows **Properties** dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device. ■ Review the COM ports configured for RealPort
Uninstall Device	You can uninstall RealPort from the device and uninstall the RealPort configuration for this device from your computer if needed, using the **Uninstall Device** shortcut menu option. ■ Uninstall the RealPort device configuration from your computer

Filter the device list displayed in the Digi Navigator

You can apply filters to limit which devices display in the device list.

Filter the device list by service option

You can filter the device list that displays in the Device page by service. This also determines which service buttons display in the Configuration pane.

The Digi Navigator uses the HTTPS service by default to discover the IP addresses for the Digi devices connected to your network. Other services can be used, if needed.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Filters** > **Services** from the toolbar to display the service options: **HTTPS**, **HTTP**, and **SSH**. To ensure that you can communicate with your device, at least one option should be selected.
4. Click on service option to select it or deselect it. A check mark displays next to a selected option.

   The selected options are included in the configuration pane. You can click on a service option in the configuration pane to use that service to log in to the device.

Filter the device list for auto-discovered devices

You can use the **Discovered Devices** option to filter which devices are included in the device list, depending on whether the device was auto-discovered or is a device that was manually added to the known device list.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. From the toolbar, click **Filters** > **Devices**. Use the **Discovered Devices** menu option to filter the devices.
   - **Selected**: Both known and discovered devices are listed.
   - **Not selected**: Only known devices are listed.

Filter the device list by RealPort configuration status

You can use the **RealPort** option to filter which devices are included in the device list, depending on the RealPort configuration status.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. From the toolbar, click **Filters** > **Devices** > **Supported Services**. Use the **RealPort** menu option to filter the devices.
   - **Selected**: Only discovered devices that are configured for the RealPort service display. Known devices are included if the device is configured for RealPort.
   - **Not selected**: All discovered devices on your network and all known devices display, regardless of RealPort service configuration status.

Specify the IP address to discover a Digi device

You can manually add a device to the known device list, using the device's IP address. This feature is useful if a device is not on the same network as your computer or the device is undiscoverable.

Before you begin

To add a device, you will need:

- The device's IP address.
- The user name and password for the device.

To add a device to the known device list:

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Configure** > **Known Devices**.
4. Click **Add**. The **New Device** dialog displays.
   a. In the **Name** field, enter a descriptive name for the device.
   b. Click **Add**.
   c. In the **IP Addresses** field, enter the IP address of the device.

      If you want to enter more than one IP address for this device, click **Add** and enter another IP address.
   d. Click the buttons for the services that you want to use to communicate with the device. The default port number for each service can be changed. After a service has been selected, you can click the button for the service to de-select it.

      To ensure that you can communicate with your device, at least one option should be selected.

      - **HTTPS**: The **HTTPS** service is selected by default. The default port number is **443**.
      - **HTTP**: The default port number is **80**.
      - **SSH**: The default port number is **22**.
      - **RealPort**: Click **RealPort** to enable the RealPort service for the device. The default port number is **1027**.
5. Click **OK**. You are returned to the **Known Devices** dialog.
6. Click the **X** in the upper right corner to close the dialog.
7. The device you just added displays in the device list.

Set an IP address for a device

You can reconfigure the IP address of a device to a DHCP address or a specified static address.

Note This feature can be used with only discovered devices. It is not enabled for known devices.

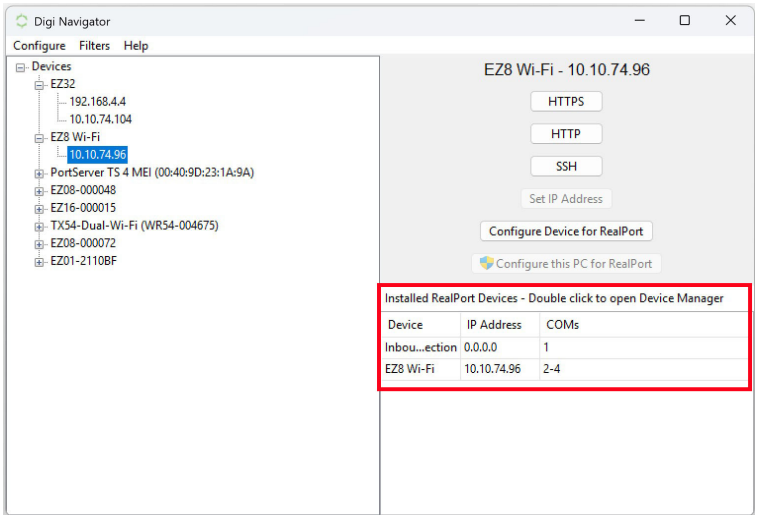
1. Make sure the IX10 is powered and connected your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. A list of the devices you have manually added displays. You can add additional devices if needed.
4. Find the device that you want to configure and expand it to display the IP addresses for the device.
5. Use one of the following methods to begin reconfiguring the IP address:

- **Configuration pane**: Click on the IP address to display options in the Configuration pane. Click **Set IP Address**. The **IP Address Configuration** dialog displays.
- **Shortcut menu**: Right-click on an IP address to display the shortcut menu, and click **Set IP Address**. The **IP Address Configuration** dialog displays.

6. In the **IP Address Configuration** dialog, enter the required information:
   - **Type**: From the **Type** list box, select an option: **DHCP** or **Static IP address**.
   - **Address**: Enter the IP address.
   - **Default gateway**: Enter the default gateway that should be used.
7. Click **OK**.

Manage the list of devices configured for RealPort

After you have enabled and configured RealPort on at least one Digi device, a list of configured devices displays at the bottom of the **Digi Navigator**. You can refresh the list and easily access the COM port configuration on your computer.



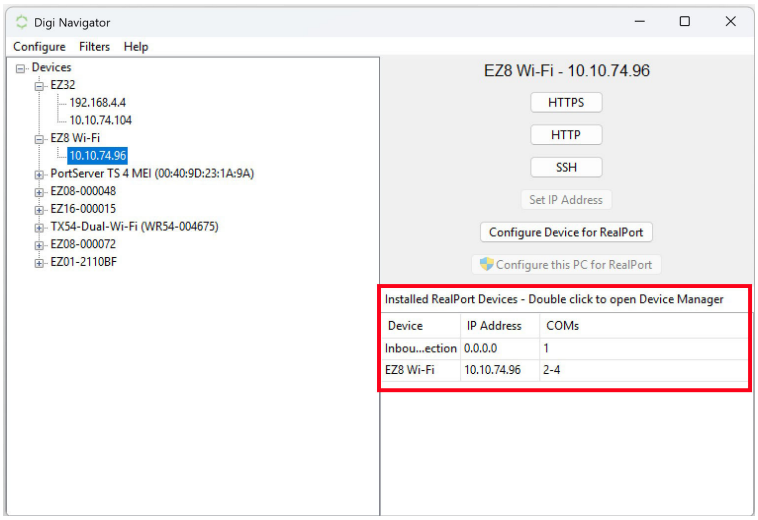
- **Refresh**: From the toolbar, choose **Configure** > **Refresh Installed RealPort Device List** to update the list of IX10 devices that have RealPort enabled and configured.
- **Device Manager**: Double-click on a device name in the list to open the Windows **Properties** dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device.
- **Uninstall the RealPort configuration on your computer**: You can use the **Uninstall Device** option to remove the RealPort device configuration on your computer for a selected device. This ensures that your computer is not able to connect to the selected device.

Refresh the RealPort device list

You can refresh the list of the Digi devices that have RealPort enabled and configured. The list displays in the **Installed RealPort Devices** pane in the Digi Navigator.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.

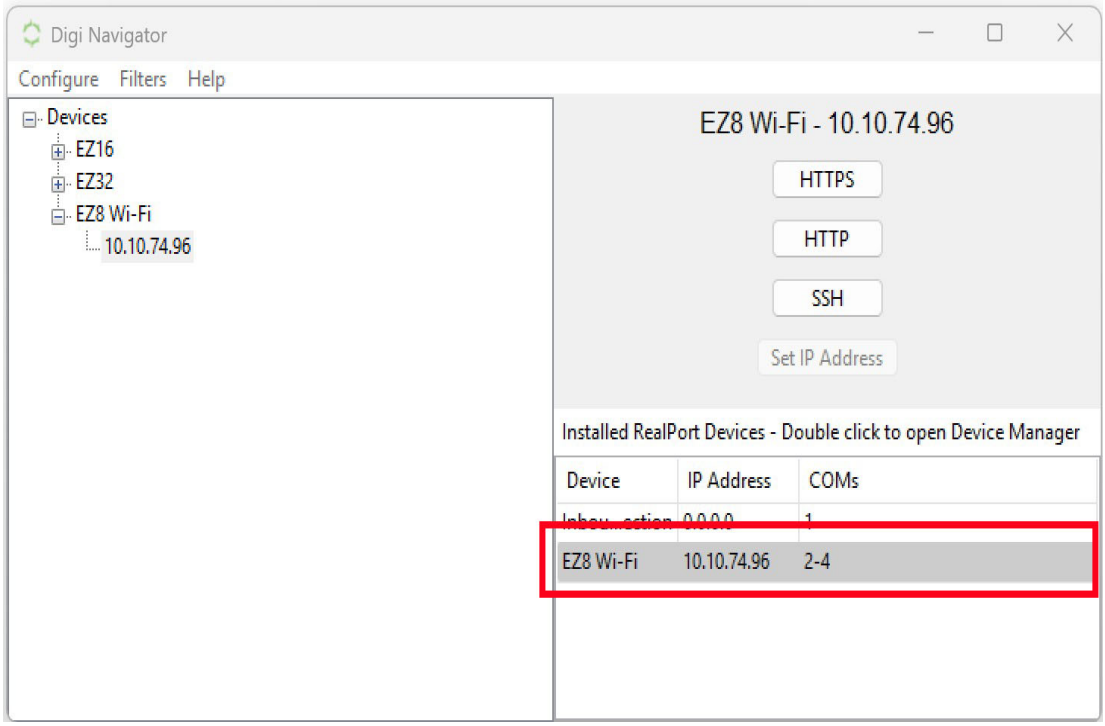
3. Click **Configure** > **Refresh Installed RealPort Device List** to refresh the list.



Review the COM ports configured for RealPort

You can open the Windows **Properties** dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. In the RealPort list section of the Digi Navigator, double-click on a name in the **Device** column.

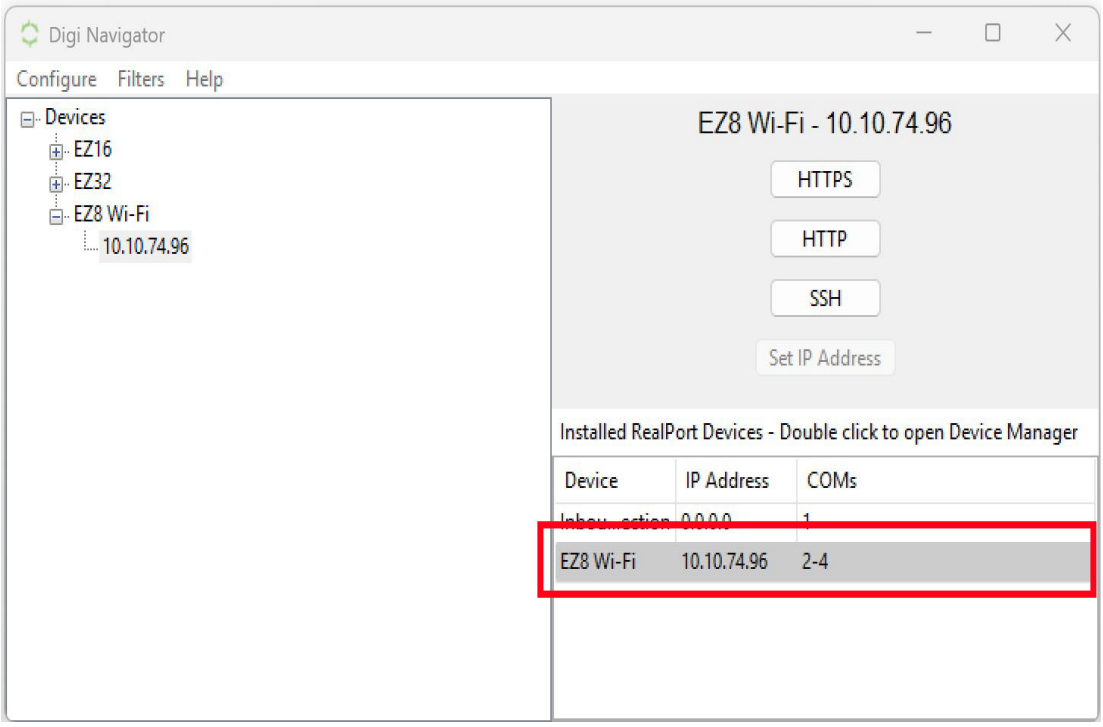


4. The standard Windows **Device Properties** dialog opens.
   a. Click the **General** tab.
   b. Click **Change settings**.
   c. Click the **Advanced** tab.
   d. Click **Properties**. The COM ports display.
   e. Click **OK** or **Cancel** to close the dialog.

Uninstall the RealPort device configuration from your computer

You can use the **Uninstall Device** option to remove the RealPort device configuration on your computer for a selected device. This ensures that your computer is not able to connect to the selected device.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. In the RealPort list section of the **Digi Navigator**, find the device that you want to uninstall.



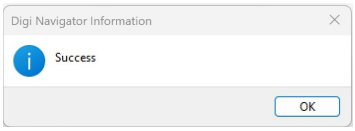
4. Right-click on an IP address in the list to display the shortcut menu.
5. Click **Uninstall Device** to remove the RealPort configuration for this device from your computer.
6. When the process is complete, a **Success** message displays in a confirmation dialog.
7. Click **OK** to close the dialog.

Reconfigure RealPort on a device

After you have initially configured RealPort on a device and established a connection with your computer, you can reconfigure RealPort on the device as needed.

Note If you reconfigure RealPort on a device, you do not need to reconfigure your computer.

1. Make sure the IX10 is powered and connected your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. A list of the devices you have manually added displays. You can add additional devices if needed.
4. Find the device that you want to configure and expand it to display the IP addresses for the device.
5. Use one of the following methods to begin configuring RealPort on the device:
   - **Configuration pane**: Click on the IP address to display options in the Configuration pane. Click **Configure Device for RealPort**. The **Enter Device Credentials** page displays.
   - **Shortcut menu**: Right-click on an IP address to display the shortcut menu, and click **Configure Device For RealPort**. The **Enter Device Credentials** page displays.
6. In the **Enter Device Credentials** page, enter the device's default user name and password in the **Username** and **Password** fields. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device. If the defaults do not work, they may have been changed. Verify with your system administrator.
7. Click **OK**.
8. When RealPort configuration is complete, the **Success** message displays.



9. Click **OK** to close the message.
10. (Optional) If desired, you can verify the RealPort configuration. See Configure the serial port for RealPort mode and Configure the RealPort service.

Access a device's web UI from the Digi Navigator

You can access the device's web UI and log in from the Configuration pane in the **Digi Navigator**, or from the shortcut menu for the device's IP address.

The service options are available in the Configuration pane or the shortcut menu if these conditions are met:

- The service button must be included in the **Services** filter. See Filter the device list by service option.
- At least one device must be configured for the service. For known devices, see Specify the IP address to discover a Digi device.

To access a device's web UI:

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.

3. A list of the devices you have manually added displays. You can add additional devices if needed.
4. Find the device that you want to access and expand it to display the IP addresses for the device.
5. Launch the web UI for the device using one of the following methods:
   - **Configuration pane**: Click on an IP address for the device to display the configured service button(s) in the Configuration pane. Click on any of the active buttons (**HTTP**, **HTTPS**, **SSH**) to access the web UI and log in.
   - **Shortcut menu**: Right-click on the IP address for a device to display the shortcut menu. Click on any of the service options (**HTTP**, **HTTPS**, **SSH**) to access the web UI and log in.

Generate a device setup script

You can generate a script of the RealPort configuration of the local PC. The script can be saved and used as a backup.The script is generated as a .cmd file.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Configure** > **Generate Device Setup Script**. The standard Windows dialog to name a file displays.
   a. Select a location and enter a descriptive name.
   b. Click **Save**.
4. The script is generated, a confirmation dialog displays when complete.
5. Click **OK** to close the dialog.

Review Digi Navigator version information

You can review the Digi Navigator version information.

1. Make sure **Digi Navigator** is installed and the IX10 is powered and connected to your local network or to your computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. From the toolbar, click **Help** > **About**. The **About Digi Navigator** dialog displays.
4. Review the information.
5. Click **OK** to close the dialog.

Uninstall Digi Navigator 1.0

If you have Digi Navigator 1.0 installed, Digi recommends that you uninstall it, as both versions of the Digi Navigator are not needed.

1. If Digi Navigator 1.0 is open, close it before you begin.
2. Launch the Windows **Control Panel**.
3. Click the **Programs** option.
4. Click **Uninstall a Program**.
5. Scroll through the list of programs to find Digi Navigator 1.x.

6. Right-click on the program name to display the menu.
7. Click **Uninstall**. The **Digi Navigator Uninstall** wizard displays.
8. Click **Next**. The uninstall process begins.

> **Note** If Digi Navigator 1.0 is open, a confirmation dialog with the message "Digi Navigator is running. Click OK to close it." displays. Click **OK** to continue with the uninstall process.

9. When complete, the **Completing Digi Navigator Uninstall** page displays.
10. Click **Finish** to complete the uninstall process.

Advanced RealPort configuration without using the Digi Navigator

You can configure the IX10 to communicate with your computer using RealPort.

Windows Operating System

This method can be used if your computer has a Windows OS installed and you choose not to use the Digi Navigator to discover devices and configure RealPort.

To complete the RealPort configuration process for Windows:

Step 1: Download the RealPort driver

Step 2: Configure RealPort on your computer

Step 3: Configure the serial port for RealPort mode

Step 4: Configure the RealPort service

Linux Operating System

To complete the RealPort configuration process for Linux OS:

Step 1: Download the RealPort driver

Step 2: To complete the RealPort configuration process, refer to the Get started: Install RealPort for LINUX section in the **RealPort Installation User's Guide**.

Download the RealPort driver

The first step is to download the RealPort application and save it to a location that you can easily access.

1. Navigate to https://hub.digi.com/support/products/realport/.
2. Scroll down to the **Product Resources** tab, and in the **Drivers & Patches** section, click **RealPort Driver**.
3. From the list box, select the appropriate Microsoft Windows option from the list of driver options. The associated RealPort for Windows option displays.
4. Click the **download** link.
5. When the download is complete, navigate to your download folder. The application is in a .zip file.
6. You can leave the .zip file in the download folder, or copy the .zip file and paste it to a location that you can easily access.

Configure RealPort on your computer

RealPort must be installed on yourcomputer, and then RealPort configured for the IP address of each device that should be allowed a RealPort connection.

You will run the RealPort Wizard for each device that you want to configure. RealPort is installed on your laptop the first time that you run the wizard. The installation process is ignored each subsequent time that you run the wizard.

Before you begin

- Download RealPort onto your laptop, and make note of the download location. See Download the RealPort driver.
- Have the IP address of the device that you want to configure.

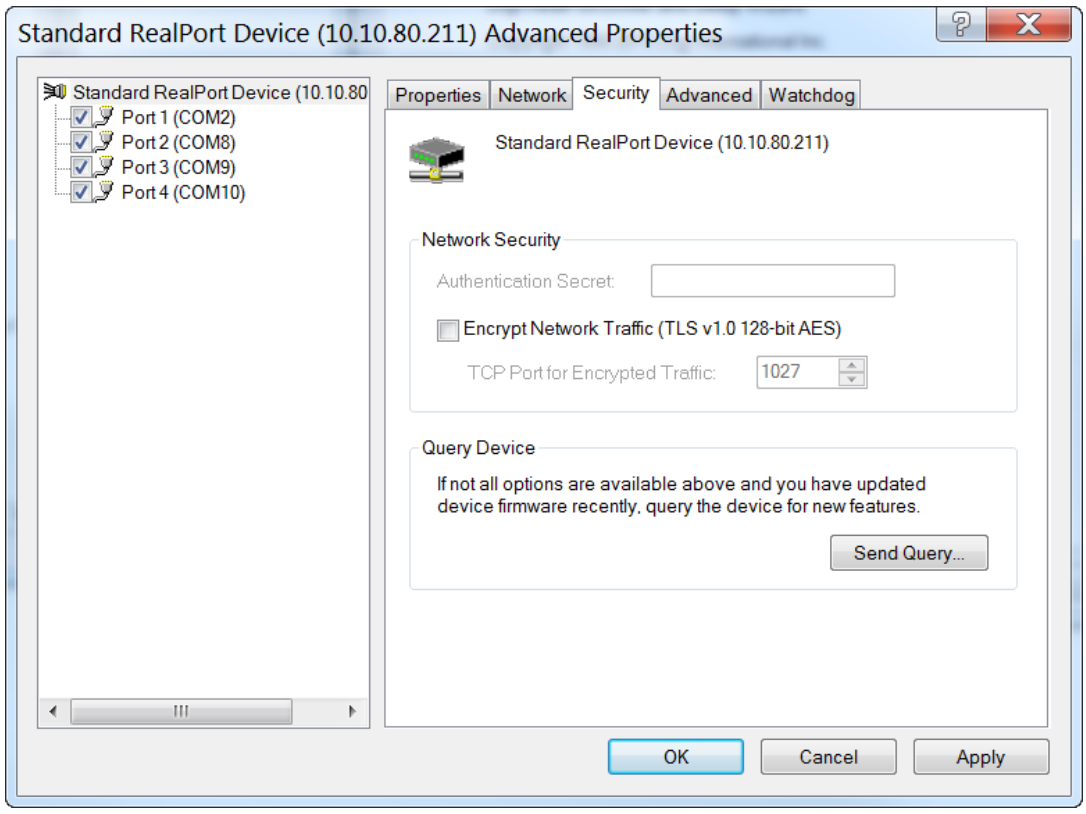
Step 1: Implement RealPort

1. Navigate to the downloaded Realport .zip file.
2. Open the .zip file.
3. Click on **setup.exe** to launch the RealPort wizard. The **Welcome to the Digi RealPort Setup Wizard** screen displays.
4. If this is not the first time you have run the wizard, select the **Add a New Device** option. If this is the first time running the wizard, no options are available on the screen.
5. Click **Next**. The **Select Device** screen displays.
   a. From the list of device options, select the **Device not listed** option.
6. Click **Next**. The **Describe the Device** screen displays.
   a. In the **Device Model Name** field, enter a descriptive name for the device.
   b. In the **Network Settings** section, select the **IP** option and enter the IP address in the associated field.
   c. In the **COM Port Settings** section, from the **No. Ports** list box, select the number of physical serial ports that you want to configure. You can specify from 1 to the maximum number of ports available on the device.
   d. In the **Device Features** section, select both the **Encryption** and **Authentication** options.
7. Click **Finish** to complete the process and close the wizard.

> **Note** If this is the first time that you have run the RealPort wizard, Realport is installed on your laptop. If it is not the first time or if RealPort is already installed, it is not installed again.

Step 2: Configure a RealPort connection on your laptop for your device

1. Follow the standard Windows process to access the **Device Manager** from your computer's operating system.
2. Select **Multi-port Serial Adapters**.
3. Right-click on your device. Click the **Properties** menu option. The **Properties** dialog appears.
4. Click the **Advanced** tab.
5. Click **Properties**. The **Advanced Properties** dialog appears
6. Click the **Security** tab.



7. Select the **Encrypt Network Traffic** check box to enable encrypted network traffic. When you select this option, the **TCP Port for Encrypted Traffic** field becomes available.
8. The **TCP Port for Encrypted Traffic** field has a default value of **1027**. The entry must match the device's TCP port setting.
9. (Optional) If you want to use authentication, configure the feature.
   a. From the the **Authentication Method** list box, select the **Shared Secret - SHA256** option.
   b. Enter the authentication password in the **Shared Secret** field.
10. Click **Apply**.
11. Click **OK** to close the **Advanced Properties** dialog.
12. Click **OK** to close the **Properties** window.

Configure the serial port for RealPort mode

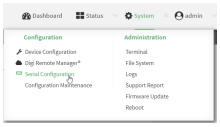
RealPort mode allows you to use Realport.

To change the configuration to match the serial configuration of the device to which you want to connect:

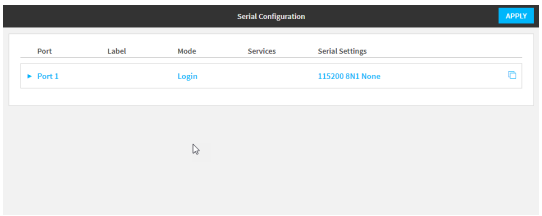
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.

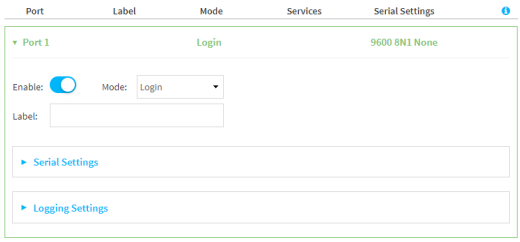


The **Serial Configuration** page is displayed.



Note You can also configure the serial port by using **Device Configuration** > **Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

2. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

3. For **Mode**, select **RealPort**.
4. Select an option from the **Sharing Mode** list box to determine which user(s) can change the port settings, and whether users can receive data from the port.
   - **None**: Only the user that opened the port can change the port settings. All other users are rejected. No other users can receive data from the port. This is the default.
   - **Primary**: Only the user that opened the port can change the port settings. All other users that try to open the port receive all of the data read to the port.
   - **Peer**: Any user that tries to open the port can change the port settings. All users that try to open the port receive all of the data read to the port.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
   - **RS-485**
     - Enable **Termination** if you want to enable electrical termination on this serial port.

   The default is **RS-232**.
7. Expand **Logging Settings** to configure logging for this serial port.

a. To enable logging, click to toggle on **Enable**.
b. In the **Log file name** field, enter a descriptive name for the log file.
c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
d. From the **Type of data to log** list box, specify the type of data that should be saved.
   - **Received**
   - **Transmitted**
   - **Both**
   - **Both with arrows**. This is the default.
e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

> **Note** You can review the message log in the **Serial Port Log** page. See Review the serial port message log.

8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode realport
(config)>
```

5. Set the sharing mode:

```
(config)> serial port1 sharing value
(config)>
```

   where **value** is one of:
   - **none**: Only the user that opened the port can change the port settings. All other users are rejected. No other users can receive data from the port. This is the default.

- **peer**: Any user that tries to open the port can change the port settings. All users that try to open the port receive all of the data read to the port.
- **primary**: Only the user that opened the port can change the port settings. All other users that try to open the port receive all of the data read to the port.

6. Set the signal mode:

```
(config)> serial port1 signal mode value
(config)>
```

where **value** is one of:

Set the signaling interface type used on this serial port:

- **rs-232**
- **rs-485**
  - Enable **termination** if you want to enable electrical termination on this serial port:

```
(config)> serial port1 termination true
(config)>
```

The default is **rs-232**.

7. Set a label that will be used when referring to this port.

```
(config)> serial port1 label label
(config)>
```

8. (Optional) Set a label that will be used when referring to this port.

```
(config)> serial port1 label label
(config)>
```

9. Configure serial port logging:
   a. Enable serial port logging:

```
(config)>serial port1 logging enable true
(config)>
```

   b. Set the file name:

```
(config)>serial port1 logging filename string
(config)>
```

   c. Set the maximum allowed log size for the serial port log when starting the log:

```
(config)>serial port1 logging size value
(config)>
```

   where *value* is the size of the log file in bytes. The default is **65536**.

   d. Specify the data type:

```
(config)>serial port1 logging type value
(config)>
```

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

e. Log the time at which date was received or transmitted:

```
(config)>serial port1 logging hex true
(config)>
```

f. Log data as hexadecimal values:

```
(config)>serial port1 logging timestamp true
(config)>
```

10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the RealPort service

After you have configured RealPort mode on the IX10, you must enable and configure the RealPort service. When this step is complete, all of the serial ports on the IX10 are configured to use the RealPort service.

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **System** > **Configuration** > **Device Configuration**.
3. Expand **Services**.
4. Expand **RealPort**.
5. Click **Enable** to enable the RealPort service.
6. For **RealPort Server Port,** enter **1027**. This is the default.
7. For **Minimum TLS version**, select the minimum TLS version that the RealPort service will accept. The default is TLS version 1.0.
8. Enable **Encryption** to enable encryption of data. This is enabled by default.
9. (Optional) Configure the authentication method the RealPort server uses to authenticate clients.
   a. From the **Authentication Method** list box, select the **Shared Secret - SHA256** option.
   b. For **Shared Secret**, enter the authentication password to ensure secure communication. Leave this field blank to disable authentication.

10. Enable **Exclusive Mode** to ensure that any connection from an IP address is closed when opening a new connection from the same IP address. This disabled by default.
11. Enable **RealPort Keepalive** to send RealPort keepalive packets. This is enabled by default.
12. Enable **TCP Port Keepalive** to send TCP keepalive packets. This is disabled by default.
13. Enable **Device Initiated connections** so users can remotely connect to serial devices as if they had a native COM/TTY port on their PC. This is disabled by default.
14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. RealPort is enabled by default. To disable:

```
(config)> service realport enable false
(config)>
```

4. Set the RealPort server port.

```
(config)> service realport port value
(config)>
```

   where **value** is the port you want to use for the RealPort service. The default is **1027**.
5. Set the select the minimum TLS version that the RealPort service will accept:

```
(config)> service realport minimum_tls_version value
(config)>
```

   where **value** is one of:
   - **TLS-1_0**. This is the default.
   - **TLS-1_1**
   - **TLS-1_2**
   - **TLS-1_3**
6. Data encryption is enabled by default. To disable:

```
(config)> service realport encryption false
(config)>
```

7. (Optional) Configure authentication.

```
(config)> service realport auth value
(config)>
```

where **value** is one of:

- **none**: Do not use authentication. This is the default.
- **shared_secret_sha256**: You must also define the authentication password to ensure secure communication. Leave this field blank to disable authentication.

```
(config)> service realport auth shared_secret_sha256 value
(config)
```

where **value** is the authentication password.

8. Exclusive mode is disabled by default. This mode ensures that any connection from an IP address is closed when opening a new connection from the same IP address. To enable:

```
(config)> service realport exclusive true
(config)
```

9. Use RealPort keepalive to send RealPort keepalive packets. This is enabled by default. To disable:

```
(config)> service realport realport_keepalive false
(config)>
```

10. TCP port keepalive to send TCP keepalive packets is disabled by default. To enable:

```
(config)> service realport tcp_keepalive true
(config)>
```

11. Device initiated connections allow users to remotely connect to serial devices as if they had a native COM/TTY port on their PC. This is disabled by default. To enable:

```
(config)> service realport device_initiated_enable true
(config)>
```

12. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

13. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disconnect a user from a serial port

From the **Serial Status** page, you can disconnect any users connected to a serial port configured for one of these modes: Login, Remote Access, PPP Dial-in, or Modem Emulator.

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the menu, click **Status** > **Connections**> **Serial**. The **Serial Status** page displays.

3. Find the port for which you want to disconnect one or more users. Verify that the port is configured for one of the following modes: Login, Remote Access, PPP Dial-in, or Modem Emulator.
4. Click the down arrow next to the user name in the **Users** column to display a pop-up box.
5. A list of the users currently connected to the port display in the pop-up box. Information about each user's connection displays. If more than one user is connected, a check box displays for each user.
   - **User**: The user's log in name or a connection type, such as Telnet, TCP, or SSH.
   - **Remote IP**: The user's IP address.
   - **Connected**: The length of time that the user has been connected to the port. The time is measured in seconds.
   - **Idle**: The length of time that connection has been idle. The time is measured in seconds.
6. Determine the user(s) that you want to disconnect.
   - If only one user is listed, that user will be selected for the disconnect by default.
   - If more than one user is connected to the port, by default the check box for each user is selected. Click on a check box to deselect a user. Click **All** to deselect or select all of the users.
7. Click **Disconnect**. The single user or set of selected users are disconnected from the serial port.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. (Optional) Review the users currently connected to the port.

   ```
   show serial port
   >
   ```

   Where *port* is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.
3. (Optional) Review information about the disconnect command.

   ```
   > system serial disconnect ?
   >
   ```

4. Disconnect a specific user from a port.

   ```
   >system serial disconnect port remoteip STRING user STRING
   >
   ```

   Where *port*is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.

   Enter one or both of the following:

- *remoteip STRING*: The remote IP address to disconnect.
- *user*: The user name of the user that you want to disconnect.

5. Disconnect all users from a port.

```
system serial disconnect port
>
```

Where *port*: is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.

6. Type **exit** to exit the Admin CLI.Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show serial port status and statistics

To show the status and statistics for the serial port:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the main menu, click **Status** > **Connections** > **Serial**. The **Serial Status** page displays. See Serial Status page for information about the features in this page.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show serial command:

```
> show serial

Label    Port  Enable  Mode   Baudrate
-------- ----- ------ ----- --------
Serial 1  port1  true   login  9600
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Serial Status page

The **Serial Status** page contains status information about all of the serial ports available on the device.

To navigate to the **Serial Status** page, log into the device's web UI and click **Status** > **Connection**> **Serial**.

Item	Description
✷ configuration icon	Click the ✷ (configuration) icon in the upper right corner of the page to access the **Serial Configuration** page. See Serial port for more information.
Status	Displays the connection status. ■ **CONNECTED**: A telnet, terminal, SSH, or TCP session is active. ■ **DISABLED**: The port is not enabled. ■ **NO SIGNAL**: CTS or DCD is not active on the port.
Port	A list of the ports on the device. The port number and name displays as a link when the port is configured for remote access. You can click the port number or name to connect to the port in the terminal page. 1. Click the link to connect to the port in the terminal page. 2. In the terminal screen, enter **~b?** to display additional commands. See Access the terminal screen from the web UI for more information about the commands. While you are connected to the terminal, the port status displays in the **Status** column as CONNECTED, and the name of the user logged into the device displays in the **User** column.
Label	A description for the port. You can change this from the **Serial Configuration** page. Click the ✷ (configuration) icon in the upper right corner of the page to access that page. The port number and name displays as a link when the port is configured for remote access. You can click the port number or name to connect to the port in the terminal page. See the description for Port (above) for more information.
Log	If configured, you can open the **Serial Port Log** page for that port. Options are: ■ **Green Log button**: The serial port mode selected for the port supports serial port logging, and logging is enabled. Click the **Log** button to open the **Serial Port Log** page for that port. See Review the serial port message log for information about that page. ■ **Gray Log button**: The serial port mode selected for the port supports serial port logging, but logging is not enabled. ■ **No button**: The serial port mode selected for the port does not support serial port logging.
User	When the port is connected to a Telnet, terminal, SSH, or TCP connection the name of the user logged into the device displays. See the description for Port (above) for more information. If a serial port is configured for one of these modes: Login, Remote Access, PPP Dial-in, or Modem Emulator, you can disconnect one or more users from the serial port using the **Disconnect** feature. See Disconnect a user from a serial port.
TX/RX Bytes	Displays the total number of bytes that have been transmitted and received.

Item	Description
Signals	Indicates the types of communication that the device is ready to send. DCD: Carrier Detected CTS: Clear to Send DTR: Data Terminal Ready RTS: Ready to Dend

Review the serial port message log

Serial port messages can be reviewed from the **Serial Port Log** page.

A serial port message log is created and saved when serial port logging has been enabled and configured for one of the following serial port modes: Login, Remote Access, RealPort, or UDP Serial. You can view the log file from the **Log** column in the **Serial Status** page.

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the main menu, click **Status**
3. Under **Connections**, click **Serial**. The **Serial Status** page displays.
4. If a green **Log** button is displayed, the serial port mode selected for the port supports serial port logging, and logging is enabled. Click the **Log** button to open the **Serial Port Log** page for that port. The **Serial port log** window displays.

   Note If the **Log** button is gray, the serial port mode selected for the port supports serial port logging, but logging is not enabled. If there is no **Log** button, the serial port mode selected for the port does not support serial port logging.

5. Review the messages in the window.
   - Click **Refresh** to refresh the log display.
   - Click **Download** to download the serial port log to your local device. The log file is saved to the /opt/serial directory. Because this is being save to the device's memory, you should use serial logging for diagnostic purposes, rather than having it permanently enabled.
   - Click **Restart** to clear and restart the serial port log.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To show the serial port's contents and logging status:

```
> system serial show port-number
Logging is active on port-number
>
```

3. To save the log to your local device:

```
> system serial save port-number path
>
```

   If a relative path is provided, /etc/config/serial will be used as the root directory for the path and file. (Required)

   The log file is saved to the /opt/serial directory. Because this is being save to the device's memory, you should use serial logging for diagnostic purposes, rather than having it permanently enabled.

4. To clear and restart the log:

```
> system serial clear port-number
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Routing

This chapter contains the following topics:

IP routing 282
Show the routing table 308
Dynamic DNS 309
Virtual Router Redundancy Protocol (VRRP) 314

IP routing

The IX10 device uses IP routes to decide where to send a packet it receives for a remote network. The process for deciding on a route to send the packet is as follows:

1. The device examines the destination IP address in the IP packet, and looks through the IP routing table to find a match for it.
2. If it finds a route for the destination, it forwards the IP packet to the configured IP gateway or interface.
3. If it cannot find a route for the destination, it uses a default route.
4. If there are two or more routes to a destination, the device uses the route with the longest mask.
5. If there are two or more routes to a destination with the same mask, the device uses the route with the lowest metric.

This section contains the following topics:

Configure a static route 283
Delete a static route 286
Policy-based routing 287
Configure a routing policy 288
Example: Dual WAN policy-based routing 295
Example: Domain-based routing with dual WAN 297
Example: Route traffic to a specific WAN interface based on the client MAC address 300
Routing services 305
Configure routing services 306

Configure a static route

A static route is a manually configured routing entry. Information about the route is manually entered rather than obtained from dynamic routing traffic.

Required configuration items

- The destination address or network.
- The interface to use to reach the destination.

Additional configuration items

- A label used to identify this route.
- The IPv4 address of the gateway used to reach the destination.
- The metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.
- The Maximum Transmission Units (MTU) of network packets using this route.

To configure a static route:

Web

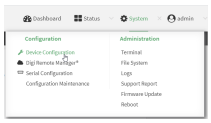
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

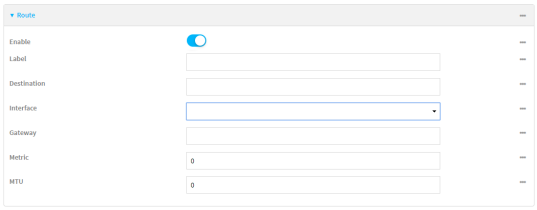
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Routes** > **Static routes**.

4. Click the to add a new static route.

The new static route configuration page is displayed:



New static route configurations are enabled by default. To disable, toggle off **Enable**.

5. (Optional) For **Label**, type a label that will be used to identify this route.
6. For **Destination**, type the IP address or network of the destination of this route.

   For example, to route traffic to the 192.168.47.0 network that uses a subnet mask of 255.255.255.0, type **192.168.47.0/24**. The **any** keyword can also be used to route packets to any destination with this static route.
7. For **Interface**, select the interface on the IX10 device that will be used with this static route.
8. (Optional) For **Gateway**, type the IPv4 address of the gateway used to reach the destination. Set to blank if the destination can be accessed without a gateway.
9. (Optional) For **Metric**, type the metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.
10. (Optional) For **MTU**, type the Maximum Transmission Units (MTU) of network packets using this route.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new static route:

```
(config)> add network route static end
(config network route static 0)>
```

New static route instances are enabled by default. To disable:

```
(config network route static 0)> enable false
(config network route static 0)>
```

4. (Optional) set a label that will be used to identify this route. For example:

```
(config network route static 0)> label "route to accounting network"
(config network route static 0)>
```

5. Set the IP address or network of the destination of this route. For example:

```
(config network route static 0)> destination ip_address[/netmask]
(config network route static 0)>
```

For example, to route traffic to the 192.168.47.0 network that uses a subnet mask of 255.255.255.0:

```
(config network route static 0)> dst 192.168.47.0/24
(config network route static 0)>
```

The **any** keyword can also be used to route packets to any destination with this static route.

6. Set the interface on the IX10 device that will be used with this static route:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config network route static 0)> interface /network/interface/eth1
(config network route static 0)>
```

7. (Optional) Set the IPv4 address of the gateway used to reach the destination. Set to blank if the destination can be accessed without a gateway.

```
(config network route static 0)> gateway IPv4_address
(config network route static 0)>
```

8. (Optional) Set the metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.

```
(config network route static 0)> metric value
(config network route static 0)>
```

where *value* is an interger between **0** and **65535**. The default is **0**.

9. (Optional) Set the Maximum Transmission Units (MTU) of network packets using this route:

```
(config network route static 0)> mtu integer
(config network route static 0)>
```

10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a static route

Web

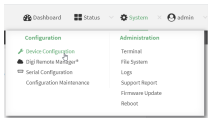
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Routes** > **Static routes**.
4. Click the menu icon (**...**) for a static route and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Determine the index number of the static route to be deleted:

```
(config)> show network route static
0
   dst 10.0.0.1
   enable true
   no gateway
   interface /network/interface/lan1
   label new_static_route
   metric 0
   mtu 0
1
   dst 192.168.5.1
   enable true
   gateway 192.168.5.1
   interface /network/interface/lan2
   label new_static_route_1
   metric 0
   mtu 0
(config)>
```

4. Use the index number to delete the static route:

```
(config)> del network route static 0
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Policy-based routing

Normally, a routing device determines how to route a network packet based on its destination address. However, you can use policy-based routing to forward the packet based on other criteria, such as the source of the packet. For example, you can configure the IX10 device so that high-priority traffic is routed through the cellular connection, while all other traffic is routed through an Ethernet (WAN) connection.

Policy-based routing for the IX10 device uses the following criteria to determine how to route traffic:

- Firewall zone (for example, internal/outbound traffic, external/inbound traffic, or IPSec tunnel traffic).
- Network interface (for example, the cellular connection, the WAN, or the LAN).

- IPv4 address.
- IPv6 address.
- MAC address.
- Domain.
- Protocol type (TCP, UDP, ICMP, or all).

The order of the policies is important. Routing policies are processed sequentially; as a result, if a packet matches an earlier policy, it will be routed using that policy's rules. It will not be processed by any subsequent rules.

Configure a routing policy

Required configuration items

- The packet matching parameters. It can any combination of the following:
  - Source interface.
  - Source address. This can be a firewall zone, an interface, a single IPv4/IPv6 address or network, or a MAC address.
  - Destination address. This can be a firewall zone, an interface, a single IPv4/IPv6 address or network, or a domain.
  - Protocol. This can be **any**, **tcp**, **udp** or **icmp**.
  - Source port. This is only used if the protocol is set to **tcp** or **udp**.
  - Destination port. This is only used if protocol is set to **tcp** or **udp**.
- The network interface used to reach the destination.

Additional configuration items

- A label for the routing policy.
- Whether packets that match this policy should be dropped when the gateway interface is disconnected, rather than forwarded through other interfaces.

To configure a routing policy:

Web

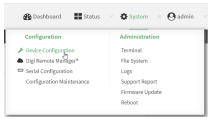
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Routes** > **Policy-based routing**.
4. Click the to add a new route policy.

The new route policy page is displayed:

New route policies are enabled by default. To disable, toggle off **Enable**.

5. (Optional) For **Label**, type a label that will be used to identify this route policy.
6. For **Interface**, select the interface on the IX10 device that will be used with this route policy.
7. (Optional) Enable **Exclusive** to configure the policy to drop packets that match the policy when the gateway interface is disconnected, rather than forwarded through other interfaces.
8. For **IP version**, select **Any**, **IPv4**, or **IPv6**.
9. For **Protocol**, select **Any**, **TCP**, **UDP**, or **ICMP**.
   - If **TCP** or **UDP** is selected for **Protocol**, type the port numbers of the **Source port** and **Destination port**, or set to **any** to match for any port.
   - If **ICMP** is selected for **Protocol**, type the ICMP type and optional code, or set to **any** to match for any ICMP type.
10. For **DSCP**, type the 6-bit hexadecimal Differentiated Services Code Point (DSCP) field match criteria. This will match packets based on the DHCP field within the ToS field of the IP header.
11. Configure source address information:
    a. Click to expand **Source address**.
    b. For **Type**, select one of the following:
       - **Zone**: Matches the source IP address to the selected firewall zone. See Firewall configuration for more information about firewall zones.
       - **Interface**: Matches the source IP address to the selected interface's network address.
       - **IPv4 address**: Matches the source IP address to the specified IP address or network. Use the format ***IPv4_address*[/*netmask*]**, or use **any** to match any IPv4 address.

- **IPv6 address**: Matches the source IP address to the specified IP address or network. Use the format ***IPv6_address*[/*prefix_length*]**, or use **any** to match any IPv6 address.
- **MAC address**: Matches the source MAC address to the specified MAC address.

12. Configure the destination address information:
    a. Click to expand **Destination address**.
    b. For **Type**, select one of the following:
        - **Zone**: Matches the destination IP address to the selected firewall zone. See Firewall configuration for more information about firewall zones.
        - **Interface**: Matches the destination IP address to the selected interface's network address.
        - **IPv4 address**: Matches the destination IP address to the specified IP address or network. Use the format *IPv4_address*/[*netmask*], or use **any** to match any IPv4 address.
        - **IPv6 address**: Matches the destination IP address to the specified IP address or network. Use the format *IPv6_address*/[*prefix_length*], or use **any** to match any IPv6 address.
        - **Domain**: Matches the destination IP address to the specified domain names. To specify domains:
            i. Click to expand **Domains**.
            ii. Click the to add a domain.
            iii. For **Domain**, type the domain name.
            iv. Repeat to add additional domains.
        - **Default route**: Matches packets destined for the default route, excluding routes for local networks.
13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

New route policies are enabled by default. To disable:

```
(config network route policy 0)> enable false
(config network route policy 0)>
```

4. (Optional) Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "New route policy"
(config network route policy 0)>
```

5. Set the interface on the IX10 device that will be used with this route policy:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config network route policy 0)> interface /network/interface/eth1
(config network route policy 0)>
```

6. (Optional) Enable **exclusive** to configure the policy to drop packets that match the policy when the gateway interface is disconnected, rather than forwarded through other interfaces:

```
(config network route policy 0)> exclusive true
(config network route policy 0)>
```

7. Select the IP version:

```
(config network route policy 0)> ip_version value
(config network route policy 0)>
```

where *value* is one of **any**, **ipv4**, or **ipv6**.

8. Set the protocol:

```
(config network route policy 0)> protocol value
(config network route policy 0)>
```

where *value* is one of:

- **any**: All protocols are matched.
- **tcp**: Source and destination ports are matched:
  a. Set the source port:

```
(config network route policy 0)> src_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the source port.
  b. Set the destination port:

```
(config network route policy 0)> dst_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the destination port.

- **upd**: Source and destination ports are matched:
  a. Set the source port:

```
(config network route policy 0)> src_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the source port.
  b. Set the destination port:

```
(config network route policy 0)> dst_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the destination port.
- **icmp**: The ICMP protocol is matched. Identify the ICMP type:

```
(config network route policy 0)> icmp_type value
(config network route policy 0)>
```

  where *value* is the ICMP type and optional code, or set to **any** to match for any ICMP type.

9. Set the source address type:

```
(config network route policy 0)> src type value
(config network route policy 0)>
```

where *value* is one of:

- **zone**: Matches the source IP address to the selected firewall zone. Set the zone:
  a. Use the **?** to determine available zones:

```
(config network route policy 0)> src zone ?

Zone: Match the IP address to the specified firewall zone.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup

Default value: any
Current value: any

(config network route policy 0)> src zone
```

b. Set the zone. For example:

```
(config network route policy 0)> src zone external
(config network route policy 0)>
```

See Firewall configuration for more information about firewall zones.

- **interface**: Matches the source IP address to the selected interface's network address. Set the interface:
  a. Use the **?** to determine available interfaces:
  b. Set the interface. For example:

```
(config network route policy 0)> src interface /network/interface/eth1
(config network route policy 0)>
```

- **address**: Matches the source IPv4 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> src address value
(config network route policy 0)>
```

  where value uses the format ***IPv4_address*[*/netmask*]**, or **any** to match any IPv4 address.
- **address6**: Matches the source IPv6 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> src address6 value
(config network route policy 0)>
```

  where value uses the format ***IPv6_address*[*/prefix_length*]**, or **any** to match any IPv6 address.
- **mac**: Matches the source MAC address to the specified MAC address. Set the MAC address to be matched:

```
(config network route policy 0)> src mac MAC_address
(config network route policy 0)>
```

10. Set the destination address type:

```
(config network route policy 0)> dst type value
(config network route policy 0)>
```

where *value* is one of:

- **zone**: Matches the destination IP address to the selected firewall zone. Set the zone:
  a. Use the **?** to determine available zones:

```
(config network route policy 0)> dst zone ?

Zone: Match the IP address to the specified firewall zone.
Format:
  any
```

```
dynamic_routes
edge
external
internal
ipsec
loopback
setup

Default value: any
Current value: any

(config network route policy 0)> dst zone
```

b. Set the zone. For example:

```
(config network route policy 0)> dst zone external
(config network route policy 0)>
```

See Firewall configuration for more information about firewall zones.

- **interface**: Matches the destination IP address to the selected interface's network address. Set the interface:
  a. Use the **?** to determine available interfaces:
  b. Set the interface. For example:

```
(config network route policy 0)> dst interface /network/interface/eth1
(config network route policy 0)>
```

- **address**: Matches the destination IPv4 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> dst address value
(config network route policy 0)>
```

where value uses the format ***IPv4_address*[*/netmask*]**, or **any** to match any IPv4 address.

- **address6**: Matches the destination IPv6 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> dst address6 value
(config network route policy 0)>
```

where value uses the format ***IPv6_address*[*/prefix_length*]**, or **any** to match any IPv6 address.

- **mac**: Matches the destination MAC address to the specified MAC address. Set the MAC address to be matched:

```
(config network route policy 0)> dst mac MAC_address
(config network route policy 0)>
```

11. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example: Dual WAN policy-based routing

This example routes traffic to a specific IP address to go through the cellular WWAN interface, while all other traffic uses the Ethernet WAN interface.

Web

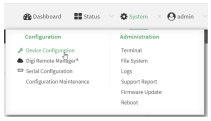
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

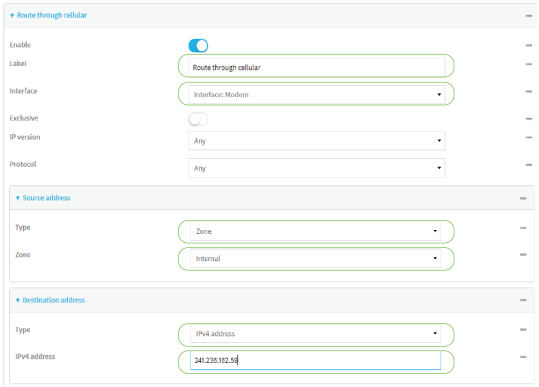
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Routes** > **Policy-based routing**.
4. Click the to add a new route policy.

5. For **Label**, type **Route through cellular**.

6. For **Interface**, select .
7. Configure the source address:
   a. Click to expand **Source address**.
   b. For **Type**, select **Zone**.
   c. For **Zone**, select **Internal**.
8. Configure the destination address:
   a. Click to expand **Destination address**.
   b. For **Type**, select **IPv4 address**.
   c. For **IPv4 address**, type the IP address that will be the destination for outgoing traffic routed through the WWAN interface. In the above example, this is 241.236.162.59.



9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create the route policy:
   a. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

   b. Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "Route through cellular"
(config network route policy 0)>
```

c. Set the interface:

```
(config network route policy 0)> interface /network/interface/
(config network route policy 0)>
```

d. Configure the source address:

i. Set the source type to **zone**:

```
(config network route policy 0)> src type zone
(config network route policy 0)>
```

ii. Set the zone to **internal**:

```
(config network route policy 0)> src zone internal
(config network route policy 0)>
```

e. Configure the destination address:

i. Set the destination to use an IPv4 address:

```
(config network route policy 0)> dst type address
(config network route policy 0)>
```

ii. Set the IP address that will be the destination for outgoing traffic routed through the WWAN interface. In the above example, this is 241.236.162.59.

```
(config network route policy 0)> dst address 241.236.162.59
(config network route policy 0)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example: Domain-based routing with dual WAN

This example routes traffic destined for a specific domain to the WAN Ethernet port, and never through the cellular modem.

Web

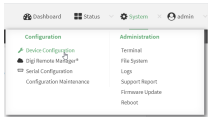
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

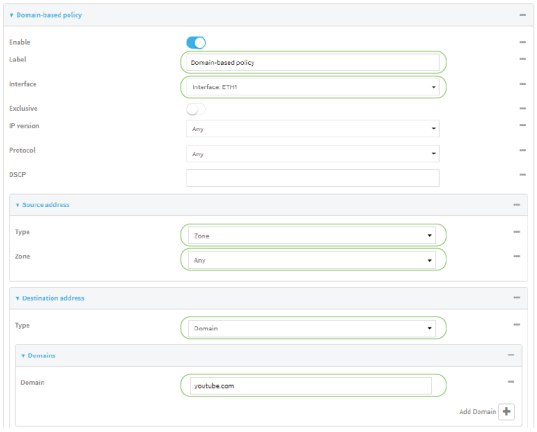
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

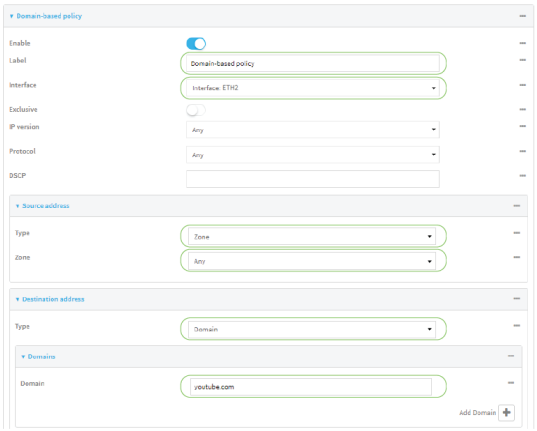


The **Configuration** window is displayed.

3. Click **Network** > **Routes** > **Policy-based routing**.
4. Click the to add a new route policy.

5. For **Label**, type **Domain-based policy**.
6. For **Interface**, select **ETH1**.
7. Configure the source address:
   a. Click to expand **Source address**.
   b. For **Type**, select **Zone**.
   c. For **Zone**, select **Any**.
8. Configure the destination address:
   a. Click to expand **Destination address**.
   b. For **Type**, select **Domain**.
   c. Click to expand **Domains**.
   d. Click the to add a new domain.
   e. For **Domain**, type **youtube.com**.
   You can add additional domains by repeating the last two steps.





9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create the route policy:
   a. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

b. Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "Domain-based policy"
(config network route policy 0)>
```

c. Set the interface:

```
(config network route policy 0)> interface /network/interface/eth1
(config network route policy 0)>
```

d. Leave the source address type at the default of **zone**.

e. Leave the source address zone at the default of **any**.

f. Configure the destination address:

i. Set the destination to use a domain:

```
(config network route policy 0)> dst type domain
(config network route policy 0)>
```

ii. Add a domain and set it to **youtube.com**:

```
(config network route policy 0)> add dst domain end youtube.com
(config network route policy 0)>
```

You can add additional domains by repeating this step with a different domain name.

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example: Route traffic to a specific WAN interface based on the client MAC address

This example routes all data from a certain client device through a cellular WAN based on the device's MAC address, while all other client devices are routed through the Ethernet WAN.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

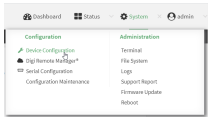
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

   b. Click the **Device ID**.

c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

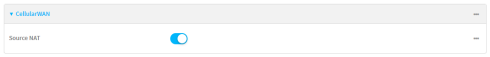
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



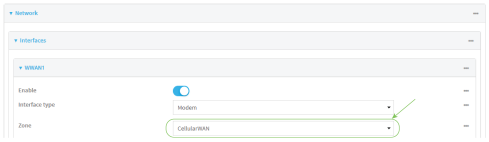
The **Configuration** window is displayed.

3. Create new firewall zones:
   a. Create a firewall zone named CellularWAN with Source NAT enabled:
      i. Click **Firewall** > **Zones**.
      ii. For **Add Zone**, type **CellularWAN** and click .

      iii. Enable Source **NAT**.



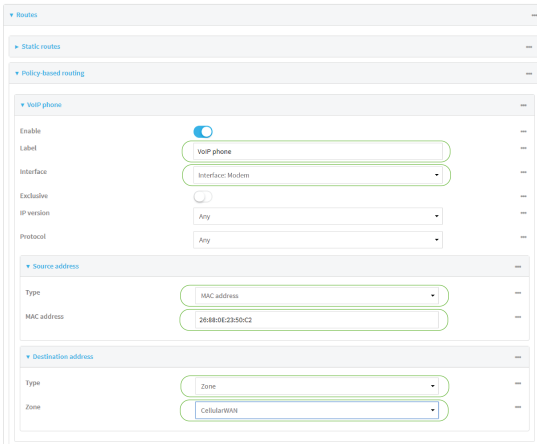
   b. Create second firewall zone named EthernetWAN with Source NAT enabled:
      i. For **Add Zone**, type **EthernetWAN** and click .
      ii. Enable Source **NAT**.
4. Configure the WAN interfaces to use the new zones:
   a. Configure the cellular WAN interface:
      i. Click **Network** > **Interfaces** > .
      ii. For **Zone**, select **CellularWAN**.



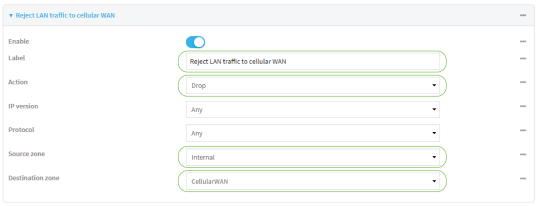
   b. Configure the Ethernet WAN interface:
      i. Click **Network** > **Interfaces** > .
      ii. For **Zone**, select **EthernetWAN**.

5. Configure the policy-based route for traffic from the client device that will be sent over the cellular WAN:
   a. Click **Network** > **Routes** > **Policy-based routing**.
   b. Click the to add a new route policy.

   c. For **Label**, type **VoIP phone**.
   d. For **Interface**, select .
   e. Configure the source as the MAC address of the VoIP phone:
      i. Click to expand **Source address**.
      ii. For **Type**, select **MAC address**.
      iii. For **MAC address**, type **26:88:0E:23:50:C2**.
   f. Configure the destination zone:
      i. Click to expand **Destination address**.
      ii. For **Type**, select **Zone**.
      iii. For **Zone**, select **CellularWAN**.



6. Create a packet filtering rule that rejects all other LAN packets on the cellular WAN interface.
   a. Click **Firewall** > **Packet filtering**.
   b. Click the to add a new packet filtering rule.
   c. For **Label**, type **Reject LAN traffic to cellular WAN**.
   d. For **Action**, select **Drop**.
   e. For **Source zone**, select **Internal**.
   f. For **Destination zone**, select **CellularWAN**.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create new firewall zones:
   a. Create a firewall zone named CellularWAN with Source NAT enabled:
      i. Create the firewall zone:

```
(config)> add firewall zone CellularWAN
(config firewall zone CellularWAN)>
```

      i. Enable Source NAT on the new zone:

```
(config firewall zone CellularWAN)> src_nat true
(config firewall zone CellularWAN)>
```

   b. Create second firewall zone named EthernetWAN with Source NAT enabled:
      i. Type **..** to move back one node in the configuration:

```
(config firewall zone CellularWAN)> ..
(config firewall zone)>
```

      ii. Create the firewall zone:

```
(config firewall zone)> add EthernetWAN
(config firewall zone EthernetWAN)>
```

      i. Enable Source NAT on the new zone:

```
(config firewall zone EthernetWAN)> src_nat true
(config firewall zone EthernetWAN)>
```

4. Configure the WAN interfaces to use the new zones:
   a. Set the zone for the cellular WAN interface:
      i. Type **...** to move to the root of the configuration:

```
(config firewall zone EthernetWAN)> ...
(config)>
```

      ii. Set the zone:

```
(config)> network interface  zone CellularWAN
(config)>
```

   b. Set the zone for the Ethernet WAN interface:

```
(config)> network interface  zone EthernetWAN
(config)>
```

5. Configure the policy-based route for traffic from the client device that will be sent over the cellular WAN:
   a. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

   b. Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "VoIP phone"
(config network route policy 0)>
```

   c. Set the interface:

```
(config network route policy 0)> interface /network/interface/
(config network route policy 0)>
```

   d. Configure the source as the MAC address of the VoIP phone:
      i. Set the source type to **mac**:

```
(config network route policy 0)> src type mac
(config network route policy 0)>
```

      ii. Set the MAC address to the MAC address of the VoIP phone:

```
(config network route policy 0)> src mac 26:88:0E:23:50:C2
(config network route policy 0)>
```

   e. Configure the destination zone:
      i. Set the source destination to **zone**:

```
(config network route policy 0)> dst type zone
(config network route policy 0)>
```

ii. Set the zone to **CellularWAN**:

```
(config network route policy 0)> dst zone CellularWAN
(config network route policy 0)>
```

6. Create a packet filtering rule that rejects all other LAN packets on the cellular WAN interface:
   a. Create a new packet filtering rule:
      i. Type **...** to move to the root of the configuration:

```
(config network route policy 0)> ...
(config)>
```

      ii. Create the packet filtering rule:

```
(config)> add firewall filter end
(config firewall filter 2)>
```

   b. Set the lable to **Reject LAN traffic to cellular WAN**:

```
(config firewall filter 2)> label "Reject LAN traffic to cellular WAN"
(config firewall filter 2)>
```

   c. Set the action to **drop**:

```
(config firewall filter 2)> action drop
(config firewall filter 2)>
```

   d. Set the source zone to **internal**:

```
(config firewall filter 2)> src_zone internal
(config firewall filter 2)>
```

   e. Set the destination zone to **CellularWAN**:

```
(config firewall filter 2)> dst_zone CellularWAN
(config firewall filter 2)>
```

7. Save the configuration and apply the change.

```
(config firewall filter 2)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Routing services

Your IX10 includes support for dynamic routing services and protocols. The following routing services are supported:

Service or protocol	Information
BGP	The Border Gateway Protocol (BGP) service supports BGP-4 (RFC1771).
IS-IS	The IPv4 and IPv6 Intermediate System to Intermediate System (IS-IS) service (RFC1142).
NHRP	Next Hop Resolution Protocol (NHRP) (RFC2332). Does not support NHRP authentication.
OSPFv2	The IPv4 Open Shortest Path First (OSPF) service supports OSPFv2 (RFC2328).
OSPFv3	The IPv6 Open Shortest Path First (OSPF) service supports OSPFv3 (RFC2740).
RIP	The IPv4 Routing Information Protocol (RIP) service supports RIPv2 (RFC2453) and RIPv1 (RFC1058).
RIPng	The IPv6 Routing Information Protocol (RIP) service supports RIPng (RFC2080).

Configure routing services

Required configuration items

- Enable routing services.
- Enable and configure the types of routing services that will be used.

Web

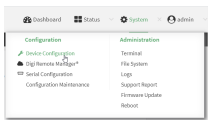
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

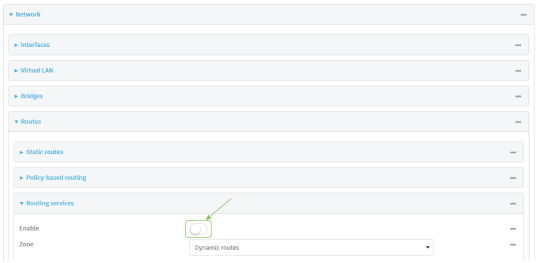
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Routes** > **Routing services**.

4. Click **Enable**.



The default firewall zone setting, **Dynamic routes**, is specifically designed to work with routing services and should be left as the default.

5. Configure the routing services that will be used:
   a. Click to expand a routing service.
   b. **Enable** the routing service.
   c. Complete the configuration of the routing service.
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable routing services:

```
(config)> network route service enable true
(config)>
```

4. Configure routing services that will be used:
   a. Use the **?** to display available routing services:

```
(config)> network route service ?

Routing services: Settings for dynamic routing services and protocols.

 Parameters            Current Value
 ------------------------------------------------------------------------------
 enable                true          Enable
 zone                  dynamic_routes  Zone

 Additional Configuration
 ------------------------------------------------------------------------------
 bgp                   BGP
```

```
isis            IS-IS
nhrp            NHRP
ospfv2          OSPFv2
ospfv3          OSPFv3
rip             RIP
ripng           RIPng

(config)>
```

b. Enable a routing service that will be used. For example, to enable the RIP service:

```
(config)> network route service rip enable true
(config)>
```

c. Complete the configuration of the routing service. For example, use the **?** to view the available parameters for the RIP service:

```
(config)> network route service rip ?

Parameters          Current Value
-------------------------------------------------------------------------------
ecmp            false       Allow ECMP
enable          true        Enable

Additional Configuration
-------------------------------------------------------------------------------
interface       Interfaces
neighbour       Neighbours
redis           Route redistribution
timer           Timers

(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show the routing table

To display the routing table:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

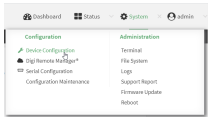
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **Status** > **Routes**.

   The **Network Routing** window is displayed.

4. Click **IPv4 Load Balance** to view IPv4 load balancing.
5. Click **IPv6 Load Balance** to view IPv6 load balancing.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type show route:

   You can limit the display to only IPv4 entries by using **show route ipv4**, or to IPv6 entries by using **show route ipv6**. You can also display more information by adding the **verbose** option to the **show route** and **show route *ip_type*** commands.

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Dynamic DNS

WARNING! The Dynamic Domain Name System uses unencrypted HTTP communication. Please ensure you are utilizing a VPN to secure your communications.

The Domain Name System (DNS) uses name servers to provide a mapping between computer-readable IP addresses and human-readable hostnames. This allows users to access websites and personal networks with easy-to-remember URLs. Unfortunately, IP addresses change frequently,

invalidating these mappings when they do. Dynamic DNS has become the standard method of addressing this problem, allowing devices to update name servers with their new IP addresses.

By providing the IX10 device with the domain name and credentials obtained from a dynamic DNS provider, the router can automatically update the remote nameserver whenever your WAN or public IP address changes.

Your IX10 device supports a number of Dynamic DNS providers as well as the ability to provide a custom provider that is not included on the list of providers.

Configure dynamic DNS

This section describes how to cofigure dynamic DNS on a IX10 device.

Required configuration items

- Add a new Dynamic DNS service.
- The interface that has its IP address registered with the Dynamic DNS provider.
- The name of a Dynamic DNS provider.
- The domain name that is linked to the interface's IP address.
- The username and password to authenticate with the Dynamic DNS provider.

Additional configuration items

- If the Dynamic DNS service provider is set to **custom**, identify the URL that should be used to update the IP address with the Dynamic DNS provider.
- The amount of time to wait to check if the interface's IP address needs to be updated.
- The amount of time to wait to force an update of the interface's IP address.
- The amount of time to wait for an IP address update to succeed before retrying the update.
- The number of times to retry a failed IP address update.

Web

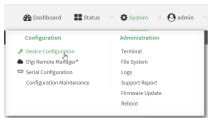
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

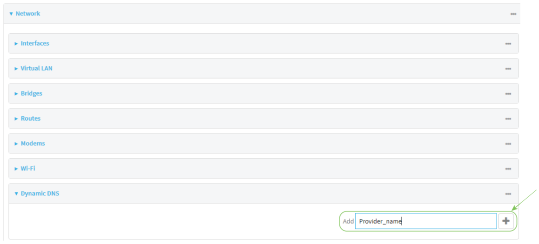
   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

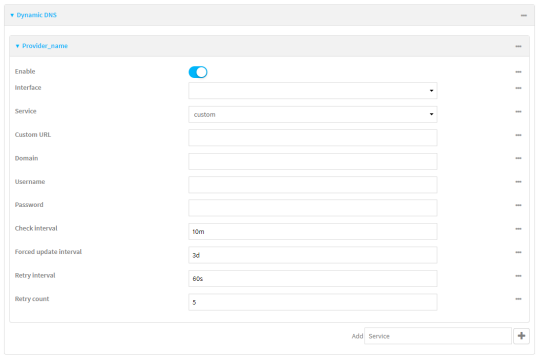


The **Configuration** window is displayed.

3. Click **Network** > **Dynamic DNS**.
4. Type a name for this Dynamic DNS instance in **Add Service** and click .



The Dynamic DNS configuration page displays.



New Dynamic DNS configurations are enabled by default. To disable, toggle off **Enable**.

5. For **Interface**, select the interface that has its IP address registered with the Dynamic DNS provider.
6. For **Service**, select the Dynamic DNS provider, or select **custom** to enter a custom URL for the Dynamic DNS provider.
7. If **custom** is selected for **Service**, type the **Custom URL** that should be used to update the IP address with the Dynamic DNS provider.
8. Type the **Domain** name that is linked to the interface's IP address.
9. Type the **Username** and **Password** used to authenticate with the Dynamic DNS provider.
10. (Optional) For **Check Interval**, type the amount of time to wait to check if the interface's IP address needs to be updated.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Check interval** to ten minutes, enter **10m** or **600s**.
11. (Optional) For **Forced update interval**, type the amount of time to wait to force an update of the interface's IP address.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Forced update interval** to ten minutes, enter **10m** or **600s**.

The setting for **Forced update interval** must be larger than the setting for **Check Interval**.

12. (Optional) For **Retry interval**, type the amount of time to wait for an IP address update to succeed before retrying the update.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Retry interval** to ten minutes, enter **10m** or **600s**.
13. (Optional) For **Retry count**, type the number of times to retry a failed IP address update.
14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new Dynamic DNS instance. For example, to add an instance named **new_ddns_instance**:

```
(config)> add network ddns new_ddns_instance
(config network ddns new_ddns_instance)>
```

   New Dynamic DNS instances are enabled by default. To disable:

```
(config network ddns new_ddns_instance)> enable false
(config network ddns new_ddns_instance)>
```

4. Set the interface for the Dynamic DNS instance:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config network ddns new_ddns_instance)> interface eth1
(config network ddns new_ddns_instance)>
```

5. Set the Dynamic DNS provider service:
   a. Use the **?** to determine available services:

```
(config network ddns new_ddns_instance)> service ?

Service: The provider of the dynamic DNS service.
Format:
 custom
```

```
3322.org
changeip.com
ddns.com.br
dnsdynamic.org
...

Default value: custom
Current value: custom

(config network ddns new_ddns_instance)> service
```

b. Set the service:

```
(config network ddns new_ddns_instance)> service service_name
(config network ddns new_ddns_instance)>
```

6. If **custom** is configured for **service**, set the custom URL that should be used to update the IP address with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> custom url
(config network ddns new_ddns_instance)>
```

7. Set the domain name that is linked to the interface's IP address:

```
(config network ddns new_ddns_instance)> domain domain_name
(config network ddns new_ddns_instance)>
```

8. Set the username to authenticate with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> username name
(config network ddns new_ddns_instance)>
```

9. Set the password to authenticate with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> password pwd
(config network ddns new_ddns_instance)>
```

10. (Optional) Set the amount of time to wait to check if the interface's IP address needs to be updated:

```
(config network ddns new_ddns_instance)> check_interval value
(config network ddns new_ddns_instance)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **check_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> check_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **10m**.

11. (Optional) Set the amount of time to wait to force an update of the interface's IP address:

```
(config network ddns new_ddns_instance)> force_interval value
(config network ddns new_ddns_instance)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **force_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> force_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **3d**.

12. (Optional) Set the amount of time to wait for an IP address update to succeed before retrying the update:

```
(config network ddns new_ddns_instance)> retry_interval value
(config network ddns new_ddns_instance)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **retry_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> retry_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **60s**.

13. (Optional) Set the number of times to retry a failed IP address update:

```
(config network ddns new_ddns_instance)> retry_count value
(config network ddns new_ddns_instance)>
```

where *value* is any interger. The default is **5**.

14. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

15. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is a standard for gateway device redundancy and failover that creates a "virtual router" with a floating IP address. Devices connected to the LAN then use this virtual router as their default gateway. Responsibility for the virtual router is assigned to one of the VRRP-enabled devices on a LAN (the "master router"), and this responsibility transparently fails over to backup VRRP devices if the master router fails. This prevents the default gateway from being a single point of failure, without requiring configuration of dynamic routing or router discovery protocols on every host.

Multiple IX10 devices can be configured as VRRP devices and assigned a priority. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of

the virtual router is mapped to the backup device with the next highest priority. Each VRRP router is configured with a unique LAN IP address, and the same shared VRRP address.

VRRP+

VRRP+ is an extension to the VRRP standard that uses network probing to monitor connections through VRRP-enabled devices and can dynamically change the priority of the devices, including changing devices from master to backup, and from backup to master, even if the device has not failed. For example, if a host becomes unreachable on the far end of a network link, then the physical default gateway can be changed by adjusting the VRRP priority of the IX10 device connected to the failing link. This provides failover capabilities based on the status of connections behind the router, in addition to the basic VRRP device failover. For IX10 devices, SureLink is used to probe network connections.

VRRP+ can be configured to probe a specified IP address by either sending an ICMP echo request (ping) or attempting to open a TCP socket to the IP address.

Configure VRRP

This section describes how to configure VRRP on a IX10 device.

Required configuration items

- Enable VRRP.
- The interface used by VRRP.
- The Router ID that identifies the virtual router instance. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool.
- The VRRP priority of this device.
- The shared virtual IP address for the VRRP virtual router. Devices connected to the LAN will use this virtual IP address as their default gateway.

See Configure VRRP+ for information about configuring VRRP+, an extension to VRRP that uses network probing to monitor connections through VRRP-enabled devices and dynamically change the VRRP priorty of devices based on the status of their network connectivity.

Web

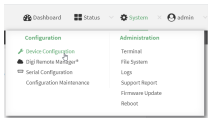
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

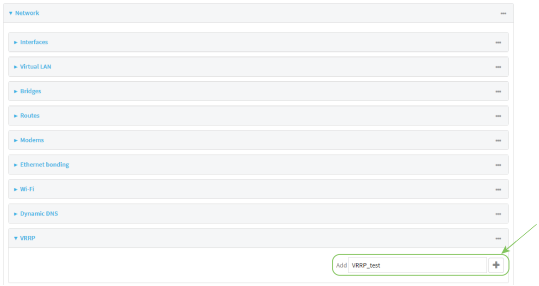
   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

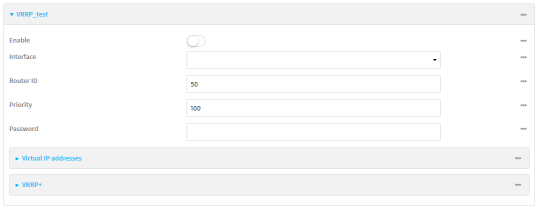


The **Configuration** window is displayed.

3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click ⚡.

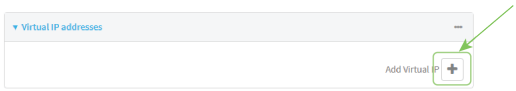


The new VRRP instance configuration is displayed.



5. Click **Enable**.
6. For **Interface**, select the interface on which this VRRP instance should run.
7. For **Router ID** field, type the ID of the virtual router instance. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool. Allowed values are from **1** and **255**, and it is configured to **50** by default.
8. For **Priority**, type the priority for this router in the group. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of the virtual router is mapped to the backup device with the next highest priority. If this device's actual IP address is being used as the virtual IP address of the VRRP pool, then the priority of this device should be set to **255** . Allowed values are from **1** and **255**, and it is configured to **100** by default.
9. (Optional) For **Password**, type a password that will be used to authenticate this VRRP router with VRRP peers. If the password length exceeds 8 characters, it will be truncated to 8 characters.

10. Configure the virtual IP addresses associated with this VRRP instance:
    a. Click to expand **Virtual IP addresses**.
    b. Click to add a virtual IP address.



    c. For **Virtual IP**, type the IPv4 or IPv6 address for a virtual IP of this VRRP instance.
    d. (Optional) Repeat to add additional virtual IPs.
11. See Configure VRRP+ for information about configuring VRRP+.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a VRRP instance. For example:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the interface on which this VRRP instance should run:
    a. Use the **?** to determine available interfaces:
    b. Set the interface, for example:

```
(config network vrrp VRRP_test)> interface /network/interface/eth
(config network vrrp VRRP_test)>
```

    c. Repeat for additional interfaces.
6. Set the router ID. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool. Allowed values are from **1** and **255**, and it is configured to **50** by default.

```
(config network vrrp VRRP_test)> router_id int
(config network vrrp VRRP_test)>
```

7. Set the priority for this router in the group. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of the virtual router is

mapped to the backup device with the next highest priority. If this device's actual IP address is being used as the virtual IP address of the VRRP pool, then the priority of this device should be set to **255** . Allowed values are from **1** and **255**, and it is configured to **100** by default.

```
(config network vrrp VRRP_test)> priority int
(config network vrrp VRRP_test)>
```

8. (Optional) Set a password that will be used to authenticate this VRRP router with VRRP peers. If the password length exceeds 8 characters, it will be truncated to 8 characters.

```
(config network vrrp VRRP_test)> password pwd
(config network vrrp VRRP_test)>
```

9. Add a virtual IP address associated with this VRRP instance. This can be an IPv4 or IPv6 address.

```
(config network vrrp VRRP_test)> add virtual_address end ip_address
(config network vrrp VRRP_test)>
```

   Additional virtual IP addresses can be added by repeating this step with different values for *ip_address*.

10. Save the configuration and apply the change.

```
(config network vrrp new_vrrp_instance)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure VRRP+

VRRP+ is an extension to the VRRP standard that uses SureLink network probing to monitor connections through VRRP-enabled devices and adjust devices' VRRP priority based on the status of the SureLink tests.

This section describes how to configure VRRP+ on a IX10 device.

Required configuration items

- Both master and backup devices:
  - A configured and enabled instance of VRRP. See Configure VRRP for information.
  - Enable VRRP+.
  - WAN interfaces to be monitored by using VRRP+.

    Note SureLink is enabled by default on all WAN interfaces, and should not be disabled on the WAN interfaces that are being monitored by VRRP+.

    If multiple WAN interfaces are being monitored on the same device, the VRRP priority will be adjusted only if all WAN interfaces fail SureLink tests.

- The amount that the VRRP priority will be modified when SureLink determines that the VRRP interface is not functioning correctly.
- Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses.

- Backup devices only:
  - Enable and configure SureLink on the VRRP interface.
  - Set the IP gateway to the IP address of the VRRP interface on the master device.

Additional configuration items

- For backup VRRP devices, enable the ability to monitor the VRRP master, so that a backup device can increase its priority when the master device fails SureLink tests.

Web

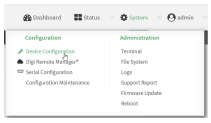
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

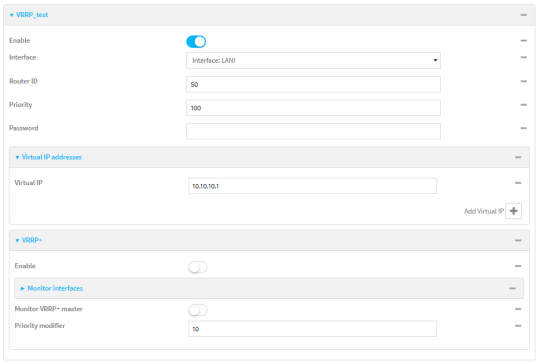
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

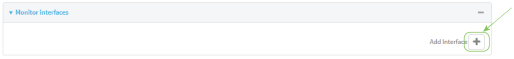
   The **Configuration** window is displayed.
3. Click **Network** > **VRRP**.
4. Create a new VRRP instance, or click to expand an existing VRRP instance.

   See Configure VRRP for information about creating a new VRRP instance.

5. Click to expand **VRRP+**.



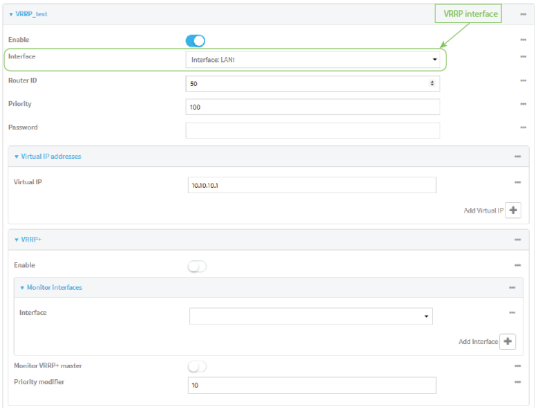
6. Click **Enable**.
7. Add interfaces to monitor:
   a. Click to expand **Monitor interfaces**.
   b. Click ⋎ to add an interface for monitoring.



   c. For **Interface**, select the local interface to monitor. Generally, this will be a cellular or WAN interface.
   d. (Optional) Click ⋎ again to add additional interfaces.
8. (Optional) For backup devices, click to enable **Monitor VRRP+ master**.

   This parameter allows a backup VRRP device to monitor the master device, and increase its priority when the master device is failing SureLink tests. This can allow a device functioning as a backup device to promote itself to master.
9. For **Priority modifier**, type or select the amount that the device's priority should be decreased due to SureLink connectivity failure, and increased when SureLink succeeds again.

   Along with the priority settings for devices in this VRRP pool, the amount entered here should be large enough to automatically demote a master device when SureLink connectivity fails. For example, if the VRRP master device has a priority of **100** and the backup device has a priority of **80**, then the **Priority modifier** should be set to an amount greater than **20** so that if SureLink fails on the master, it will lower its priority to below **80**, and the backup device will assume the master role.
10. Configure the VRRP interface. The VRRP interface is defined in the **Interface** parameter of the VRRP configuration, and generally should be a LAN interface:

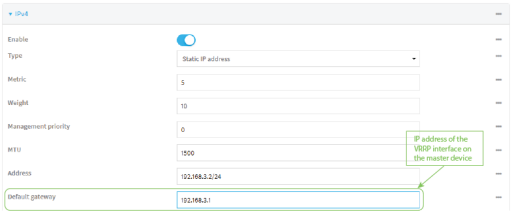


To configure the VRRP interface:

a. Click to expand **Network** > **Interfaces**.

b. Click to expand the appropriate VRRP interface (for example, **LAN1**).

c. For backup devices, for **Default Gateway**, type the IP address of the VRRP interface on the master device.

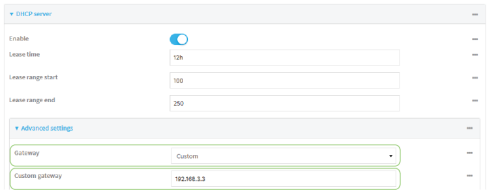


d. Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses:

   i. Click to expand **DHCP Server** > **Advanced settings**.

   ii. For **Gateway**, select **Custom**.

   iii. For **Custom gateway**, enter the IP address of one of the virtual IPs used by this VRRP instance.



e. For backup devices, enable and configure SureLink on the VRRP interface. Generally, this should be a LAN interface; VRRP+ will then monitor the LAN using SureLink to determine if the interface has network connectivity and promote a backup to master if SureLink fails.

   i. Click to expand **IPv4** > **SureLink**.

   ii. Click **Enable**.

iii. For **Interval**, type a the amount of time to wait between connectivity tests. To guarantee seamless internet access for VRRP+ purposes, SureLink tests should occur more often than the default of 15 minutes.

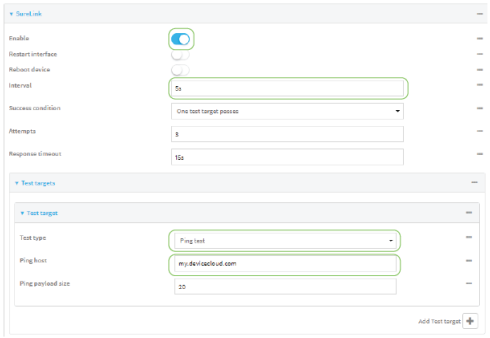
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}. For example, to set **Interval** to five seconds, enter **5s**.

iv. Click to expand **Test targets** > **Test target**.

v. Configure the test target. For example, to configure SureLink to verify internet connectivity on the LAN by pinging https://remotemanager.digi.com:

i. For **Test Type**, select **Ping test**.

ii. For **Ping host**, type **https://remotemanager.digi.com**.



11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new VRRP instance, or edit an existing one. See Configure VRRP for information about creating a new VRRP instance.

4. Enable VRRP+:

```
(config)> network vrrp VRRP_test vrrp_plus enable true
(config)>
```

5. Add interfaces to monitor. Generally, this will be a cellular or WAN interface.

   a. Use the **?** to determine available interfaces:

   b. Set the interface, for example:

```
(config)> add network vrrp VRRP_test vrrp_plus monitor_interface end
/network/interface/modem
(config)>
```

c. (Optional) Repeat for additional interfaces.

6. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success:

```
(config)> network vrrp VRRP_test vrrp_plus weight value
(config)>
```

where *value* is an integer between **1** and **254**. The default is **10**.

Along with the priority settings for devices in this VRRP pool, the amount entered here should be large enough to automatically demote a master device when SureLink connectivity fails. For example, if the VRRP master device has a priority of **100** and the backup device has a priority of **80**, then **weight** should be set to an amount greater than **20** so that if SureLink fails on the master, it will lower its priority to below **80**, and the backup device will assume the master role.

7. (Optional) For backup devices, enable the ability for the device to monitor the master device. This allows a backup VRRP device to monitor the master device, and increase its priority when the master device is failing SureLink tests. This can allow a device functioning as a backup device to promote itself to master.

```
(config)> network vrrp VRRP_test vrrp_plus monitor_master true
(config)>
```

8. Configure the VRRP interface:
   a. Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses:
      i. Set the DHCP server gateway type to custom:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway custom
(config)>
```

      ii. Determine the VRRP virtual IP addresses:

```
(config)> show network vrrp VRRP_test virtual_address
0 192.168.3.3
1 10.10.10.1

(config)>
```

      iii. Set the custom gateway to one of the VRRP virtual IP addresses. For example:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway_custom 192.168.3.3
(config)>
```

   b. For backup devices, set the default gateway to the IP address of the VRRP interface on the master device. For example:

```
(config)> network interface eth ipv4 gateway 192.168.3.1
(config)>
```

c. For backup devices, enable and configure SureLink on the VRRP interface.

i. Determine the VRRP interface. Generally, this should be a LAN interface; VRRP+ will then monitor the LAN using SureLink to determine if the interface has network connectivity and promote a backup to master if SureLink fails.

```
(config)> show network vrrp VRRP_test interface
/network/interface/eth
(config)>
```

ii. Enable SureLink on the interface:

```
(config)> network interface eth ipv4 surelink enable true
(config)>
```

iii. Set the amount of time to wait between connectivity tests:

```
(config)> network interface eth ipv4 surelink interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interval** to ten minutes, enter **5s**:

```
(config)> network interface eth ipv4 surelink interval 5s
(config)>
```

iv. Create a SureLink test target:

```
(config)> add network interface eth ipv4 surelink target end
(config network interface eth ipv4 surelink target 0)>
```

v. Configure the type of test for the test target:

```
(config network interface eth ipv4 surelink target 0)> test value
(config network interface eth ipv4 surelink target 0)>
```

where *value* is one of:

- **ping**: Tests connectivity by sending an ICMP echo request to a specified hostname or IP address.
  - Specify the hostname or IP address:

    ```
    (config network interface eth ipv4 surelink target 0)> ping_host host
    (config network interface eth ipv4 surelink target 0)>
    ```

  - (Optional) Set the size, in bytes, of the ping packet:

    ```
    (config network interface eth ipv4 surelink target 0)> ping_size [num]
    (config network interface eth ipv4 surelink target 0)>
    ```

- **dns**: Tests connectivity by sending a DNS query to the specified DNS server.
  - Specify the DNS server. Allowed value is the IP address of the DNS server.

```
(config network interface eth ipv4 surelinktarget 0)> dns_server ip_address
(config network interface eth ipv4 surelinktarget 0)>
```

- **dns_configured**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **http**: Tests connectivity by sending an HTTP or HTTPS GET request to the specified URL.
  - Specify the url:

```
(config network interface eth ipv4 surelink target 0)> http_url value
(config network interface eth ipv4 surelink target 0)>
```

    where *value* uses the format **http[s]://*hostname*/[*path*]**

- **interface_up**: The interface is considered to be down based on the interfaces down time, and the amount of time an initial connection to the interface takes before this test is considered to have failed.
  - (Optional) Set the amount of time that the interface can be down before this test is considered to have failed:

```
(config network interface eth ipv4 surelink target 0)> interface_down_time value
(config network interface eth ipv4 surelink target 0)>
```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

    For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

```
(config network interface eth ipv4 surelink target 0)> interface_down_time 600s
(config network interface eth ipv4 surelink target 0)>
```

    The default is 60 seconds.

  - (Optional) Set the amount of time to wait for an initial connection to the interface before this test is considered to have failed:

```
(config network interface eth ipv4 surelink target 0)> interface_timeout value
(config network interface eth ipv4 surelink target 0)>
```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

    For example, to set **interface_timeout**to ten minutes, enter either **10m** or **600s**:

```
(config network interface eth ipv4 surelink target 0)> interface_timeout 600s
(config network interface eth ipv4 surelink target 0)>
```

The default is 60 seconds.

9. Save the configuration and apply the change.

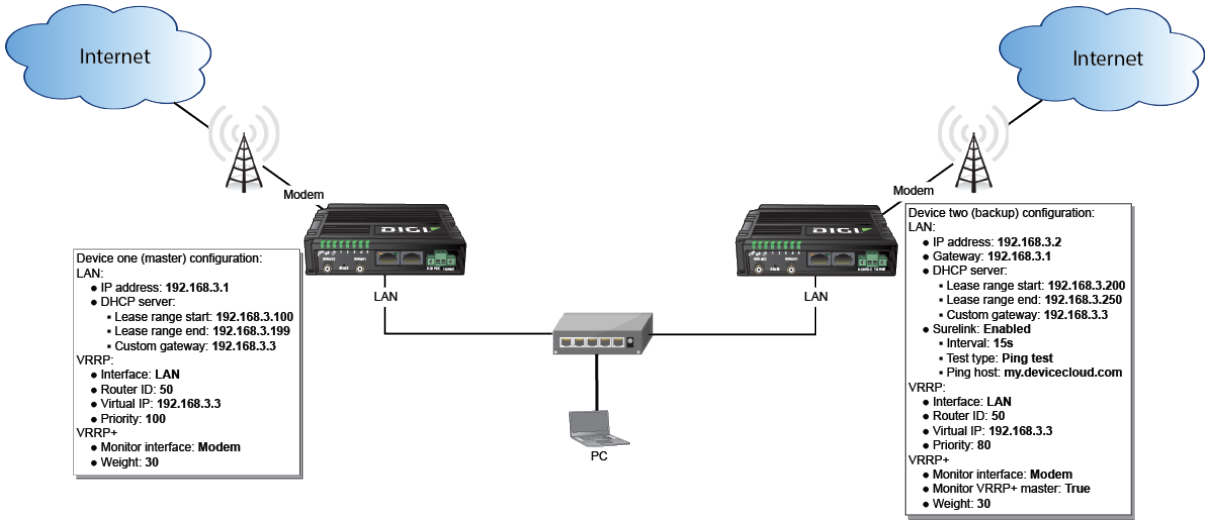
```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example: VRRP/VRRP+ configuration

This example configuration creates a VRRP pool containing two IX10 devices:



Configure device one (master device)

Web

Task 1: Configure VRRP on device one

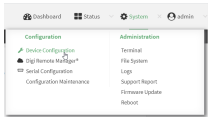
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

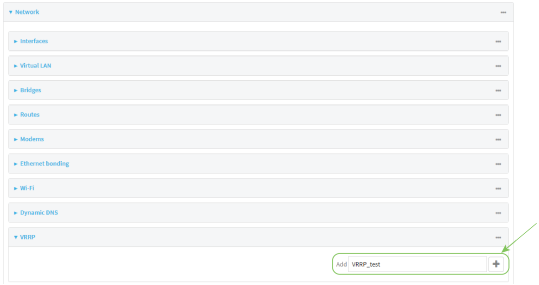
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

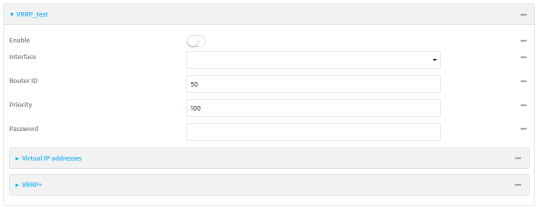


The **Configuration** window is displayed.

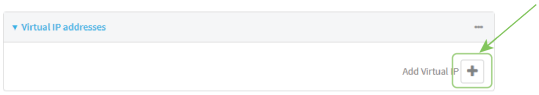
3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click ⊕.



The new VRRP instance configuration is displayed.



5. Click **Enable**.
6. For **Interface**, select **Interface: ETH**.
7. For **Router ID**, leave at the default setting of **50**.
8. For **Priority**, leave at the default setting of **100**.
9. Click to expand **Virtual IP addresses**.
10. Click ⊕ to add a virtual IP address.



11. For **Virtual IP**, type **192.168.3.3**.

Task 2: Configure VRRP+ on device one

1. Click to expand **VRRP+**.
2. Click **Enable**.
3. Click to expand **Monitor interfaces**.

4. Click to add an interface for monitoring.

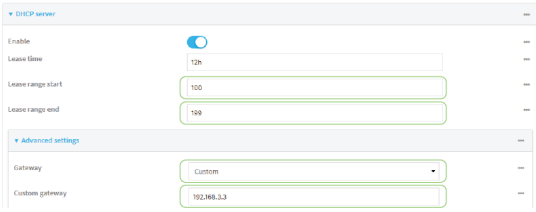
5. Select **Interface: Modem**.
6. For **Priority modifier**, type **30**.

Task 3: Configure the IP address for the VRRP interface, ETH, on device one

1. Click **Network** > **Interfaces** > **ETH** > **IPv4**
2. For **Address**, type **192.168.3.1/24**.

Task 4: Configure the DHCP server for ETH on device one

1. Click to expand **Network** > **Interfaces** > **ETH** > **IPv4** > **DHCP Server**
2. For **Lease range start**, leave at the default of **100**.
3. For **Lease range end**, type **199**.
4. Click to expand **Advanced settings**.
5. For **Gateway**, select **Custom**.
6. For **Custom gateway**, enter **192.168.3.3**.



7. Click **Apply** to save the configuration and apply the change.

Command line

Task 1: Configure VRRP on device one

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create the VRRP instance:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the VRRP interface to ETH:

```
(config network vrrp VRRP_test)> interface /network/interface/eth
(config network vrrp VRRP_test)>
```

6. Add the virtual IP address associated with this VRRP instance.

```
(config network vrrp VRRP_test)> add virtual_address end 192.168.3.3
(config network vrrp VRRP_test)>
```

Task 2: Configure VRRP+ on device one

1. Enable VRRP+:

```
(config network vrrp VRRP_test)> vrrp_plus enable true
(config network vrrp VRRP_test )>
```

2. Add the interface to monitor:

```
(config network vrrp VRRP_test)> add vrrp_plus monitor_interface end /network/interface/modem
(config network vrrp VRRP_test)>
```

3. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success to **30**:

```
(config network vrrp VRRP_test )> network vrrp VRRP_test vrrp_plus weight 30
(config network vrrp VRRP_test )>
```

Task 3: Configure the IP address for the VRRP interface, ETH, on device one

1. Type **...** to return to the root of the config prompt:

```
(config network vrrp VRRP_test )> ...
(config)>
```

2. Set the IP address for ETH:

```
(config)> network interface eth ipv4 address 192.168.3.1/24
(config)>
```

Task 4: Configure the DHCP server for ETH on device one

1. Set the start and end addresses of the DHCP pool to use to assign DHCP addresses to clients:
   a. Set the start address to **100**:

```
(config)> network interface eth ipv4 dhcp_server lease_start 100
(config)>
```

   b. Set the end address to **199**:

```
(config)> network interface eth ipv4 dhcp_server lease_end 199
(config)>
```

2. Set the DHCP server gateway type to custom:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway custom
(config)>
```

3. Set the custom gateway to **192.168.3.3**:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway_custom 192.168.3.3
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure device two (backup device)

Web

Task 1: Configure VRRP on device two

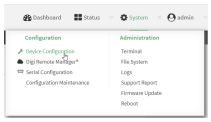
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

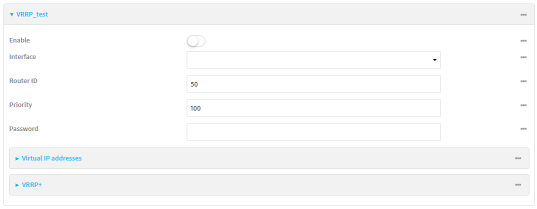
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



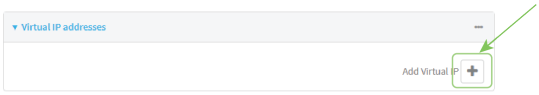
The **Configuration** window is displayed.

3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click .

The new VRRP instance configuration is displayed.



5. Click **Enable**.
6. For **Interface**, select **Interface: ETH**.
7. For **Router ID**, leave at the default setting of **50**.
8. For **Priority**, type **80**.
9. Click to expand **Virtual IP addresses**.
10. Click to add a virtual IP address.



11. For **Virtual IP**, type **192.168.3.3**.

Task 2: Configure VRRP+ on device two

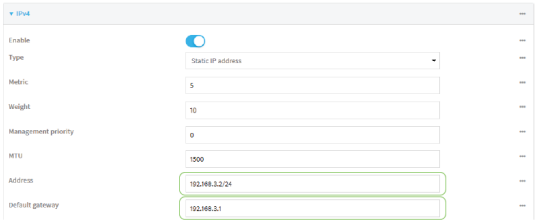
1. Click to expand **VRRP+**.
2. Click **Enable**.
3. Click to expand **Monitor interfaces**.

4. Click to add an interface for monitoring.

5. Select **Interface: Modem**.
6. Click to enable **Monitor VRRP+ master**.
7. For **Priority modifier**, type **30**.

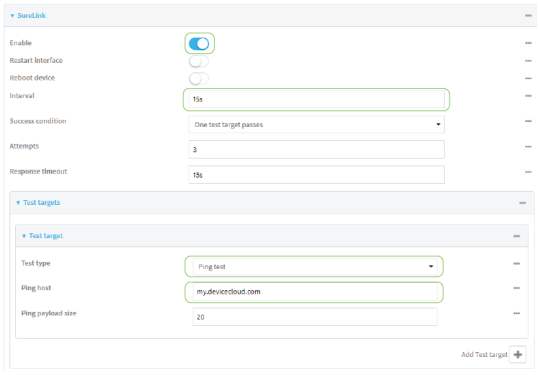
Task 3: Configure the IP address for the VRRP interface, ETH, on device two

1. Click **Network** > **Interfaces** > **ETH** > **IPv4**
2. For **Address**, type **192.168.3.2/24**.
3. For **Default gateway**, type the IP address of the VRRP interface on the master device, configured above in Task 3, step 2 (**192.168.3.1**).



Task 4: Configure SureLink for ETHon device two

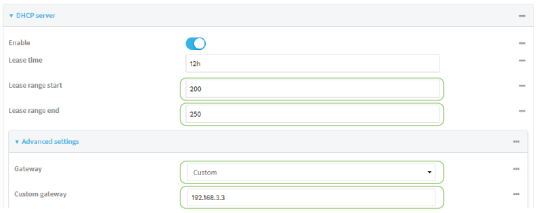
1. Click **Network** > **Interfaces** > **ETH** > **IPv4** > **SureLink**.
2. Click **Enable**.
3. For **Interval**, type **15s**.
4. Click to expand **Test targets** > **Test target**.
5. For **Test Type**, select **Ping test**.
6. For **Ping host**, type **https://remotemanager.digi.com**.



Task 5: Configure the DHCP server for ETH on device two

1. Click to expand **Network** > **Interfaces** > **ETH** > **IPv4** > **DHCP Server**
2. For **Lease range start**, type **200**.

3. For **Lease range end**, type **250**.
4. Click **Advanced settings**.
5. For **Gateway**, select **Custom**.
6. For **Custom gateway**, enter **192.168.3.3**.



7. Click **Apply** to save the configuration and apply the change.

Command line

Task 1: Configure VRRP on device two

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create the VRRP instance:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the VRRP interface to ETH:

```
(config network vrrp VRRP_test)> interface /network/interface/eth
(config network vrrp VRRP_test)>
```

6. Add the virtual IP address associated with this VRRP instance.

```
(config network vrrp VRRP_test)> add virtual_address end 192.168.3.3
(config network vrrp VRRP_test)>
```

Task 2: Configure VRRP+ on device two

1. Enable VRRP+:

```
(config network vrrp VRRP_test)> vrrp_plus enable true
(config network vrrp VRRP_test )>
```

2. Add the interface to monitor:

```
(config network vrrp VRRP_test)> add vrrp_plus monitor_interface end /network/interface/modem
(config network vrrp VRRP_test)>
```

3. Enable the ability to monitor the master device:

```
(config network vrrp VRRP_test)> vrrp_plus monitor_master true
(config network vrrp VRRP_test)>
```

4. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success to **30**:

```
(config network vrrp VRRP_test )> network vrrp VRRP_test vrrp_plus weight 30
(config network vrrp VRRP_test )>
```

Task 3: Configure the IP address for the VRRP interface, ETH, on device two

1. Type **...** to return to the root of the config prompt:

```
(config network vrrp VRRP_test )> ...
(config)>
```

2. Set the IP address for ETH:

```
(config)> network interface eth ipv4 address 192.168.3.2
(config)>
```

3. Set the default gateway to the IP address of the VRRP interface on the master device, configured above in Task 3, step 2 (**192.168.3.1**).

```
(config)> network interface eth ipv4 gateway 192.168.3.1
(config)>
```

Task 4: Configure SureLink for ETH on device two

1. Enable SureLink on the ETH interface:

```
(config)> network interface eth ipv4 surelink enable true
(config)>
```

2. Create a SureLink test target:

```
(config)> add network interface eth ipv4 surelink target end
(config network interface eth ipv4 surelink target 0)>
```

3. Set the type of test to ping:

```
(config network interface eth ipv4 surelink target 0)> test ping
(config network interface eth ipv4 surelink target 0)>
```

4. Set **https://remotemanager.digi.com** as the hostname to ping:

```
(config network interface eth ipv4 surelink target 0)> ping_host https://remotemanager.digi.com
(config network interface eth ipv4 surelink target 0)>
```

Task 5: Configure the DHCP server for ETH on device two

1. Type **...** to return to the root of the configuration prompt:

```
(config network interface eth ipv4 surelink target 0)> ...
(config)>
```

2. Set the start and end addresses of the DHCP pool to use to assign DHCP addresses to clients:
   a. Set the start address to **200**:

```
(config)> network interface eth ipv4 dhcp_server lease_start 200
(config)>
```

   b. Set the end address to **250**:

```
(config)> network interface eth ipv4 dhcp_server lease_end 250
(config)>
```

3. Set the DHCP server gateway type to custom:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway custom
(config)>
```

4. Set the custom gateway to **192.168.3.3**:

```
(config)> network interface eth ipv4 dhcp_server advanced gateway_custom 192.168.3.3
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show VRRP status and statistics

This section describes how to display VRRP status and statistics for a IX10 device. VRRP status is available from the Web UI only.

Web

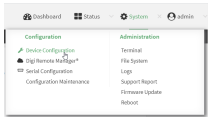
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

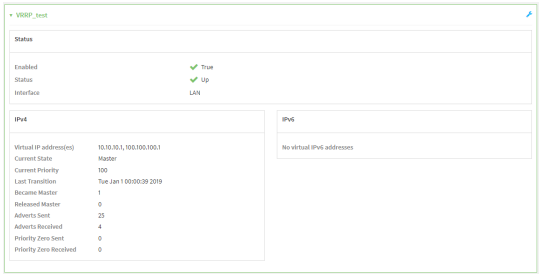
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Status** > **VRRP**.

   The **Virtual Router Redundancy Protocol** window is displayed.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type show vrrp:

```
> show vrrp

 VRRP     Status  Proto  State   Virtual IP
 ----     ------  -----  ------  -------------
```

```
VRRP_test Up    IPv4  Backup 10.10.10.1
VRRP_test Up    IPv4  Backup 100.100.100.1
>
```

3. To display additional information about a specific VRRP instance, at the Admin CLI prompt, type show vrrp name *name*:

```
> show vrrp name VRRP_test

VRRP_test VRRP Status
---------------------
Enabled              : True
Status               : Up
Interface            : lan

IPv4
 ----
 Virtual IP address(es) : 10.10.10.1, 100.100.100.1
 Current State        : Master
 Current Priority     : 100
 Last Transition      : Tue Jan  1 00:00:39 2019
 Became Master        : 1
 Released Master      : 0
 Adverts Sent         : 71
 Adverts Received     : 4
 Priority Zero Sent   : 0
 Priority zero Received : 0

>
```

Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) are used to securely connect two private networks together so that devices can connect from one network to the other using secure channels.

This chapter contains the following topics:

IPsec 339
OpenVPN 400
Generic Routing Encapsulation (GRE) 439
Dynamic Multipoint VPN (DMVPN) 459
L2TP 466
L2TPv3 Ethernet 478
MACsec 484
NEMO 486
WireGuard VPN 492

IPsec

IPsec is a suite of protocols for creating a secure communication link—an IPsec tunnel—between a host and a remote IP network or between two IP networks across a public network such as the Internet.

IPsec data protection

IPsec protects the data being sent across a public network by providing the following:

Data origin authentication
Authentication of data to validate the origin of data when it is received.

Data integrity
Authentication of data to ensure it has not been modified during transmission.

Data confidentiality
Encryption of data sent across the IPsec tunnel to ensure that an unauthorized device cannot read the data.

Anti-Replay
Authentication of data to ensure an unauthorized device has not injected it into the IPsec tunnel.

IPsec mode

The IX10 supports IPsec mode. You can set this mode to run using either the **Tunnel** or **Transport** options.

Tunnel
The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.

Transport
Only the payload of the IP packet is encrypted and/or authenticated. The IP header is left untouched. This mode has limitations when using an authentication header, because the IP addresses in the IP header cannot be translated (for example, with Network Address Translation (NAT), as it would invalidate the authentication hash value.

Internet Key Exchange (IKE) settings

IKE is a key management protocol that allows IPsec to negotiate the security associations (SAs) that are used to create the secure IPsec tunnel. Both IKEv1 and IKEv2 are supported.

SA negotiations are performed in two phases, known as **phase 1** and **phase 2**.

Phase 1

In phase 1, IKE creates a secure authenticated communication channel between the device and the peer (the remote device which is at the other end of the IPsec tunnel) using the configured pre-shared key and the Diffie-Hellman key exchange. This creates the IKE SAs that are used to encrypt further IKE communications.

For IKEv1, there are two modes for the phase 1 negotiation: **Main mode** and **Aggressive mode**. IKEv2 does not use these modes.

Main mode
Main mode is the default mode. It is slower than aggressive mode, but more secure, in that all sensitive information sent between the device and its peer is encrypted.

Aggressive mode

Aggressive mode is faster than main mode, but is not as secure as main mode, because the device and its peer exchange their IDs and hash information in clear text instead of being encrypted. Aggressive mode is usually used when one or both of the devices have a dynamic external IP address.

Phase 2

In phase 2, IKE negotiates the SAs for IPsec. This creates two unidirectional SAs, one for each direction. Once the phase 2 negotiation is complete, the IPsec tunnel should be fully functional.

IPsec and IKE renegotiation

To reduce the chances of an IPsec tunnel being compromised, the IPsec SAs and IKE SA are renegotiated at a regular interval. This results in different encryption keys being used in the IPsec tunnel.

Authentication

Client authenticaton

XAUTH (extended authentication) pre-shared key authentication mode provides additional security by using client authentication credentials in addition to the standard pre-shared key. The IX10 device can be configured to authenticate with the remote peer as an XAUTH client.

RSA Signatures

With RSA signatures authentication, the IX10 device uses a private RSA key to authenticate with a remote peer that is using a corresponding public key.

Certificate-based Authentication

X.509 certificate-based authentication makes use of private keys on both the server and client which are secured and never shared. Both the server and client have a certificate which is generated with their respective private key and signed by a Certificate Authority (CA).

The IX10 implementation of IPsec can be configured to use X.509 certificate-based authentication using the private keys and certificates, along with a root CA certificate from the signing authority and, if available, a Certificate Revocation List (CRL).

Configure an IPsec tunnel

Configuring an IPsec tunnel with a remote device involves configuring the following items:

Required configuration items

- **IPsec tunnel configuration items:**
  - A name for the tunnel.

    Note If the tunnel name is more than eight characters, the name will be truncated in the underlying network interface to the first six characters followed by three digits, incrementing from 000. This affects any custom scripts or firewall rules that may be trying to adjust the tunnel's interface or routing table entries.

  - The mode: either tunnel or transport.

- Enable the IPsec tunnel.

  The IPsec tunnel is enabled by default.
- The firewall zone of the IPsec tunnel.
- The routing metric for routes associated with this IPsec tunnel.
- The authentication type and pre-shared key or other applicable keys and certificates.

  If SCEP certificates will be selected as the Authentication type, create the SCEP client prior to configuring the IPsec tunnel. See Configure a Simple Certificate Enrollment Protocol client for instructions.
- The local endpoint type and ID values, and the remote endpoint host and ID values.

- **IKE configuration items**
  - The IKE version, either IKEv1 or IKEv2.
  - Whether to initiate a key exchange or wait for an incoming request.
  - The IKE mode, either main aggressive.
  - The IKE authentication protocol to use for the IPsec tunnel negotiation during phase 1 and phase 2.
  - The IKE encryption protocol to use for the IPsec tunnel negotiation during phase 1 and phase 2.
  - The IKE Diffie-Hellman group to use for the IPsec tunnel negotiation during phase 1 and phase 2.
- Enable dead peer detection and configure the delay and timeout.
- Destination networks that require source NAT.
- Active recovery configuration. See Configure SureLink active recovery for IPsec for information about IPsec active recovery.

Additional configuration items

The following additional configuration settings are not typically configured to get an IPsec tunnel working, but can be configured as needed:

- Determine whether the device should use UDP encapsulation even when it does not detect that NAT is being used.
- If using IPsec failover, identify the primary tunnel during configuration of the backup tunnel.
- The Network Address Translation (NAT) keep alive time.
- The protocol, either Encapsulating Security Payload (ESP) or Authentication Header (AH).
- The management priority for the IPsec tunnel interface. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
- Enable XAUTH client authentication, and the username and password to be used to authenticate with the remote peer.
- Enable Mode-configuration (MODECFG) to receive configuration information, such as the private IP address, from the remote peer.
- Disable the padding of IKE packets. This should normally not be done except for compatibility purposes.
- Destination networks that require source NAT.

- Depending on your network and firewall configuration, you may need to add a packet filtering rule to allow incoming IPsec traffic.
- **Tunnel and key renegotiating**
  - The lifetime of the IPsec tunnel before it is renegotiated.
  - The amount of time before the IKE phase 1 lifetime expires.
  - The amount of time before the IKE phase 2 lifetime expires
  - The lifetime margin, a randomizing amount of time before the IPsec tunnel is renegotiated.

Note If the remote networks for an IPsec tunnel overlap with the networks for a WAN internet connection (wired, cellular, or otherwise), you must configure a static route to direct the traffic either through the IPsec tunnel, or through the WAN (outside of the IPsec tunnel). See Configure a static route for information about configuring a static route.

Web

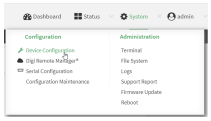
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

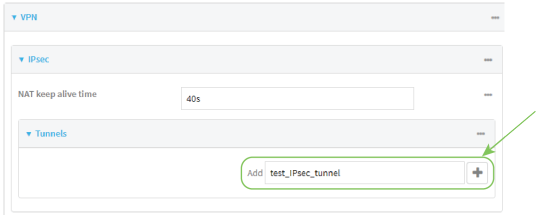
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

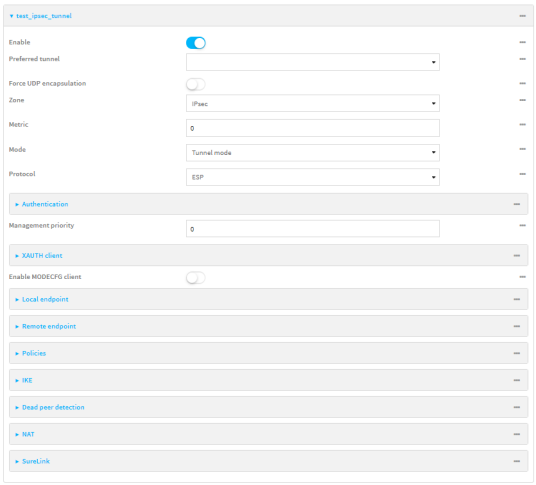
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec**.
4. Click to expand **Tunnels**.
5. For **Add IPsec tunnel**, type a name for the tunnel and click .



The new IPsec tunnel configuration is displayed.

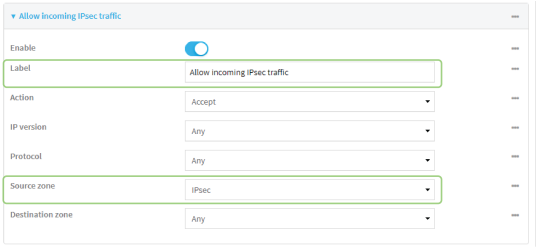


6. The IPsec tunnel is enabled by default. To disable, toggle off **Enable**.
7. (Optional) **Preferred tunnel** provides an optional mechanism for IPsec failover behavior. See Configure IPsec failover for more information.
8. (Optional) Enable **Force UDP encapsulation** to force the tunnel to use UDP encapsulation even when it does not detect that NAT is being used.
9. For **Zone**, select the firewall zone for the IPsec tunnel. Generally this should be left at the default of **IPsec**.

Note Depending on your network configuration, you may need to add a packet filtering rule to allow incoming traffic. For example, for the **IPsec** zone:

a. Click to expand **Firewall** > **Packet filtering**.
b. For **Add packet filter**, click ♈.
c. For **Label**, type **Allow incoming IPsec traffic**.
d. For **Source zone**, select **IPsec**.

Leave all other fields at their default settings.



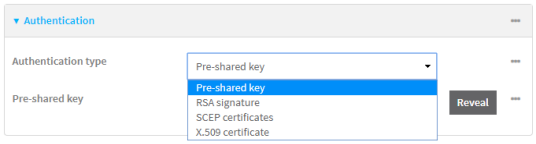
---

10. For **Metric**, enter or select the priority of routes associated with this IPsec tunnel. When more than one active route matches a destination, the route with the lowest metric is used.

    The metric can also be used in tandem with SureLink to configure IPsec failover behavior. See Configure IPsec failover for more information.
11. For **Mode**, select **Tunnel mode**. **Transport mode** is not currently supported.

12. Select the Mode, either:
    - **Tunnel mode**: The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.
    - **Transport mode**: Only the payload of the IP packet is encrypted and/or authenticated. The IP header is unencrypted.
13. Select the **Protocol**, either:
    - **ESP** (Encapsulating Security Payload): Provides encryption as well as authentication and integrity.
    - **AH** (Authentication Header): Provides authentication and integrity only.
14. **Strict routing** is disabled by default. Toggle on to enable.

    Strict routing makes IPsec behave like a policy-based VPN, rather than a route-based VPN.
15. Click to expand **Authentication**.



    a. For **Authentication type**, select one of the following:
       - **Pre-shared key**: Uses a pre-shared key (PSK) to authenticate with the remote peer.
         i. Type the **Pre-shared key**.
       - **Asymmetric pre-shared keys**: Uses asymmetric pre-shared keys to authenticate with the remote peer.
         i. For **Local key**, type the local pre-shared key. This must be the same as the remote key on the remote host.
         ii. For **Remote key**, type the remote pre-shared key. This must be the same as the local key on the remote host.
       - **RSA signature**: Uses a private RSA key to authenticate with the remote peer.
         i. For **Private key**, paste the device's private RSA key in PEM format.
         ii. Type the **Private key passphrase** that is used to decrypt the private key. Leave blank if the private key is not encrypted.
         iii. For **Peer public key**, paste the peer's public RSA key in PEM format.
       - **SCEP certificates**: Uses Simple Certificate Enrollment Protocol (SCEP) to download a private key, certificates, and an optional Certificate Revocation List (CRL) to the IX10 device from a SCEP server.

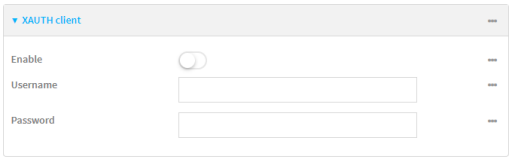
         You must create the SCEP client prior to configuring the IPsec tunnel. See Configure a Simple Certificate Enrollment Protocol client for instructions.
         i. For **SCEP Client**, select the SCEP client.
       - **X.509 certificate**: Uses private key and X.509 certificates to authenticate with the remote peer.
         i. For **Private key**, paste the device's private RSA key in PEM format.
         ii. Type the **Private key passphrase** that is used to decrypt the private key. Leave blank if the private key is not encrypted.

iii. For **Certificate**, paste the local X.509 certificate in PEM format.

iv. For Peer verification, select either:

- **Peer certificate**: For **Peer certificate**, paste the peer's X.509 certificate in PEM format.
- **Certificate Authority**: For **Certificate Authority chain**, paste the Certificate Authority (CA) certificates. These must include all peer certificates in the chain up to the root CA certificate, in PEM format.

16. (Optional) For **Management Priority**, set the management priority for this IPsec tunnel. A tunnel that is up and has the highest priority will be used for central management and direct device access.
17. (Optional) To configure the device to connect to its remote peer as an XAUTH client:
    a. Click to expand **XAUTH client**.



    b. Click **Enable**.
    c. Type the **Username** and **Password** that the device will use to authenticate as an XAUTH client with the peer.
18. (Optional) Click **Enable MODECFG client** to receive configuration information, such as the private IP address, from the remote peer.
19. Click to expand **Local endpoint**.
    a. For **Type**, select either:
        - **Default route**: Uses the same network interface as the default route.
        - **Interface**: Select the **Interface** to be used as the local endpoint.
    b. Click to expand **ID**.
        i. Select the ID type:
            - **Auto**: The ID will be automatically determined from the value of the tunnels endpoints.
            - **Raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack.

              For **Raw ID value**, type the ID that will be passed.
            - **Any**: Any ID will be accepted.
            - **IPv4**: The ID will be interpreted as an IP address and sent as an ID_IPV4_ADDR IKE identity.

              For **IPv4 ID value**, type an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.
            - **IPv6**: The ID will be interpreted as an IP address and sent as an ID_IPV6_ADDR IKE identity.

              For **IPv6 ID value**, type an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.

- **RFC822/Email**: The ID will be interpreted as an RFC822 (email address).

  For **RFC822 ID value**, type the ID in internet email address format.
- **FQDN**: The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID_FQDN IKE identity.

  For **FQDN ID value**, type the ID as an FQDN.
- **KeyID**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  For **KEYID ID value**, type the key ID.
- **MAC address**: The device's primary MAC address will be used as the ID and sent as a ID_KEY_ID IKE identity.
- **Serial number**: The device's serial number will be used as the ID and sent as a ID_KEY_ID IKE identity.

20. Click to expand **Remote endpoint**.
    a. For **IP version**, select either **IPv4** or **IPv6**.
    b. For **Hostname list selection**, select one of the following:
       - **Round robin**: Attempts to connect to hostnames sequentially based on the list order.
       - **Random**: Randomly selects an IPsec peer to connect to from the hostname list.
       - **Priority ordered**: Selects the first hostname in the list that is resolvable.
    c. Click to expand **Hostname**.
       i. Click next to **Add Hostname**.
       ii. For Hostname, type a hostname or IPv4 address. If your device is not configured to initiate the IPsec connection (see **IKE** > **Initiate connection**), you can also use the keyword **any**, which means that the hostname is dynamic or unknown.
       iii. Click again to add additional hostnames.
    d. Click to expand **ID**.
       i. Select the ID type:
          - **Auto**: The ID will be automatically determined from the value of the tunnels endpoints.
          - **Raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack.

            For **Raw ID value**, type the ID that will be passed.
          - **Any**: Any ID will be accepted.
          - **IPv4**: The ID will be interpreted as an IPv4 address and sent as an ID_IPV4_ADDR IKE identity.

            For **IPv4 ID value**, type an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.
          - **IPv6**: The ID will be interpreted as an IPv6 address and sent as an ID_IPV6_ADDR IKE identity.

            For **IPv6 ID value**, type an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.
          - **RFC822/Email**: The ID will be interpreted as an RFC822 (email address).

            For **RFC822 ID value**, type the ID in internet email address format.

- **FQDN**: The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID_FQDN IKE identity.

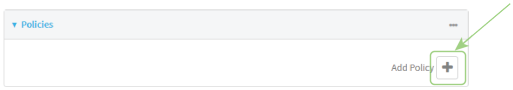
  For **FQDN ID value**, type the ID as an FQDN.
- **KeyID**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  For **KEYID ID value**, type the key ID.
- **MAC address**: The device's primary MAC address will be used as the ID and sent as a ID_KEY_ID IKE identity.
- **Serial number**: The device's serial number will be used as the ID and sent as a ID_KEY_ID IKE identity.

21. Click to expand **Policies**.

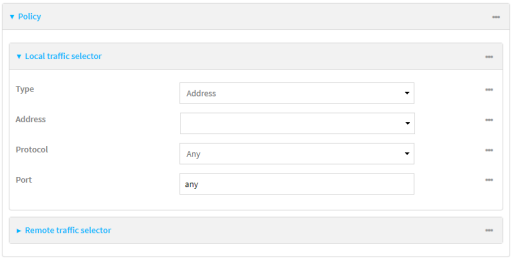
    Policies define the network traffic that will be encapsulated by this tunnel.

    a. Click to create a new policy.

    The new policy configuration is displayed.

    b. Click to expand **Local traffic selector**.

    c. For **Type**, select one of the following:
    - **Address**: The address of a local network interface.

      For **Address**, select the appropriate interface.
    - **Network**: The subnet of a local network interface.

      For **Address**, select the appropriate interface.
    - **Custom network**: A user-defined network.

      For **Custom network**, enter the IPv4 address and optional netmask.
    - **Request a network**: Requests a network from the remote peer.
    - **Dynamic**: Uses the address of the local endpoint.

    d. For **Protocol**, select one of the following:
    - **Any**: Matches any protocol.
    - **TCP**: Matches TCP protocol only.
    - **UDP**: Matches UDP protocol only.
    - **ICMP**: Matches ICMP requests only.

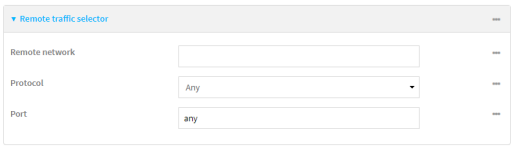
- **Other protocol**: Matches an unlisted protocol.

  If **Other protocol** is selected, type the number of the protocol.

e. For **Port**, type the port matching criteria.

   Allowed values are a port number, a range of port numbers, or **any**.

f. (Optional) Click to expand **Remote traffic selector**.



g. For **Remote network**, enter the IP address and optional netmask of the remote network.

h. For **Protocol**, select one of the following:

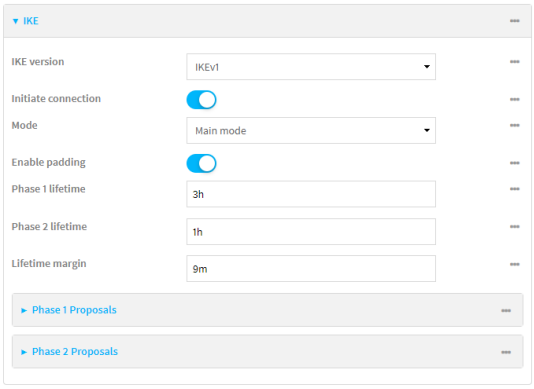
- **Any**: Matches any protocol.
- **TCP**: Matches TCP protocol only.
- **UDP**: Matches UDP protocol only.
- **ICMP**: Matches ICMP requests only.
- **Other protocol**: Matches an unlisted protocol.

  If **Other protocol** is selected, type the number of the protocol.

i. For **Port**, type the port matching criteria.

   Allowed values are a port number, a range of port numbers, or **any**.

22. Click to expand **IKE**.



a. For **IKE version**, select either IKEv1 or IKEv2. This setting must match the peer's IKE version.

b. **Initiate connection** instructs the device to initiate the key exchange, rather than waiting for an incoming request. This must be disabled if **Remote endpoint** > **Hostname** is set to **any**.

c. For **Mode**, select either **Main mode** or **Aggressive mode**.

d. For **IKE fragmentation**, select one of the following:

- **If supported by the peer**: Send oversized IKE messages in fragments, if the peer supports receiving them.

- **Always**: Always send IKEv1 messages in fragments. For IKEv2, this option is equivalent to **If supported by the peer**.
- **Never**: Do not send oversized IKE messages in fragments.
- **Accept**: Do not send oversized IKE messages in fragments, but announce support for fragmentation to the peer.

The default is **Always**.

e. For **Enable padding**, click to disable the padding of IKE packets. This should normally not be disabled except for compatibility purposes.

f. For Phase 1 lifetime, enter the amount of time that the IKE security association expires after a successful negotiation and must be re-authenticated.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Phase 1 lifetime** to ten minutes, enter **10m** or **600s**.

g. For Phase 2 lifetime, enter the amount of time that the IKE security association expires after a successful negotiation and must be rekeyed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Phase 2 lifetime** to ten minutes, enter **10m** or **600s**.

h. For Lifetime margin, enter a randomizing amount of time before the IPsec tunnel is renegotiated.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Lifetime margin** to ten minutes, enter **10m** or **600s**.

i. Click to expand **Phase 1 Proposals**.

i. Click to create a new phase 1 proposal.

ii. For **Cipher**, select the type of encryption.

iii. For **Hash**, select the type of hash to use to verify communication integrity.

iv. For **Diffie-Hellman group**, select the type of Diffie-Hellman group to use for key exchange.

v. You can add additional Phase 1 proposals by clicking next to **Add Phase 1 Proposal**.

j. Click to expand **Phase 2 Proposals**.

i. Click to create a new phase 2 proposal.

ii. For **Cipher**, select the type of encryption.

iii. For **Hash**, select the type of hash to use to verify communication integrity.

iv. For **Diffie-Hellman group**, select the type of Diffie-Hellman group to use for key exchange.

v. You can add additional Phase 2 proposals by clicking next to **Add Phase 2 Proposal**.

23. (Optional) Click to expand **Dead peer detection**. Dead peer detection is enabled by default. Dead peer detection uses periodic IKE transmissions to the remote endpoint to detect whether tunnel communications have failed, allowing the tunnel to be automatically

restarted when failure occurs.

a. To enable or disable dead peer detection, click **Enable**.

b. For **Delay**, type the number of seconds between transmissions of dead peer packets. Dead peer packets are only sent when the tunnel is idle.

c. For **Timeout**, type the number of seconds to wait for a response from a dead peer packet before assuming the tunnel has failed.

24. (Optional) Click to expand **NAT** to create a list of destination networks that require source NAT.

a. Click next to **Add NAT destination**.

b. For **Destination network**, type the IPv4 address and optional netmask of a destination network that requires source NAT. You can also use **any**, meaning that any destination network connected to the tunnel will use source NAT.

25. See Configure SureLink active recovery for IPsec for information about IPsec **Active recovery**.

26. (Optional) Click **Advanced** to set various IPsec-related time out, keep alive, and related values.

27. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add an IPsec tunnel. For example, to add an IPsec tunnel named **ipsec_example**:

```
(config)> add vpn ipsec tunnel ipsec_example
(config vpn ipsec tunnel ipsec_example)>
```

   The IPsec tunnel is enabled by default. To disable:

```
(config vpn ipsec tunnel ipsec_example)> enable false
(config vpn ipsec tunnel ipsec_example)>
```

4. (Optional) Set the tunnel to use UDP encapsulation even when it does not detect that NAT is being used:

```
(config vpn ipsec tunnel ipsec_example)> force_udp_encap true
(config vpn ipsec tunnel ipsec_example)>
```

5. Set the firewall zone for the IPsec tunnel. Generally this should be left at the default of **ipsec**.

```
(config vpn ipsec tunnel ipsec_example)> zone zone
(config vpn ipsec tunnel ipsec_example)>
```

   To view a list of available zones:

```
(config vpn ipsec tunnel ipsec_example)> zone ?

Zone: The firewall zone assigned to this IPsec tunnel. This can be used by packet filtering rules
and access control lists to restrict network traffic on this tunnel.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Default value: ipsec
Current value: ipsec

(config vpn ipsec tunnel ipsec_example)>
```

Note Depending on your network configuration, you may need to add a packet filtering rule to allow incoming traffic. For example, for the **IPsec** zone:

a. Type **...** to move to the root of the configuration:

```
(config vpn ipsec tunnel ipsec_example)> ...
(config)>
```

b. Add a packet filter:

```
(config)> add firewall filter end
(config firewall filter 2)>
```

c. Set the label to **Allow incoming IPsec traffic**:

```
(config config firewall filter 2)> label "Allow incoming IPsec traffic"
(config firewall filter 2)>
```

d. Set the source zone to **ipsec**:

```
(config config firewall filter 2)> src_zone ipsec
(config firewall filter 2)>
```

6. Set the metric for the IPsec tunnel. When more than one active route matches a destination, the route with the lowest metric is used. The metric can also be used in tandem with SureLink to configure IPsec failover behavior. See Configure IPsec failover for more information.

```
(config vpn ipsec tunnel ipsec_example)> metric value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any integer between **0** and **65535**.

7. Set the mode:

```
(config vpn ipsec tunnel ipsec_example)> mode mode
(config vpn ipsec tunnel ipsec_example)>
```

where *mode* is either:

- **tunnel**: The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.
- **transport**: Only the payload of the IP packet is encrypted and/or authenticated. The IP header is unencrypted.

The default is **tunnel**.

8. Set the protocol:

```
(config vpn ipsec tunnel ipsec_example)> type protocol
(config vpn ipsec tunnel ipsec_example)>
```

where *protocol* is either:

- **esp** (Encapsulating Security Payload): Provides encryption as well as authentication and integrity.
- **ah** (Authentication Header): Provides authentication and integrity only.

The default is **esp**.

9. (Optional) Set the management priority for this IPsec tunnel:

```
(config vpn ipsec tunnel ipsec_example)> mgmt value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any interger between **0** and **1000**.

10. Set the authentication type:

```
(config vpn ipsec tunnel ipsec_example)> auth type value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is one of:

- **secret**: Uses a pre-shared key (PSK) to authenticate with the remote peer.
  a. Set the pre-shared key:

```
(config vpn ipsec tunnel ipsec_example)> auth secret key
(config vpn ipsec tunnel ipsec_example)>
```

- **asymmetric-secrets**: Uses asymmetric pre-shared keys to authenticate with the remote peer.
  a. Set the local pre-shared key. This must be the same as the remote key on the remote host.:

```
(config vpn ipsec tunnel ipsec_example)> auth local_secret key
(config vpn ipsec tunnel ipsec_example)>
```

  b. Set the remote pre-shared key. This must be the same as the local key on the remote host.:

```
(config vpn ipsec tunnel ipsec_example)> auth remote_secret key
(config vpn ipsec tunnel ipsec_example)>
```

- **rsasig**: Uses a private RSA key to authenticate with the remote peer.
  a. For the **private_key** parameter, paste the device's private RSA key in PEM format:

```
(config vpn ipsec tunnel ipsec_example)> auth private_key key
(config vpn ipsec tunnel ipsec_example)>
```

  b. Set the private key passphrase that is used to decrypt the private key. Leave blank if the private key is not encrypted.

```
(config vpn ipsec tunnel ipsec_example)> auth private_key_passphrase passphrase
(config vpn ipsec tunnel ipsec_example)>
```

  c. For the **peer_public_key** parameter, paste the peer's public RSA key in PEM format:

```
(config vpn ipsec tunnel ipsec_example)> auth peer_public_key key
(config vpn ipsec tunnel ipsec_example)>
```

- **x509**: Uses private key and X.509 certificates to authenticate with the remote peer.
  a. For the **private_key** parameter, paste the device's private RSA key in PEM format:

```
(config vpn ipsec tunnel ipsec_example)> auth private_key key
(config vpn ipsec tunnel ipsec_example)>
```

  b. Set the private key passphrase that is used to decrypt the private key. Leave blank if the private key is not encrypted.

```
(config vpn ipsec tunnel ipsec_example)> auth private_key_passphrase passphrase
(config vpn ipsec tunnel ipsec_example)>
```

  c. For the **cert** parameter, paste the local X.509 certificate in PEM format:

```
(config vpn ipsec tunnel ipsec_example)> auth cert certificate
(config vpn ipsec tunnel ipsec_example)>
```

  d. Set the method for verifying the peer's X.509 certificate:

```
(config vpn ipsec tunnel ipsec_example)> auth peer_verify value
(config vpn ipsec tunnel ipsec_example)>
```

  where *value* is either:

  - **cert**: Uses the peer's X.509 certificate in PEM format for verification.
    - For the **peer_cert** parameter, paste the peer's X.509 certificate in PEM format:

```
(config vpn ipsec tunnel ipsec_example)> auth peer_cert certificate
(config vpn ipsec tunnel ipsec_example)>
```

- **ca**: Uses the Certificate Authority chain for verification.
  - For the **ca_cert** parameter, paste the Certificate Authority (CA) certificates. These must include all peer certificates in the chain up to the root CA certificate, in PEM format.

```
(config vpn ipsec tunnel ipsec_example)> auth ca_cert cert_chain
(config vpn ipsec tunnel ipsec_example)>
```

11. (Optional) Configure the device to connect to its remote peer as an XAUTH client:
    a. Enable XAUTH client functionality:

```
(config vpn ipsec tunnel ipsec_example)> xauth_client enable true
(config vpn ipsec tunnel ipsec_example)>
```

    b. Set the XAUTH client username:

```
(config vpn ipsec tunnel ipsec_example)> xauth_client username name
(config vpn ipsec tunnel ipsec_example)>
```

    c. Set the XAUTH client password:

```
(config vpn ipsec tunnel ipsec_example)> xauth_client password pwd
(config vpn ipsec tunnel ipsec_example)>
```

12. (Optional) Enable MODECFG client functionality:

    MODECFG client functionality configures the device to receive configuration information, such as the private IP address, from the remote peer.
    a. Enable MODECFG client functionality:

```
(config vpn ipsec tunnel ipsec_example)> modecfg_client enable true
(config vpn ipsec tunnel ipsec_example)>
```

13. Configure the local endpoint:
    a. Set the method for determining the local network interface:

```
(config vpn ipsec tunnel ipsec_example)> local type value
(config vpn ipsec tunnel ipsec_example)>
```

    where *value* is either:
    - **defaultroute**: Uses the same network interface as the default route.
    - **interface**: Select the **Interface** to be used as the local endpoint.

    b. Set the ID type:

```
(config vpn ipsec tunnel ipsec_example)> local id type value
(config vpn ipsec tunnel ipsec_example)>
```

    where *value* is one of:
    - **auto**: The ID will be automatically determined from the value of the tunnels endpoints.

- **raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack.

  Set the unmodified ID that will be passed:

  ```
  (config vpn ipsec tunnel ipsec_example)> local id type raw_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **any**: Any ID will be accepted.
- **ipv4**: The ID will be interpreted as an IPv4 address and sent as an ID_IPV4_ADDR IKE identity.

  Set an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.

  ```
  (config vpn ipsec tunnel ipsec_example)> local id type ipv4_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **ipv6**: The ID will be interpreted as an IPv6 address and sent as an ID_IPV6_ADDR IKE identity.

  Set an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.

  ```
  (config vpn ipsec tunnel ipsec_example)> local id type ipv6_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **rfc822**: The ID will be interpreted as an RFC822 (email address).

  Set the ID in internet email address format:

  ```
  (config vpn ipsec tunnel ipsec_example)> local id type rfc822_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **fqdn**: The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID_FQDN IKE identity.
- **keyid**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  Set the key ID:

  ```
  (config vpn ipsec tunnel ipsec_example)> local id type keyid_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **mac_address**: The device's MAC address will be used for the Key ID and sent as an ID_KEY_ID IKE identity.
- **serial_number**: The ID device's serial number will be used for the Key ID and sent as an ID_KEY_ID IKE identity.

14. Configure the remote endpoint:
    a. Add a remote hostname:

    ```
    (config vpn ipsec tunnel ipsec_example)> add remote hostname end value
    (config vpn ipsec tunnel ipsec_example)>
    ```

    where *value* is the hostname or IPv4 address of the IPsec peer. If your device is not configured to initiate the IPsec connection (see ike initiate), you can also use the keyword **any**, which means that the hostname is dynamic or unknown.

Repeat for additional hostnames.

b. Set the hostname selection type:

```
(config vpn ipsec tunnel ipsec_example)> remote hostname_selection value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is one of:

- **round_robin**: Attempts to connect to hostnames sequentially based on the list order.
- **random**: Randomly selects an IPsec peer to connect to from the hostname list.
- **priority**: Selects the first hostname in the list that is resolvable.

c. Set the ID type:

```
(config vpn ipsec tunnel ipsec_example)> remote id type value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is one of:

- **auto**: The ID will be automatically determined from the value of the tunnels endpoints.
- **raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack.

  Set the unmodified ID that will be passed:

  ```
  (config vpn ipsec tunnel ipsec_example)> remote id type raw_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **any**: Any ID will be accepted.
- **ipv4**: The ID will be interpreted as an IPv4 address and sent as an ID_IPV4_ADDR IKE identity.

  Set an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.

  ```
  (config vpn ipsec tunnel ipsec_example)> remote id type ipv4_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **ipv6**: The ID will be interpreted as an IPv6 address and sent as an ID_IPV6_ADDR IKE identity.

  Set an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.

  ```
  (config vpn ipsec tunnel ipsec_example)> remote id type ipv6_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **rfc822**: The ID will be interpreted as an RFC822 (email address).

  Set the ID in internet email address format:

  ```
  (config vpn ipsec tunnel ipsec_example)> remote id type rfc822_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **fqdn**: The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID_FQDN IKE identity.
- **keyid**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  Set the key ID:

  ```
  (config vpn ipsec tunnel ipsec_example)> remote id type keyid_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **mac_address**: The device's MAC address will be used for the Key ID and sent as an ID_KEY_ID IKE identity.
- **serial_number**: The ID device's serial number will be used for the Key ID and sent as an ID_KEY_ID IKE identity.

15. Configure IKE settings:
    a. Set the IKE version:

    ```
    (config vpn ipsec tunnel ipsec_example)> ike version value
    (config vpn ipsec tunnel ipsec_example)>
    ```

    where *value* is either **ikev1** or **ikev2**. This setting must match the peer's IKE version.

    b. Determine whether the device should initiate the key exchange, rather than waiting for an incoming request. By default, the device will initiate the key exchange. This must be disabled if remote hostname is set to **any**. To disable:

    ```
    (config vpn ipsec tunnel ipsec_example)> ike initiate false
    (config vpn ipsec tunnel ipsec_example)>
    ```

    c. Set the IKE phase 1 mode:

    ```
    (config vpn ipsec tunnel ipsec_example)> ike mode value
    (config vpn ipsec tunnel ipsec_example)>
    ```

    where *value* is either **aggressive** or **main**.

    d. Set the IKE fragmentation:

    ```
    (config vpn ipsec tunnel ipsec_example)> ike fragmentation value
    (config vpn ipsec tunnel ipsec_example)>
    ```

    where *value* is one of:

    - **if_supported**: Send oversized IKE messages in fragments, if the peer supports receiving them.
    - **always**: Always send IKEv1 messages in fragments. For IKEv2, this option is equivalent to **if supported**.
    - **never**: Do not send oversized IKE messages in fragments.
    - **accept**: Do not send oversized IKE messages in fragments, but announce support for fragmentation to the peer.

    The default is **always**.

    e. Padding of IKE packets is enabled by default and should normally not be disabled except for compatibility purposes. To disable:

```
(config vpn ipsec tunnel ipsec_example)> ike pad false
(config vpn ipsec tunnel ipsec_example)>
```

f. Set the amount of time that the IKE security association expires after a successful negotiation and must be re-authenticated:

```
(config vpn ipsec tunnel ipsec_example)> ike phase1_lifetime value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **phase1_lifetime** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> ike phase1_lifetime 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is three hours.

g. Set the amount of time that the IKE security association expires after a successful negotiation and must be rekeyed.

```
(config vpn ipsec tunnel ipsec_example)> ike phase2_lifetime value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **phase2_lifetime** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> ike phase2_lifetime 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is one hour.

h. Set a randomizing amount of time before the IPsec tunnel is renegotiated:

```
(config vpn ipsec tunnel ipsec_example)> ike lifetime_margin value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **lifetime_margin** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> ike lifetime_margin 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is nine minutes.

i. Configure the types of encryption, hash, and Diffie-Hellman group to use during phase 1:

   i. Add a phase 1 proposal:

```
(config vpn ipsec tunnel ipsec_example)> add ike phase1_proposal end
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

ii. Set the type of encryption to use during phase 1:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> cipher value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

where *value* is one of:

- **3des**
- **aes128**
- **aes128gcm128**
- **aes128gcm64**
- **aes128gcm96**
- **aes192**
- **aes192gcm128**
- **aes192gcm64**
- **aes192gcm96**
- **aes256**
- **aes256gcm128**
- **aes256gcm64**
- **aes256gcm96**
- **null**

The default is **3des**.

iii. Set the type of hash to use during phase 1 to verify communication integrity:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> hash value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

where *value* is one of:

- **md5**
- **sha1**
- **sha256**
- **sha384**
- **sha512**

The default is **sha1**.

iv. Set the type of Diffie-Hellman group to use for key exchange during phase 1:

i. Use the **?** to determine available Diffie-Hellman group types:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> dh_group ?
curve25519
curve448
ecp192
ecp224
...
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

ii. Set the Diffie-Hellman group type:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> dh_group value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

The default is **modp2048**.

v. (Optional) Add additional phase 1 proposals:

i. Move back one level in the schema:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> ..
(config vpn ipsec tunnel ipsec_example ike phase1_proposal)>
```

ii. Add an additional proposal:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal)> add end
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 1)>
```

Repeat the above steps to set the type of encryption, hash, and Diffie-Hellman group for the additional proposal.

iii. Repeat to add more phase 1 proposals.

j. Configure the types of encryption, hash, and Diffie-Hellman group to use during phase 2:

i. Move back two levels in the schema:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> .. ..
(config vpn ipsec tunnel ipsec_example ike)>
```

ii. Add a phase 2 proposal:

```
(config vpn ipsec tunnel ipsec_example ike)> add ike phase2_proposal end
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

iii. Set the type of encryption to use during phase 2:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> cipher value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

where *value* is one of:

- **3des**
- **aes128**
- **aes128gcm128**
- **aes128gcm64**
- **aes128gcm96**
- **aes192**
- **aes192gcm128**
- **aes192gcm64**
- **aes192gcm96**
- **aes256**
- **aes256gcm128**

- **aes256gcm64**
- **aes256gcm96**
- **null**

The default is **3des**.

iv. Set the type of hash to use during phase 2 to verify communication integrity:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> hash value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

where *value* is one of:

- **md5**
- **sha1**
- **sha256**
- **sha384**
- **sha512**

The default is **sha1**.

v. Set the type of Diffie-Hellman group to use for key exchange during phase 2:

i. Use the **?** to determine available Diffie-Hellman group types:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> dh_group ?
curve25519
curve448
ecp192
ecp224
...
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

ii. Set the Diffie-Hellman group type:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> dh_group value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

The default is **modp2048**.

vi. (Optional) Add additional phase 2 proposals:

i. Move back one level in the schema:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> ..
(config vpn ipsec tunnel ipsec_example ike phase2_proposal)>
```

ii. Add an additional proposal:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal)> add end
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 1)>
```

Repeat the above steps to set the type of encryption, hash, and Diffie-Hellman group for the additional proposal.

iii. Repeat to add more phase 2 proposals.

16. (Optional) Configure dead peer detection:

Dead peer detection is enabled by default. Dead peer detection uses periodic IKE transmissions to the remote endpoint to detect whether tunnel communications have failed, allowing the tunnel to be automatically restarted when failure occurs.

a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> ...
(config)>
```

b. To disable dead peer detection:

```
(config)> vpn ipsec tunnel ipsec_example dpd enable false
(config)>
```

c. Set the number of seconds between transmissions of dead peer packets. Dead peer packets are only sent when the tunnel is idle. The default is **60**.

```
(config)> vpn ipsec tunnel ipsec_example dpd delay value
(config)>
```

d. Set the number of seconds to wait for a response from a dead peer packet before assuming the tunnel has failed. The default is **90**.

```
(config)> vpn ipsec tunnel ipsec_example dpd timeout value
(config)>
```

17. (Optional) Create a list of destination networks that require source NAT:

a. Add a destination network:

```
(config)> add vpn ipsec tunnel ipsec_example nat end
(config vpn ipsec tunnel ipsec_example nat 0)>
```

b. Set the IPv4 address and optional netmask of a destination network that requires source NAT. You can also use **any**, meaning that any destination network connected to the tunnel will use source NAT.

```
(config vpn ipsec tunnel ipsec_example nat 0)> dst value
(config vpn ipsec tunnel ipsec_example nat 0)>
```

18. Configure policies that define the network traffic that will be encapsulated by this tunnel:

a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example nat 0)> ...
(config)>
```

b. Add a policy:

```
(config)> add vpn ipsec tunnel ipsec_example policy end
(config vpn ipsec tunnel ipsec_example policy 0)>
```

c. Set the type of local traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local type value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is one of:

- **address**: The address of a local network interface.

  Set the address:

  i. Use the **?** to determine available interfaces:

  ii. Set the interface. For example:

  ```
  (config vpn ipsec tunnel ipsec_example policy 0)> local address eth1
  (config vpn ipsec tunnel ipsec_example policy 0)>
  ```

- **network**: The subnet of a local network interface.

  Set the network:

  i. Use the **?** to determine available interfaces:

  ii. Set the interface. For example:

  ```
  (config vpn ipsec tunnel ipsec_example policy 0)> local network eth1
  (config vpn ipsec tunnel ipsec_example policy 0)>
  ```

- **custom**: A user-defined network.

  Set the custom network:

  ```
  (config vpn ipsec tunnel ipsec_example policy 0)> local custom value
  (config vpn ipsec tunnel ipsec_example policy 0)>
  ```

  where *value* is the IPv4 address and optional netmask. The keyword **any** can also be used.

- **request**: Requests a network from the remote peer.
- **dynamic**: Uses the address of the local endpoint.

d. Set the port matching criteria for the local traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local port value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is the port number, a range of port numbers, or the keyword **any**.

e. Set the protocol matching criteria for the local traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local protocol value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is one of:

- **any**: Matches any protocol.
- **tcp**: Matches TCP protocol only.
- **udp**: Matches UDP protocol only.
- **icmp**: Matches ICMP requests only.

- **other**: Matches an unlisted protocol.

  If **other** is used, set the number of the protocol:

  ```
  (config vpn ipsec tunnel ipsec_example policy 0)> local protocol_other int
  (config vpn ipsec tunnel ipsec_example policy 0)>
  ```

  Allowed values are an integer between **1** and **255**.

f. Set the IP address and optional netmask of the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote network value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

g. Set the port matching criteria for the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote port value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is the port number, a range of port numbers, or the keyword **any**.

h. Set the protocol matching criteria for the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote protocol value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is one of:

- **any**: Matches any protocol.
- **tcp**: Matches TCP protocol only.
- **udp**: Matches UDP protocol only.
- **icmp**: Matches ICMP requests only.
- **other**: Matches an unlisted protocol.

  If **other** is used, set the number of the protocol:

  ```
  (config vpn ipsec tunnel ipsec_example policy 0)> remote protocol_other int
  (config vpn ipsec tunnel ipsec_example policy 0)>
  ```

  Allowed values are an integer between **1** and **255**.

19. (Optional) You can also configure various IPsec related time out, keep alive, and related values:

a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example policy 0)> ...
(config)>
```

b. Use the **?** to determine available options:

```
(config)> vpn ipsec advanced ?

Advanced: Advanced configuration that applies to all IPsec tunnels.

 Parameters             Current Value
 ------------------------------------------------------------------------------
```

```
debug                 none        Debug level
ike_fragment_size     1280        Maximum IKE fragment size
ike_retransmit_tries  5           IKE retransmit tries
keep_alive            40s         NAT keep alive time

Additional Configuration
------------------------------------------------------------------------------
connection_retry_timeout  Connection retry timeout
connection_try_interval   Connection try interval
ike_timeout               IKE timeout

(config)>
```

Generally, the default settings for these should be sufficient.

c. You can also enable debugging for IPsec:

```
(config)> vpn ipsec advanced debug value
(config)>
```

where *value* is one of:

- **none**
- **basic_auditing**
- **detailed_control**
- **generic_control**
- **raw_data**
- **sensitive_data**

20. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

21. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure IPsec failover

You can configure the IX10 device to fail over from a primary IPsec tunnel to a backup tunnel:

- **SureLink** active recovery—You can use SureLink along with the IPsec tunnel's metric to configure two or more tunnels so that when the primary tunnel is determined to be inactive by SureLink, a secondary tunnel can begin serving traffic that the primary tunnel was serving.
- **Preferred tunnel**—When multiple IPsec tunnels are configured, one tunnel can be configured as a backup to another tunnel by defining a preferred tunnel for the backup device.

Required configuration items

- Two or more configured IPsec tunnels: The primary tunnel, and one or more backup tunnels.
- Either:
  - SureLink configured on the primary tunnel with **Restart Interface** enabled, and the metric for all tunnels set appropriately to determine which IPsec tunnel has priority. With this failover configuration, both tunnels are active simultaneously, and there is minimal downtime due to failover.
  - Identify the preferred tunnel during configuration of the backup tunnel. In this scenario, the backup tunnel is not active until the preferred tunnel fails.

IPsec failover using SureLink

With this configuration, when two IPsec tunnels are configured with the same local and remote endpoints but different metrics, traffic addressed to the remote endpoint will be routed through the IPsec tunnel with the lower metric.

If **SureLink** > **Restart Interface** is enabled for the tunnel with the lower metric, and SureLink determines that the tunnel is not functioning properly (for example, pings to a host at the other end of the tunnel are failing), then:

1. SureLink will shut down the tunnel and renegotiate its IPsec connection.
2. While the tunnel with the lower metric is down, traffic addressed to the remote endpoint will be routed through the tunnel with the higher metric.

For example:

- Tunnel_1:
  - **Metric**: 10
  - **Local endpoint** > **Interface**: ETH
  - **Remote endpoint** > **Hostname**: 192.168.10.1
  - **SureLink** configuration:
    - **Restart Interface** enabled
    - **Test target**:
      - **Test type**: Ping test
      - **Ping host**: 192.168.10.2
- Tunnel_2:

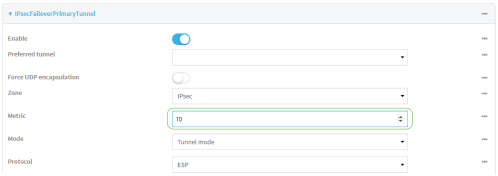
- **Metric**: 20
- **Local endpoint** > **Interface**: ETH
- **Remote endpoint** > **Hostname**: 192.168.10.1

In this configuration:

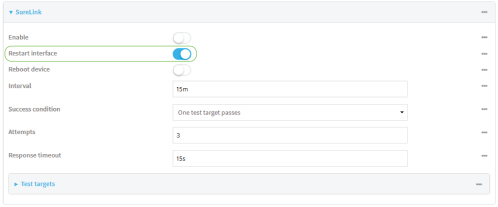
1. Tunnel_1 will normally be used for traffic destined for the 192.168.10.1 endpoint.
2. If pings to 192.168.10.2 fail, SureLink will shut down the tunnel and renegotiate its IPsec connection.
3. While Tunnel_1 is down, Tunnel_2 will be used for traffic destined for the 192.168.10.1 endpoint.

Web

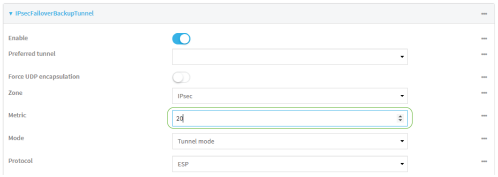
1. Configure the primary IPsec tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a low value (for example, **10**).



   - Configure SureLink for the primary IPsec tunnel and enable **Restart interface**. See Configure SureLink active recovery for IPsec for instructions.



2. Create a backup IPsec tunnel. Configure this tunnel to use the same local and remote endpoints as the primary tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a value that is higher than the metric of the primary tunnel (for example, **20**).



Command line

1. Configure the primary IPsec tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a low value (for example, **10**):

```
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)> metric 10
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)>
```

- Configure SureLink for the primary IPsec tunnel and enable **Restart interface**. See Configure SureLink active recovery for IPsec for instructions.

```
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)> surelink restart true
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)>
```

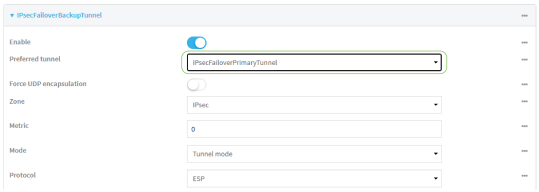
2. Create a backup IPsec tunnel. Configure this tunnel to use the same local and remote endpoints as the primary tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a value that is higher than the metric of the primary tunnel (for example, **20**):

```
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)> metric 20
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)>
```

IPsec failover using Preferred tunnel

Web

1. Configure the primary IPsec tunnel. See Configure an IPsec tunnel for instructions.
2. Create a backup IPsec tunnel. See Configure an IPsec tunnel for instructions.
3. During configuration of the backup IPsec tunnel, identify the primary IPsec tunnel in the **Preferred tunnel** parameter:



Command line

1. Configure the primary IPsec tunnel. See Configure an IPsec tunnel for instructions.
2. Create a backup IPsec tunnel. See Configure an IPsec tunnel for instructions.
3. During configuration of the backup IPsec tunnel, identify the primary IPsec tunnel:
   a. Use the **?** to view a list of available tunnels:

```
(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover ?

Preferred tunnel: This tunnel will not start until the preferred tunnel has failed. It will continue
to operate until the preferred tunnel returns to full operation status.
Format:
 primary_ipsec_tunnel
 backup_ipsec_tunnel
Optional: yes
Current value:
```

```
(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover
```

b. Set the primary IPsec tunnel:

```
(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover primary_ipsec_tunnel
(config vpn ipsec tunnel backup_ipsec_tunnel)>
```

Configure SureLink active recovery for IPsec

You can configure the IX10 device to regularly probe IPsec tunnels to determine if the connection has failed and take remedial action.

You can also configure the IPsec tunnel to fail over to a backup tunnel. See Configure IPsec failover for further information.

Required configuration items

- A valid IPsec configuration. See Configure an IPsec tunnel for configuration instructions.
- Enable IPsec SureLink.
- The behavior of the IX10 device upon IPsec failure: either
  - Restart the IPsec interface
  - Reboot the device.

Additional configuration items

- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.
- The number of probe failures before the IPsec connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe failures before considering it to have failed.

To configure the IX10 device to regularly probe the IPsec connection:

Web

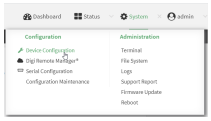
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

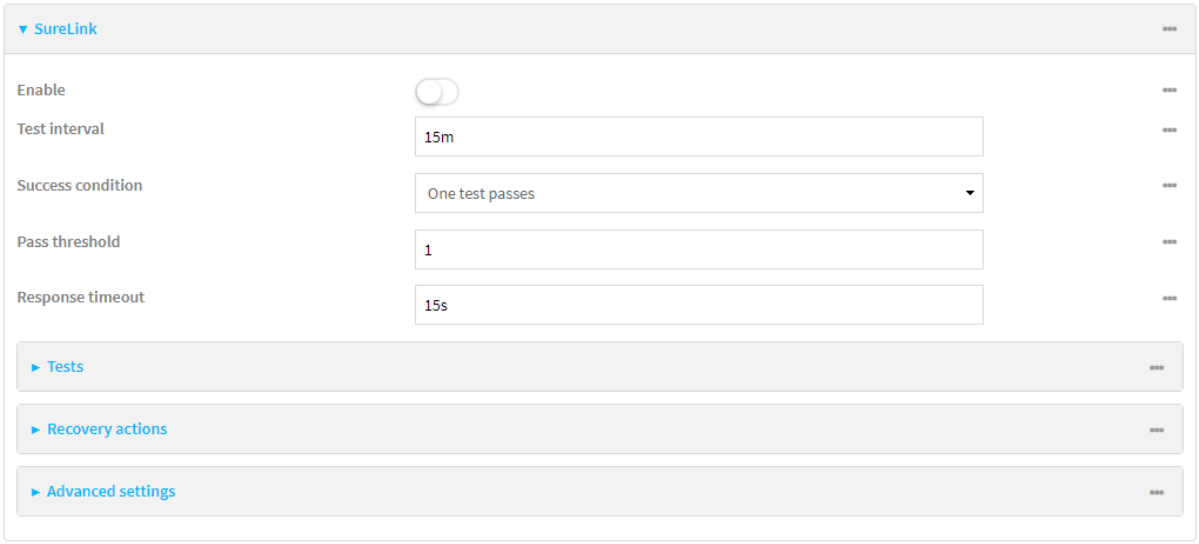
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN** > **IPsec**.
4. Create a new IPsec tunnel or select an existing one:
   - To create a new IPsec tunnel, see Configure an IPsec tunnel.
   - To edit an existing IPsec tunnel, click to expand the appropriate tunnel.
5. After creating or selecting the IPsec tunnel, click **SureLink**.



6. **Enable** SureLink.
7. (Optional) Change the **Test interval** between connectivity tests.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Interval** to ten minutes, enter **10m** or **600s**.

   The default is 15 minutes.
8. (Optional) If more than one test target is configured, for **Success condition**, select either:
   - **One test passes**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **All test pass**: All tests need to pass for SureLink to consider the interface to be up.
9. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
10. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

The default is 15 seconds.

11. Click to expand **Tests**.

    By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

    a. Click .

    New tests are enabled by default. To disable, click to toggle off **Enable**.

    b. Type a **Label** for the test.

    c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.

    d. Select the **Test type**.

    Available test types:

    - **Ping test**: Uses ICMP to determine connectivity.

      If **Ping test** is selected, complete the following:

      - **Ping target:** The type of target for the ping, one of:
        - **Hostname or IP address** of an external server.
          - **Ping host**: hostname or IP address of the server.
        - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
        - The **Interface address**.
        - The **Interface DNS** server.
      - **Ping payload size:** The number of bytes to send as part of the ping payload.
    - **DNS test**: Performs a DNS query to the named DNS server.

      If **DNS test** is selected, complete the following:

      - **DNS server**: The IP address of the DNS server.
    - **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

      If **HTTP test** is selected, complete the following:

      - **Web server**: The URL of the web server.
    - **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
    - **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **Test the interface status** is selected, complete the following:

- **Down time**: The amount of time that the interface is down before the test can be considered to have failed.

  Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

  For example, to set **Down time** to ten minutes, enter **10m** or **600s**.
- **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

  Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

  For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test**: Tests the interface with custom commands.

  If **Custom test** is selected, complete the following:

  - The **Commands to run to test**.
- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

  If **TCP connection test** is selected, complete the following:

  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.
- **Test another interface's status**: Tests the status of another interface.

  If **Test another interface's status** is selected, complete the following:

  - **Test interface**: The interface to test.
  - **IP version**: The type of IP connection, one of:
    - **Any**: Either the IPv4 or IPv6 connection must be up.
    - **Both**: Both the IPv4 or IPv6 connection must be up.
    - **IPv4**: The IPv4 connection must be up.
    - **IPv6**: The IPv6 connection must be up.
  - **Expected status**: The status required for the test to past.
    - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

e. Repeat for each additional test.

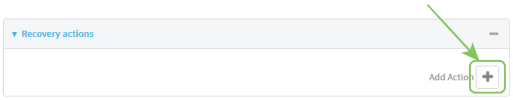
12. Add recovery actions:

    a. Click to expand **Recovery actions**.

    By default, there are two preconfigured recovery actions:

    - **Update routing**: Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
    - **Restart interface**.

b. Click .



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

c. Type a **Label** for the recovery action.

d. For **Recovery type**, select **Reboot device**.

e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

- **Change default gateway**: Increases the interface's metric to change the default gateway.

  If **Change default gateway** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Increase metric to change active default gateway**: Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Restart interface**.

  If **Restart interface** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Reset modem**: This recovery action is available for WWAN interfaces only.

  If **Reset modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Switch to alternate SIM**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **Switch to alternate SIM** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Reboot device**.

  If **Reboot device** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- Execute custom **Recovery commands**.

  If **Recovery commands** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - The **Commands to run to recovery connectivity**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Powercycle the modem**. This recovery action is available for WWAN interfaces only.

  If **Powercycle the modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

f. Repeat for each additional recovery action.

13. (Optional) Configure advanced SureLink parameters:
    a. Click to expand **Advanced settings**.
    b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

       Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

       For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

       The default is 300 seconds.

    c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

       Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

       For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

       The default is 300 seconds.

    d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.

14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new IPsec tunnel, or edit an existing one:
   - To create a new IPsec tunnel, see Configure an IPsec tunnel.
   - To edit an existing IPsec tunnel, change to the IPsec tunnel's node in the configuration schema. For example, for an IPsec tunnel named **ipsec_example**, change to the **ipsec_example** node in the configuration schema:

```
(config)> vpn ipsec tunnel ipsec_example
(config vpn ipsec tunnel ipsec_example)>
```

4. Enable SureLink:

```
(config vpn ipsec tunnel ipsec_example)> surelink enable true
(config vpn ipsec tunnel ipsec_example)>
```

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

   To add additional tests:

   a. Add a test:

```
(config vpn ipsec tunnel ipsec_example)> add surelink tests end
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

   b. New tests are enabled by default. To disable:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> enable false
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

   c. Create a label for the test:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> label string
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

   d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> ipv6 true
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

   e. Set the test type:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> test value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

where *value* is one of:

- **ping**: Uses ICMP to determine connectivity.

  If **ping** is selected, complete the following:

  - Set the **ping_method**:

    ```
    (config vpn ipsec tunnel ipsec_example surelink tests 1)> ping_method value
    (config vpn ipsec tunnel ipsec_example surelink tests 1)>
    ```

    where *value* is one of:

    - **hostname**: The hostname or IP address of an external server.
      - Set **ping_host** to the hostname or IP address of the server:

        ```
        (config vpn ipsec tunnel ipsec_example surelink tests 1)> ping_host
        hostname/IP_address
        (config vpn ipsec tunnel ipsec_example surelink tests 1)>
        ```

    - **interface_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - **interface_address**.
    - **interface_dns**: The interface's DNS server.

  - Set the number of bytes to send as part of the ping payload:

    ```
    (config vpn ipsec tunnel ipsec_example ipsec tunnel ipsec_example surelink tests
    1)> ping_size int
    (config vpn ipsec tunnel ipsec_example surelink tests 1)>
    ```

- **dns**: Performs a DNS query to the named DNS server.

  If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

  ```
  (config vpn ipsec tunnel ipsec_example surelink tests 1)> dns_server IP_address
  (config vpn ipsec tunnel ipsec_example surelink tests 1)>
  ```

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **http** is set, set the URL of the web server.

  ```
  (config vpn ipsec tunnel ipsec_example surelink tests 1)> http url
  (config vpn ipsec tunnel ipsec_example surelink tests 1)>
  ```

- **dns_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **interface_up** is set, complete the following:

- Set the amount of time that the interface is down before the test can be considered to have failed.

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> interface_down_time
value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> interface_down_time 600s
(config)>
```

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> interface_timeout value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> interface_timeout 600s
(config)>
```

- **custom_test**: Tests the interface with custom commands.

  If **custom_test** is set, set the commands to run to perform the test:

```
(config vpn ipsec tunnel ipsec_example  surelink tests 1)> custom_test_commands
"string"
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

- **tcp_connection**: Tests that the interface can reach a destination port on the configured host.

  If **tcp_connection** is selected, complete the following:

  - Set the hostname or IP address of the host to create a TCP connection to:

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> tcp_host hostname/IP_
address
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

  - Set the TCP port to create a TCP connection to.

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> tcp_port port
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

- **other**: Tests the status of another interface.

  If **other** is selected, complete the following:

  - Set the interface to test.
    i. Use the **?** to determine available interfaces:
    ii. Set the interface. For example:

    ```
    (config vpn ipsec tunnel ipsec_example surelink tests 1)> other_interface
    /network/interface/eth1
    (config vpn ipsec tunnel ipsec_example surelink tests 1)>
    ```

  - Set the type of IP connection:

    ```
    (config vpn ipsec tunnel ipsec_example surelink tests 1)> other_ip_version value
    (config vpn ipsec tunnel ipsec_example surelink tests 1)>
    ```

    where *value* is one of:
    - **any**: Either the IPv4 or IPv6 connection must be up.
    - **both**: Both the IPv4 or IPv6 connection must be up.
    - **ipv4** The IPv4 connection must be up.
    - **ipv6**: The IPv6 connection must be up.
  - The status required for the test to past.

    ```
    (config vpn ipsec tunnel ipsec_example surelink tests 1)> other_status value
    (config vpn ipsec tunnel ipsec_example surelink tests 1)>
    ```

    where *value* is one of:
    - **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

6. Add recovery actions:
   a. Type **...** to return to the root of the configuration:

   ```
   (config vpn ipsec tunnel ipsec_example surelink tests 1)> ...
   (config)>
   ```

   b. Add a recovery action:

   ```
   (config)> add vpn ipsec tunnel ipsec_example surelink actions end
   (config vpn ipsec tunnel ipsec_example surelink actions 0)>
   ```

   c. New actions are enabled by default. To disable:

   ```
   (config vpn ipsec tunnel ipsec_example surelink actions 0)> enable false
   (config vpn ipsec tunnel ipsec_example surelink actions 0)>
   ```

d. Create a label for the action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> label string
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

e. Set the type of recovery action to **reboot_device**:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> action reboot_device
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

  ```
  (config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
  (config vpn ipsec tunnel ipsec_example surelink actions 0)>
  ```

  The default is **3**.
- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

  ```
  (config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
  (config vpn ipsec tunnel ipsec_example surelink actions 0)>
  ```

f. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed. The command varies depending on whether the interface is a WAN or WWAN:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> modem_action value
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- WAN interfaces:

  ```
  (config vpn ipsec tunnel ipsec_example surelink actions 0)> action value
  (config vpn ipsec tunnel ipsec_example surelink actions 0)>
  ```

- WWAN interfaces:

  ```
  (config vpn ipsec tunnel ipsec_example surelink actions 0)> modem_action value
  (config vpn ipsec tunnel ipsec_example surelink actions 0)>
  ```

where *value* is one of:

- **update_routing_table**: Increases the interface's metric to change the default gateway.

  If **update_routing_table** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
    (config vpn ipsec tunnel ipsec_example surelink actions 0)>
    ```

    The default is **3**.

- Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> metric_adjustment_
modem int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

  The default is **100**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **restart_interface**.

  If **restart_interface** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **reset_modem**: This recovery action is available for WWAN interfaces only.

  If **reset_modem** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **switch_sim**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **switch_sim** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

  The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **modem_power_cycle**: This recovery action is available for WWAN interfaces only.

  If **modem_power_cycle** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **reboot_device**.

  If **reboot_device** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **custom_action**: Execute custom recovery commands.

  If **custom_action** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the commands to run to attempt to recovery connectivity.

```
(config network interface my_wan surelink actions 0)> custom_action_commands_
modem "string"
(config network interface my_wan surelink actions 0)>
```

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

g. Repeat for each additional recovery action.

7. Optional SureLink configuration parameters:
   a. Type **...** to return to the root of the configuration:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> ...
(config)>
```

   b. Set the test interval between connectivity tests:

```
(config)> vpn ipsec tunnel ipsec_example surelink interval value
(config)>
```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn ipsec tunnel ipsec_example surelink interval 600s
(config)>
```

   The default is **15m**.

   c. If more than one test target is configured, set the success condition:

```
(config)> vpn ipsec tunnel ipsec_example surelink success_condition value
(config)>
```

   where *value* is either:

   - **one**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **all**: All tests need to pass for SureLink to consider the interface to be up.

   d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

```
(config)> vpn ipsec tunnel ipsec_example surelink pass_threshold int
(config)>
```

   The default is **1**.

e. Set the amount of time that the device should wait for a response to a test attempt before considering it to have failed:

```
(config)> vpn ipsec tunnel ipsec_example surelink timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn ipsec tunnel ipsec_example surelink timeout 600s
(config)>
```

The default is **15s**.

f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced delayed_start value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **delayed_start** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced delayed_start 600s
(config)>
```

The default is **300s**.

g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced backoff_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **backoff_interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced backoff_interval 600s
(config)>
```

The default is 300 seconds.

h. The **interface_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced interface_gateway hostname/IP_
address
(config)>
```

8. Save the configuration and apply the change.

```
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show IPsec status and statistics

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status** > **IPsec**.

   The **IPsec** page appears.

2. To view configuration details about an IPsec tunnel, click the ✷ (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To display details about all configured IPsec tunnels, type the following at the prompt:

```
> show ipsec all

 Name   Enable  Status   Hostname
------ ------ ------- ---------------
ipsec1  true    up      192.168.2.1
vpn1    false   pending  192.168.3.1

>
```

3. To display details about a specific tunnel:

```
> show ipsec tunnel ipsec1

 Tunnel              : ipsec1
 Enable              : true
 Status              : pending
 Hostname            : 192.168.2.1
 Zone                : ipsec
 Mode                : tunnel
 Type                : esp
```

```
>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Debug an IPsec configuration

If you experience issues with an IPsec tunnel not being successfully negotiated with the remote end of the tunnel, you can enable IPsec debug messages to be written to the system log. See View system and event logs for more information about viewing the system log.

Web

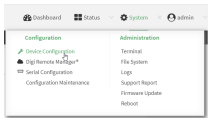
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec**.
4. Click to expand **Advanced**.
5. For **Debug level**, select one of the following:
   - **Disable debug messages**.
   - **Basic auditing debug**: Logs basic auditing information, (for example, SA up/SA down).
   - **Generic control flow** : Select this for basic debugging information.
   - **Detailed control flow** : More detailed debugging control flow.
   - **Raw data**: Includes raw data dumps in hexadecimal format.
   - **Sensitive material**: Also includes sensitive material in dumps (for example, encryption keys).
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```
3. Set the IPsec debug value:

   ```
   config> vpn ipsec advanced debug value
   config>
   ```

   where *value* is one of:

   - **none**. (Default) No debug messages are written.
   - **basic_auditing**: Logs basic auditing information, (for example, SA up/SA down).
   - **generic_control**: Select this for basic debugging information.
   - **detailed_control**: More detailed debugging control flow.
   - **raw_data**: Includes raw data dumps in hexadecimal format.
   - **sensitive_data**: Also includes sensitive material in dumps (for example, encryption keys).
4. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```
5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure a Simple Certificate Enrollment Protocol client

WARNING! The Simple Certificate Enrollment Protocol (SCEP) uses unencrypted HTTP communication. Please ensure you are utilizing a VPN to secure your communications.

Simple Certificate Enrollment Protocol (SCEP) is a mechanism that allows for large-scale X.509 certificate deployment. You can configure IX10 device to function as a SCEP client that will connect to a SCEP server that is used to sign Certificate Signing Requests (CSRs), provide Certificate Revocation Lists (CRLs), and distribute valid certificates from a Certificate Authority (CA).

Required configuration

- Enable the SCEP client.
- The fully-qualified domain name of the SCEP server to be used for certificate requests.
- The challenge password provided by the SCEP server that the SCEP client will use when making SCEP requests.
- The distinguished name to be used for the CSR.

Additional configuration

- The number of days that the certificate enrollment can be renewed, prior to the request expiring.

Web

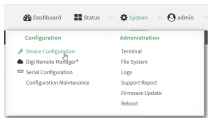
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

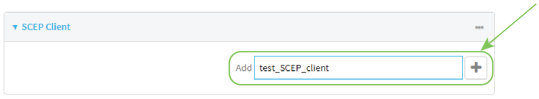
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

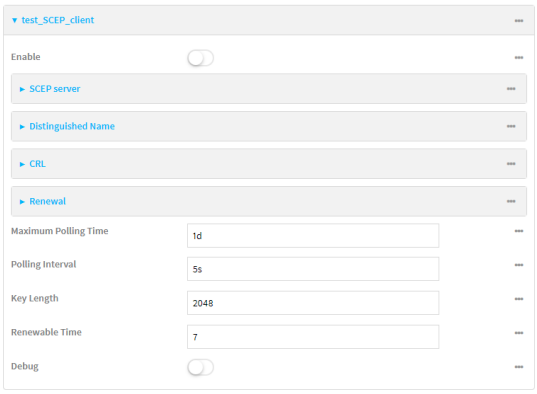
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **SCEP Client**.
4. For **Add clients**, enter a name for the SCEP client and click .

   The new SCEP client configuration is displayed.



5. Click **Enable** to enable the SCEP client.
6. For **Maximum Polling Time**, type the maximum time that the device will poll the SCEP server, when operating in manual mode.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

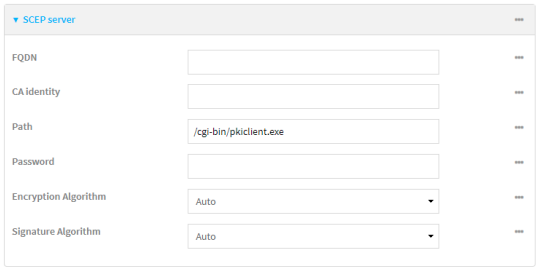
   For example, to set **Maximum Polling Time** to ten minutes, enter **10m** or **600s**.

   The default is **1d**.
7. For **Polling Interval**, type the amount of time that the device should wait between polling attempts, when operating in manual mode.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

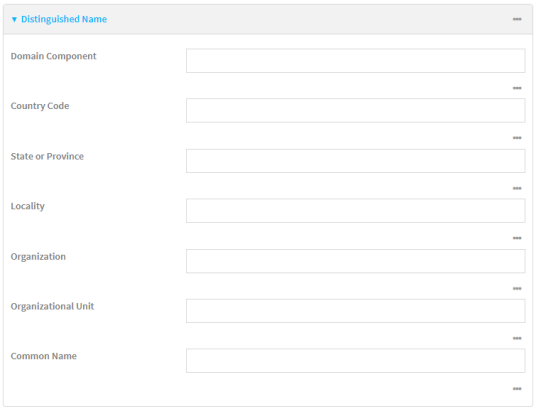
   For example, to set **Polling Interval** to ten minutes, enter **10m** or **600s**.

   The default is **5s**.
8. For **Key Length**, type the bit size of the private key. The default is **2048**.
9. For **Renewable Time**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value is configured on the SCEP server, and is used by the IX10 device to determine when to start attempting to auto-renew an existing certificate. The default is **7**.
10. (Optional) Click **Debug** to enable verbose logging in /var/log/scep_client.
11. Click to expand **SCEP server**.



12. For **FQDN**, type the fully qualified domain name or IP address of the SCEP server.
13. (Optional) For **CA identity**, type a string that will be understood by the certificate authority. For example, it could be a domain name or a user name. If the certificate authority has multiple CA certificates, this field can be used to distinguish which is required.

14. For **Path**, Type the HTTP URL path required for accessing the certificate authority. You should leave this option at the default of **/cgi-bin/pkiclient.exe** unless directed by the CA to use another path.
15. For **Password**, type the challenge password as configured on the SCEP server.
16. For **Encryption Algorithm**, select the PKCS#7 encryption algorithm. The default is **Auto**, which automatically selects the best algorithm.
17. For **Signature Algorithm**, select the PKCS#7 signature algorithm. The default is **Auto**, which automatically selects the best algorithm.
18. Click to expand **Distinguished Name**.



19. Type the value for each appropriate Distinguished Name attribute.
20. (Optional) Configure the certificate revocation list (CRL):
    a. Click to expand **CRL**.
    b. Click **Enable** to enable the CRL.
    c. For **Type**, select the type of CRL:
        - **URL**: The URL to the file name used to access the certificate revocation list from the CA.
        - **CRLDP**: The CRL distribution point.
        - **getCRL**: A CRL query using the issuer name and serial number from the certificate whose revocation status is being queried.

       The default is **URL**.
    d. If **Type** is set to **URL**, for **URL**, type the URL to be used.
21. Configure certificate renewal:
    a. Click to expand **Renewal**.
    b. Click **Use New Private Key** to enable the creation of a new private key for renewal requests.
    c. **Use Client Certificate** is enabled by default. Click to disable the use of a client certificate for renewal requrests.
22. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new SCEP client:

```
(config)> add network scep_client scep_client_name
(config network scep_client scep_client_name
)>
```

4. Enable the SCEP client:

```
(config network scep_client scep_client_name)> enable true
(config network scep_client scep_client_name)>
```

5. Set the url parameter to the fully qualified domain name or IP address of the SCEP server:

```
(config network scep_client scep_client_name)> server url https://scep.example.com
(config network scep_client scep_client_name)>
```

6. (Optional) Set a CA identity string that will be understood by the certificate authority. For example, it could be a domain name or a user name. If the certificate authority has multiple CA certificates, this field can be used to distinguish which is required.

```
(config network scep_client scep_client_name)> server ca_ident string
(config network scep_client scep_client_name)>
```

7. Set the HTTP URL path required for accessing the certificate authority. You should leave this option at the default of **/cgi-bin/pkiclient.exe** unless directed by the CA to use another path.

```
(config network scep_client scep_client_name)> server path path
(config network scep_client scep_client_name)>
```

8. Set the challenge password as configured on the SCEP server:

```
(config network scep_client scep_client_name)> server password challenge_password
(config network scep_client scep_client_name)>
```

9. Set Distinguished Name attributes:
   a. Set the Domain Component:

```
(config network scep_client scep_client_name)> distinguished_name dc value
(config network scep_client scep_client_name)>
```

   b. Set the two letter Country Code:

```
(config network scep_client scep_client_name)> distinguished_name c value
(config network scep_client scep_client_name)>
```

c. Set the State or Province:

```
(config network scep_client scep_client_name)> distinguished_name st value
(config network scep_clientscep_client_name )>
```

d. Set the Locality:

```
(config network scep_client scep_client_name)> distinguished_name l value
(config network scep_client scep_client_name)>
```

e. Set the Organization:

```
(config network scep_client scep_client_name)> distinguished_name o value
(config network scep_client scep_client_name)>
```

f. Set the Organizational Unit:

```
(config network scep_client scep_client_name)> distinguished_name ou value
(config network scep_client scep_client_name)>
```

g. Set the Common Name:

```
(config network scep_client scep_client_name)> distinguished_name cn value
(config network scep_client scep_client_name)>
```

10. (Optional) Configure the certificate revocation list (CRL):

a. Enable the CRL:

```
(config network scep_client scep_client_name)> crl enable true
(config network scep_client scep_client_name)>
```

b. Set the type of CRL:

```
(config network scep_client scep_client_name)> crl type value
(config network scep_client scep_client_name)>
```

where *value* is one of:

- **url**: The URL to the file name used to access the certificate revocation list from the CA.
- **crldp**: The CRL distribution point.
- **getCRL**: A CRL query using the issuer name and serial number from the certificate whose revocation status is being queried.

The default is **url**.

c. If **type** is set to **url**, set the URL that should be used:

```
(config network scep_client scep_client_name)> crl url value
(config network scep_client scep_client_name)>
```

11. Configure certificate renewal:

a. To enable the creation of a new private key for renewal requests:

```
(config network scep_client scep_client_name)> renewal new_key true
(config network scep_client scep_client_name)>
```

b. The use of a client certificate for renewal requests is enabled by default. To disable:

```
(config network scep_client scep_client_name)> renewal use_client_cert false
(config network scep_client scep_client_name)>
```

12. Set the maximum time that the device will poll the SCEP server, when operating in manual mode:

```
(config network scep_client scep_client_name)> max_poll_time value
(config network scep_client scep_client_name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **max_poll_time** to ten minutes, enter either **10m** or **600s**:

```
(config network scep_client scep_client_name)> max_poll_time 600s
(config network scep_client scep_client_name)>
```

The default is **1d**.

13. Set the amount of time that the device should wait between polling attempts, when operating in manual mode:

```
(config network scep_client scep_client_name)> polling_interval value
(config network scep_client scep_client_name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **polling_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network scep_client scep_client_name)> polling_interval 600s
(config network scep_client scep_client_name)>
```

The default is **5s**.

14. Set the bit size of the private key:

```
(config network scep_client scep_client_name)> key_length int
(config network scep_client scep_client_name)>
```

The default is **2048**.

15. Set the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value is configured on the SCEP server, and is used by the IX10 device to determine when to start attempting to auto-renew an existing certificate. The default is **7**.

```
(config network scep_client scep_client_name)> renewable_time integer
(config network scep_client scep_client_name)>
```

16. (Optional) Enable verbose logging in /var/log/scep_client:

```
(config network scep_client scep_client_name)> debug true
(config network scep_client scep_client_name)>
```

17. Save the configuration and apply the change.

```
(config network scep_client scep_client_name)> save
Configuration saved.
>
```

18. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example: SCEP client configuration with Fortinet SCEP server

In this example configuration, we will configure the IX10 device as a SCEP client that will connect to a Fortinet SCEP server.

Fortinet configuration

On the Fortinet server:

1. Enable ports for SCEP services:
   a. From the menu, select **Network** > **Interfaces**.
   b. Select the appopriate port and click **Edit**.
   c. For **Access Rights** > **Services**, enable the following services:
      - **HTTPS** > **SCEP**
      - **HTTPS** > **CRL Downloads**
      - **HTTP** > **SCEP**
      - **HTTP** > **CRL Downloads**
   d. The remaining fields can be left at their defaults or changed as appropriate.
   e. Click **OK**.
2. Create a Certificate Authority (CA):
   a. From the menu, click **Certificate Authorities** > **Local CAs**.
   b. Click **Create New**.
   c. Type a **Certificate ID** for the CA, for example, **fortinet_example_ca**.
   d. Complete the **Subject Information** fields.
   e. The remaining fields can be left at their defaults or changed as appropriate.
   f. Click **OK**.
3. Edit SCEP settings:
   a. From the menu, click **SCEP** > **General**.
   b. Click **Enable SCEP** if it is not enabled.
   c. For **Default enrollment password**, enter a password. The password entered here must correspond to the challenge password configured for the SCEP client on the IX10 device.

d. The remaining fields can be left at their defaults or changed as appropriate.
e. Click **OK**.

4. Create an **Enrollment Request**:
   a. From the menu, click **SCEP** > **Enrollment Requests**.
   b. Click **Create New**.
   c. For **Automatic request type**, select **Wildcard**.
   d. For **Certificate authority**, select the CA created in step 1, above.
   e. Complete the **Subject Information** fields. The Distinguished Name (DN) attributes entered here must correspond to the Distinguished Name attributes configured for the SCEP client on the IX10 device.
   f. For **Renewal** > **Allow renewal *x* days before the certified is expired**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. The **Renewable Time** setting on the IX10 device must match the setting of this parameter.
   g. The remaining fields can be left at their defaults or changed as appropriate.
   h. Click **OK**.

IX10 configuration

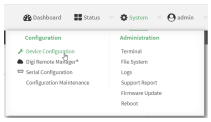
On the IX10 device:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

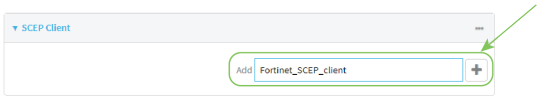
   Remote Manager:
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

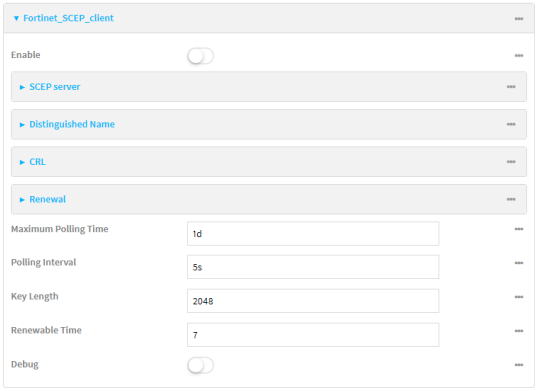
   

   The **Configuration** window is displayed.
3. Click **Network** > **SCEP Client**.

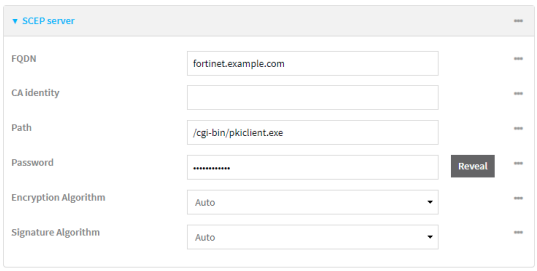
4. For **Add clients**, enter a name for the SCEP client and click ♡.



The new SCEP client configuration is displayed.

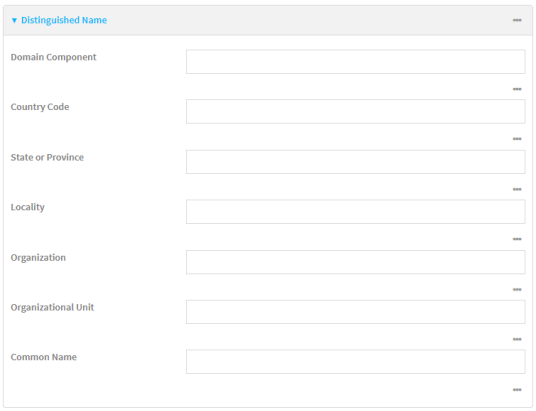


5. Click **Enable** to enable the SCEP client.
6. For **Renewable Time**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value must match the setting of the **Allow renewal *x* days before the certified is expired** option on the Fortinet server.
7. (Optional) Click **Debug** to enable verbose logging in /var/log/scep_client.
8. Click to expand **SCEP server**.



9. For **FQDN**, type the fully qualified domain name or IP address of the Fortinet server.
10. For **Password**, type the challenge password. This corresponds to the **Default enrollment password** on the Fortinet server.

11. Click to expand **Distinguished Name**.



12. Type the value for each appropriate Distinguished Name attribute. The values entered here must correspond to the DN attributes in the **Enrollment Request** on the Fortinet server.
13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new SCEP client, for example, **Fortinet_SCEP_client**:

```
(config)> add network scep_client Fortinet_SCEP_client
(config network scep_client Fortinet_SCEP_client
)>
```

4. Enable the SCEP client:

```
(config network scep_client Fortinet_SCEP_client)> enable true
(config network scep_client Fortinet_SCEP_client)>
```

5. Set the url parameter to the fully qualified domain name or IP address of the SCEP server:

```
(config network scep_client Fortinet_SCEP_client)> server url https://fortinet.example.com
(config network scep_client Fortinet_SCEP_client)>
```

6. Set the challenge password as configured on the SCEP server. This corresponds to the **Default enrollment password** on the Fortinet server.

```
(config network scep_client Fortinet_SCEP_client)> server password challenge_password
(config network scep_client Fortinet_SCEP_client)>
```

7. Set Distinguished Name attributes. The values entered here must correspond to the DN attributes in the **Enrollment Request** on the Fortinet server.
   a. Set the Domain Component:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name dc value
   (config network scep_client Fortinet_SCEP_client)>
   ```

   b. Set the two letter Country Code:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name c value
   (config network scep_client Fortinet_SCEP_client)>
   ```

   c. Set the State or Province:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name st value
   (config network scep_client  Fortinet_SCEP_client)>
   ```

   d. Set the Locality:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name l value
   (config network scep_client Fortinet_SCEP_client)>
   ```

   e. Set the Organization:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name o value
   (config network scep_client Fortinet_SCEP_client)>
   ```

   f. Set the Organizational Unit:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name ou value
   (config network scep_client Fortinet_SCEP_client)>
   ```

   g. Set the Common Name:

   ```
   (config network scep_client Fortinet_SCEP_client)> distinguished_name cn value
   (config network scep_client Fortinet_SCEP_client)>
   ```

8. Set the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value must match the setting of the **Allow renewal *x* days before the certified is expired** option on the Fortinet server.

   ```
   (config network scep_client Fortinet_SCEP_client)> renewable_time integer
   (config network scep_client Fortinet_SCEP_client)>
   ```

9. (Optional) Enable verbose logging in /var/log/scep_client:

   ```
   (config network scep_client Fortinet_SCEP_client)> debug true
   (config network scep_client Fortinet_SCEP_client)>
   ```

10. Save the configuration and apply the change.

    ```
    (config network scep_client Fortinet_SCEP_client)> save
    Configuration saved.
    >
    ```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show SCEP client status and information

You can show general SCEP client information for all SCEP clients, and specific information for an individual SCEP client.

This procedure is only available from the Admin CLI.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured SCEP clients, type the following at the prompt:

```
> show scep-client

SCEP   Enabled  Expiry
-----  -------  -------
test   true     Jun  4 19:05:25 2022 GMT
test1  false

>
```

3. To display details about a specific SCEP client:

```
> show scep-client name name
```

   For example:

```
> show scep-client name test

test SCEP Status
----------------
Enabled    : true

Client Certificate
------------------
Subject    : C=US,ST=MA,L=BOS,O=Digi,OU=IT1,CN=dummy
Issuer     : CN=TA-SCEP-1-CA
Serial     : 1100000017A30C8EDD3805EB52000000000017
Expiry     : Jun  4 19:05:25 2022 GMT

Certificate Authority Certificate {1}
--------------------------------------
Subject    : C=US,CN=TA-SCEP-1-MSCEP-RA
Issuer     : CN=TA-SCEP-1-CA
```

```
Serial     : 1100000002A1E755981C0C3F34000000000002
Expiry     : Apr 25 13:42:47 2023 GMT

Certificate Authority Certificate {2}
-------------------------------------
Subject    : C=US,CN=TA-SCEP-1-MSCEP-RA
Issuer     : CN=TA-SCEP-1-CA
Serial     : 1100000003268AFB5E98BFCA73000000000003
Expiry     : Apr 25 13:42:48 2023 GMT

Certificate Authority Certificate {3}
-------------------------------------
Subject    : CN=TA-SCEP-1-CA
Issuer     : CN=TA-SCEP-1-CA
Serial     : 681670E9EFB7FCB74E79C33DD9D54847
Expiry     : Apr 25 13:36:42 2027 GMT

Certificate Revocation List
---------------------------
Issuer     : CN=TA-SCEP-1-CA
Last Update : May 23 13:27:21 2022 GMT


>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

OpenVPN

OpenVPN is an open-source Virtual Private Network (VPN) technology that creates secure point-to-point or site-to-site connections in routed or bridged configurations. OpenVPN uses a custom security protocol that is Secure Socket Layer (SSL) / Transport Layer Security (TLS) for key exchange. It uses standard encryption and authentication algorithms for data privacy and authentication over TCP or UDP.

The OpenVPN server can push the network configuration, such as the topology and IP routes, to OpenVPN clients. This makes OpenVPN simpler to configure as it reduces the chances of a configuration mismatch between the client and server. OpenVPN also supports cipher negotiation between the client and server. This means you can configure the OpenVPN server and clients with a range of different cipher options and the server will negotiate with the client on the cipher to use for the connection.

For more information on OpenVPN, see www.openvpn.net.

OpenVPN modes:

There are two modes for running OpenVPN:

- Routing mode, also known as TUN.
- Bridging mode, also known as TAP.

Routing (TUN) mode

In routing mode, each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.

The manner in which the IP subnets are defined depends on the OpenVPN topology in use. The IX10 device supports two types of OpenVPN topology:

OpenVPN Topology	Subnet definition method
net30	Each OpenVPN client is assigned a **/30** subnet within the IP subnet specified in the OpenVPN server configuration. With net30 topology, pushed routes are used, with the exception of the default route. Automatic route pushing (exec) is not allowed, because this would not inform the firewall and would be blocked.
subnet	Each OpenVPN client connected to the OpenVPN server is assigned an IP address within the IP subnet specified in the OpenVPN server configuration. For the IX10 device, pushed routes are not allowed; you will need to manually configure routes on the device.

For more information on OpenVPN topologies, see OpenVPN topology.

Bridging (TAP) mode

In bridging mode, a LAN interface on the OpenVPN server is assigned to OpenVPN. The LAN interfaces of the OpenVPN clients are on the same IP subnet as the OpenVPN server's LAN interface. This means that devices connected to the OpenVPN client's LAN interface are on the same IP subnet as devices. The IX10 device supports two mechanisms for configuring an OpenVPN server in TAP mode:

- OpenVPN managed—The IX10 device creates the interface and then uses its standard configuration to set up the connection (for example, its standard DHCP server configuration).
- Device only—IP addressing is controlled by the system, not by OpenVPN.

Additional OpenVPN information

For more information on OpenVPN, see these resources:

Bridging vs. routing

OpenVPN/Routing

Configure an OpenVPN server

Required configuration items

- Enable the OpenVPN server.

  The OpenVPN server is enabled by default.
- The mode used by the OpenVPN server, one of:
  - **TUN (OpenVPN managed)**—Also known as routing mode. Each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.
  - **TAP - OpenVPN managed**—Also know as bridging mode. A more advanced implementation of OpenVPN. The IX10 device creates an OpenVPN interface and uses standard interface configuration (for example, a standard DHCP server configuration).
  - **TAP - Device only**—An alternate form of OpenVPN bridging mode, in which the device, rather than OpenVPN, controls the interface configuration. If this method is is, the OpenVPN server must be included as a device in either an interface or a bridge.
- The firewall zone to be used by the OpenVPN server.
- The IP network and subnet mask of the OpenVPN server.
- The server's Certificate authority (CA) certificate, and public, private and Diffie-Hellman (DH) keys.
- An OpenVPN authentication group and an OpenVPN user.
- Determine the method of certificate management:
  - Certificates managed by the server.
  - Certificates created externally and added to the server.
- If certificates are created and added to the server, determine the level of authentication:
  - Certificate authentication only.
  - Username and password authentication only.
  - Certificate and username and password authentication.

  If username and password authentication is used, you must create an OpenVPN authentication group and user. See Configure an OpenVPN Authentication Group and User for instructions.

- Certificates and keys:
  - The **CA certificate** (usually in a ca.crt file).
  - The **Public key** (for example, server.crt)
  - The **Private key** (for example, server.key).
  - The **Diffie Hellman key** (usually in dh2048.pem).
- Active recovery configuration. See Configure SureLink active recovery for OpenVPN for information about OpenVPN active recovery.

Additional configuration items

- The route metric for the OpenVPN server.
- The range of IP addresses that the OpenVPN server will provide to clients.
- The TCP/UDP port to use. By default, the IX10 device uses port **1194**.
- Access control list configuration to restrict access to the OpenVPN server through the firewall.
- Additional OpenVPN parameters.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

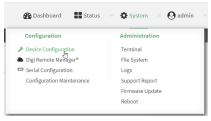
   b. Click the **Device ID**.

   c. Click **Settings**.

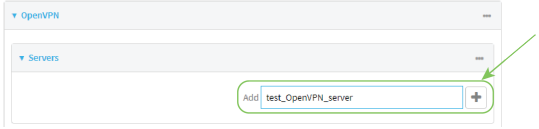
   d. Click to expand **Config**.

   Local Web UI:

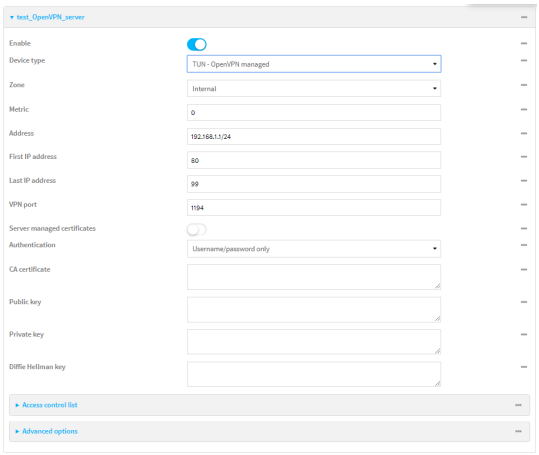
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **OpenVPN** > **Servers**.
4. For **Add**, type a name for the OpenVPN server and click .



The new OpenVPN server configuration is displayed.



The OpenVPN server is enabled by default. To disable, toggle off **Enable**.

5. For **Device type**, select the mode used by the OpenVPN server, either:
   - **TUN (OpenVPN managed)**
   - **TAP - OpenVPN managed**
   - **TAP - Device only**

   See OpenVPN for information about OpenVPN server modes.
6. If **TUN (OpenVPN managed)** or **TAP - OpenVPN managed** is selected for **Device type**:
   a. For **Zone**, select the firewall zone for the OpenVPN server. For TUN device types, this should be set to **Internal** to treat clients as LAN devices.
   b. (Optional) Select the **Metric** for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used. The default setting is **0**.
   c. For **Address**, type the IP address and subnet mask of the OpenVPN server.
   d. (Optional) For **First IP address** and **Last IP address**, set the range of IP addresses that the OpenVPN server will use when providing IP addresses to clients. The default is from **80** to **99**.
7. (Optional) Set the **VPN port** that the OpenVPN server will use. The default is **1194**.
8. For **Server managed certificates**, determine the method of certificate management. If enabled, the server will manage certificates. If not enabled, certificates must be created externally and added to the server.
9. If **Server managed certificates** is not enabled:
   a. Select the **Authentication** type:
      - **Certificate only**: Uses only certificates for client authentication. Each client requires a public and private key.
      - **Username/password only**: Uses a username and password for client authentication. You must create an OpenVPN authentication group and user. See Configure an OpenVPN Authentication Group and User for instructions.
      - **Certificate and username/password**: Uses both certificates and a username and password for client authentication. Each client requires a public and private key,

and you must create an OpenVPN authentication group and user. See Configure an OpenVPN Authentication Group and User for instructions.

b. Paste the contents of the **CA certificate** (usually in a ca.crt file), the **Public key** (for example, server.crt), the **Private key** (for example, server.key), and the **Diffie Hellman key** (usually in dh2048.pem) into their respective fields. The contents will be hidden when the configuration is saved.

10. (Optional) Click to expand **Access control list** to restrict access to the OpenVPN server:
    - To limit access to specified IPv4 addresses and networks:
      a. Click **IPv4 Addresses**.
      b. For **Add Address**, click .
      c. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
         - A single IP address or host name.
         - A network designation in CIDR notation, for example, 192.168.1.0/24.
         - **any**: No limit to IPv4 addresses that can access the service-type.
      d. Click again to list additional IP addresses or networks.
    - To limit access to specified IPv6 addresses and networks:
      a. Click **IPv6 Addresses**.
      b. For **Add Address**, click .
      c. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
         - A single IP address or host name.
         - A network designation in CIDR notation, for example, 2001:db8::/48.
         - **any**: No limit to IPv6 addresses that can access the service-type.
      d. Click again to list additional IP addresses or networks.
    - To limit access to hosts connected through a specified interface on the device:
      a. Click **Interfaces**.
      b. For **Add Interface**, click .
      c. For **Interface**, select the appropriate interface from the dropdown.
      d. Click again to allow access through additional interfaces.
    - To limit access based on firewall zones:
      a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
      b. For **Add Zone**, click .
      c. For **Zone**, select the appropriate firewall zone from the dropdown.
         See Firewall configuration for information about firewall zones.
      d. Click again to allow access through additional firewall zones.

11. (Optional) Click to expand **Advanced Options** to manually set additional OpenVPN parameters.
    a. Click **Enable** to enable the use of additional OpenVPN parameters.
    b. Click **Override** if the additional OpenVPN parameters should override default options.

c. For **OpenVPN parameters**, type the additional OpenVPN parameters.

12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> add vpn openvpn server name
(config vpn openvpn server name)>
```

   where *name* is the name of the OpenVPN server.

   The OpenVPN server is enabled by default. To disable the server, type:

```
(config vpn openvpn server name)> enable false
(config vpn openvpn server name)>
```

4. Set the mode used by the OpenVPN server:

```
(config vpn openvpn server name)> device_type value
(config vpn openvpn server name)>
```

   where *value* is one of:

   - **TUN (OpenVPN managed)**—Also known as routing mode. Each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.
   - **TAP - OpenVPN managed**—Also know as bridging mode. A more advanced implementation of OpenVPN. The IX10 device creates an OpenVPN interface and uses standard interface configuration (for example, a standard DHCP server configuration).
   - **TAP - Device only**—An alternate form of OpenVPN bridging mode, in which the device, rather than OpenVPN, controls the interface configuration. If this method is is, the OpenVPN server must be included as a device in either an interface or a bridge.

   See OpenVPN for information about OpenVPN modes. The default is **tun**.

5. If **tap** or **tun** are set for **device_type**:

   a. Set the IP address and subnet mask of the OpenVPN server.

```
(config vpn openvpn server name)> address ip_address/netmask
(config vpn openvpn server name)>
```

b. Set the firewall zone for the OpenVPN server. For TUN device types, this should be set to **internal** to treat clients as LAN devices.

```
(config vpn openvpn server name)> zone value
(config vpn openvpn server name)>
```

To view a list of available zones:

```
(config vpn openvpn server name)> firewall zone ?

Zone: The zone for the local TUN interface. To treat clients as LAN devices this would usually be
set to internal.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:

(config vpn openvpn server name)>
```

c. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

```
(config vpn openvpn server name)> metric value
(config vpn openvpn server name)>
```

where *value* is an interger between **0** and **65535**. The default is **0**.

d. (Optional) Set the range of IP addresses that the OpenVPN server will use when providing IP addresses to clients:

   i. Set the first address in the range limit:

```
(config vpn openvpn server name)> server_first_ip value
(config vpn openvpn server name)>
```

   where *value* is a number between **1** and **255**. The number entered here will represent the first client IP address. For example, if **address** is set to **192.168.1.1/24** and **server_first_ip** is set to **80**, the first client IP address will be 192.168.1.80.

   The default is from **80**.

   ii. Set the last address in the range limit:

```
(config vpn openvpn server name)> server_last_ip value
(config vpn openvpn server name)>
```

   where *value* is a number between **1** and **255**. The number entered here will represent the last client IP address. For example, if **address** is set to **192.168.1.1/24** and **server_last_ip** is set to **99**, the last client IP address will be 192.168.1.80.

The default is from **80**.

6. (Optional) Set the port that the OpenVPN server will use:

```
(config vpn openvpn server name)> port port
(config vpn openvpn server name)>
```

The default is **1194**.

7. Determine the method of certificate management:
   a. To allow the server to manage certificates:

```
(config vpn openvpn server name)> autogenerate true
(config vpn openvpn server name)>
```

   b. To create certificates externally and add them to the server

```
(config vpn openvpn server name)> autogenerate false
(config vpn openvpn server name)>
```

   The default setting is **false**.

   c. If **autogenerate** is set to false:
      i. Set the authentication type:

```
(config vpn openvpn server name)> authentication value
(config vpn openvpn server name)>
```

      where *value* is one of:
      - **cert**: Uses only certificates for client authentication. Each client requires a public and private key.
      - **passwd**: Uses a username and password for client authentication. You must create an OpenVPN authentication group and user. See Configure an OpenVPN Authentication Group and User for instructions.
      - **cert_passwd**: Uses both certificates and a username and password for client authentication. Each client requires a public and private key, and you must create an OpenVPN authentication group and user. See Configure an OpenVPN Authentication Group and User for instructions.

      ii. Paste the contents of the CA certificate (usually in a ca.crt file) into the value of the **cacert** parameter:

```
(config vpn openvpn server name)> cacert value
(config vpn openvpn server name)>
```

      iii. Paste the contents of the public key (for example, server.crt) into the value of the **server_cert** parameter:

```
(config vpn openvpn server name)> server_cert value
(config vpn openvpn server name)>
```

      iv. Paste the contents of the private key (for example, server.key) into the value of the **server_key** parameter:

```
(config vpn openvpn server name)> server_key value
(config vpn openvpn server name)>
```

v. Paste the contents of the Diffie Hellman key (usually in dh2048.pem) into the value of the **diffie** parameter:

```
(config vpn openvpn server name)> diffie value
(config vpn openvpn server name)>
```

8. (Optional) Set the access control list to restrict access to the OpenVPN server:
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config vpn openvpn server name)> add acl address end value
     (config vpn openvpn server name)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

     ```
     (config vpn openvpn server name)> add acl address6 end value
     (config vpn openvpn server name)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

     ```
     (config vpn openvpn server name)> add acl interface end value
     (config vpn openvpn server name)>
     ```

     Where *value* is an interface defined on your device.

     Display a list of available interfaces:

     Use **... network interface ?** to display interface information:

     ```
     (config vpn openvpn server name)> ... network interface ?

     Interfaces

     Additional Configuration
     ----------------------------------------
     setupip          Setup IP
     setuplinklocalip     Setup Link-local IP
     eth              ETH
     ```

```
loopback        Loopback
modem           Modem

config vpn openvpn server name)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config vpn openvpn server name)> add acl zone end value
(config vpn openvpn server name)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config vpn openvpn server name)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config vpn openvpn server name)>
```

Repeat this step to include additional firewall zones.

9. (Optional) Set additional OpenVPN parameters.
   a. Enable the use of additional OpenVPN parameters:

```
(config vpn openvpn server name)> advanced_options enable true
(config vpn openvpn server name)>
```

   b. Configure whether the additional OpenVPN parameters should override default options:

```
(config vpn openvpn server name)> advanced_options override true
(config vpn openvpn server name)>
```

   c. Set the additional OpenVPN parameters:

```
(config vpn openvpn server name)> extra parameters
(config vpn openvpn server name)>
```

10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure an OpenVPN Authentication Group and User

If username and password authentication is used for the OpenVPN server, you must create an OpenVPN authentication group and user.

See Configure an OpenVPN server for information about configuring an OpenVPN server to use username and password authentication. See IX10 user authentication for more information about creating authentication groups and users.

Web

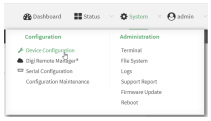
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

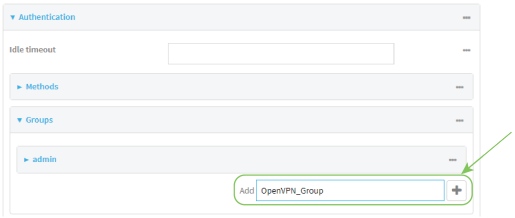
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

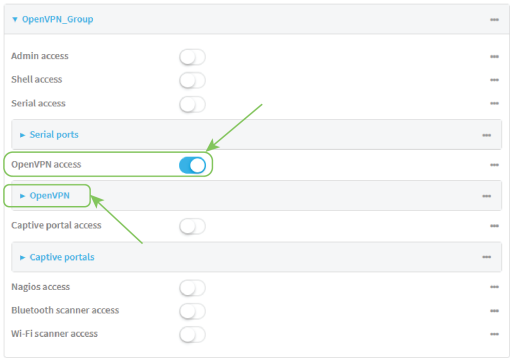
   

   The **Configuration** window is displayed.

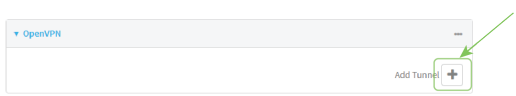
3. Add an OpenVPN authentication group:
   a. Click **Authentication** > **Groups**.
   b. For **Add Group**, type a name for the group (for example, **OpenVPN_Group**) and click ⚡



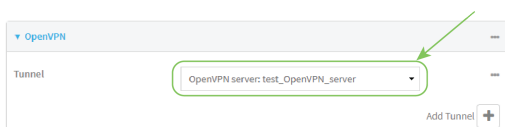
The new authentication group configuration is displayed.



   c. Click **OpenVPN access** to enable OpenVPN access rights for users of this group.
   d. Click to expand the **OpenVPN** node.
   e. Click ⚡ to add a tunnel.

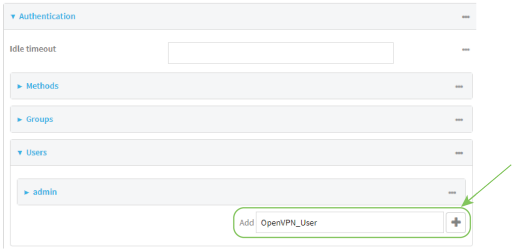


   f. For **Tunnel**, select an OpenVPN tunnel to which users of this group will have access.



   g. Repeat to add additional OpenVPN tunnels.

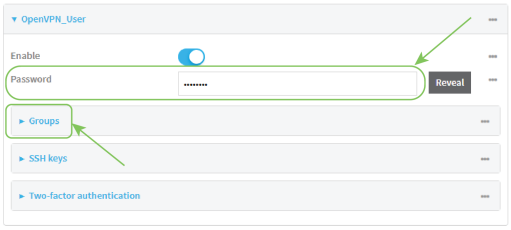
4. Add an OpenVPN authentication user:
   a. Click **Authentication** > **Users**.
   b. For **Add**, type a name for the user (for example, **OpenVPN_User**) and click ⊕.



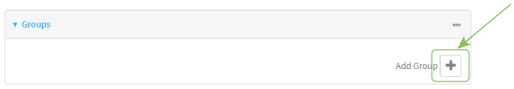
   c. Type a password for the user.

      This password is used for local authentication of the user. You can also configure the user to use RADIUS or TACACS+ authentication by configuring authentication methods. See User authentication methods for information.

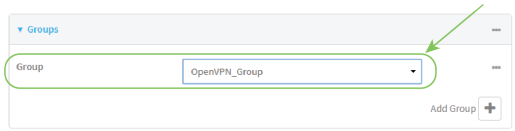
   d. Click to expand the **Groups** node.



   e. Click ⊕ to add a group to the user.



   f. Select a **Group** with **OpenVPN access** enabled.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **add auth group** command to add a new authentication. For example, to add a group named **OpenVPN_Group**:

```
(config)> add auth group OpenVPN_Group
(config auth group OpenVPN_Group)>
```

4. Enable OpenVPN access rights for users of this group:

```
(config auth group OpenVPN_Group)> acl openvpn enable true
```

5. Add an OpenVPN tunnel to which users of this group will have access:

   a. Determine available tunnels:

```
(config auth group OpenVPN_Group)> .. .. .. vpn openvpn server ?

Servers: A list of openvpn servers

 Additional Configuration
 ------------------------------------------------------------------------------
OpenVPN_server1         OpenVPN server

(config auth group OpenVPN_Group)>
```

   b. Add a tunnel:

```
(config auth group OpenVPN_Group)> add auth group test acl openvpn tunnels end
/vpn/openvpn/server/OpenVPN_server1
(config auth group OpenVPN_Group)>
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure an OpenVPN client by using an .ovpn file

Required configuration items

- Enable the OpenVPN client.

  The OpenVPN client is enabled by default.
- The firewall zone to be used by the OpenVPN client.

Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.

See Configure SureLink active recovery for OpenVPN for information about OpenVPN active recovery.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

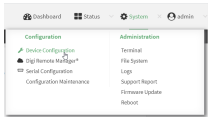
   b. Click the **Device ID**.

   c. Click **Settings**.

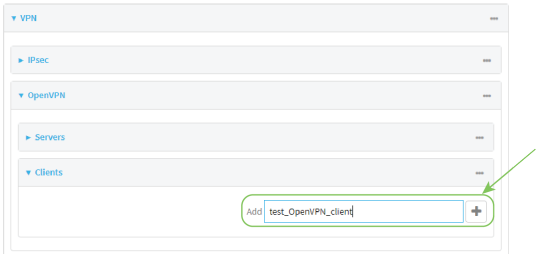
   d. Click to expand **Config**.

   Local Web UI:

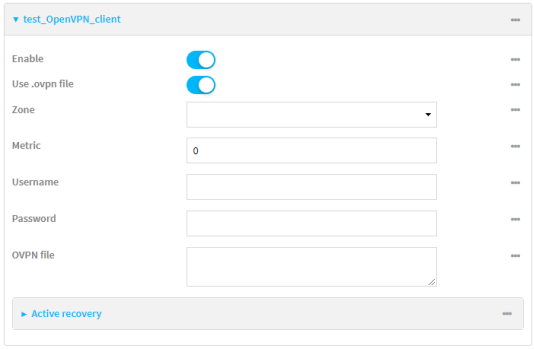
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **OpenVPN** > **Clients**.
4. For **Add**, type a name for the OpenVPN client and click .



The new OpenVPN client configuration is displayed.



5. The OpenVPN client is enabled by default. To disable, toggle off **Enable**.
6. The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually, click **Use .ovpn file** to disable. If **Use .ovpn file** is disabled, see Configure an OpenVPN client without using an .ovpn file for configuration information.
7. For **Zone**, select the firewall zone for the OpenVPN client.
8. (Optional) Select the **Metric** for the OpenVPN client. If multiple active routes match a destination, the route with the lowest metric will be used.
9. (Optional) For **Username** and **Password**, type the login credentials as configured on the OpenVPN server.
10. For **OVPN file**, paste the content of the client.ovpn file.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> add vpn openvpn client name
(config vpn openvpn client name)>
```

   where *name* is the name of the OpenVPN server.

   The OpenVPN client is enabled by default. To disable the client, type:

```
(config vpn openvpn client name)> enable false
(config vpn openvpn client name)>
```

4. Set the firewall zone for the OpenVPN client:

```
(config vpn openvpn client name)> zone value
(config vpn openvpn client name)>
```

   To view a list of available zones:

```
(config vpn openvpn client name)> zone ?

Zone: The zone for the openvpn client interface.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:

(config vpn openvpn client name)>
```

5. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

```
(config vpn openvpn client name)> metric value
(config vpn openvpn client name)>
```

   where *value* is an interger between **0** and **65535**. The default is **0**.

6. (Optional) Set the login credentials as configured on the OpenVPN server:

```
(config vpn openvpn client name)> username value
(config vpn openvpn client name)> password value
(config vpn openvpn client name)>
```

7. Paste the content of the client.ovpn file into the value of the **config_file** parameter:

```
(config vpn openvpn client name)> config_file value
(config vpn openvpn client name)>
```

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure an OpenVPN client without using an .ovpn file

Required configuration items

- Enable the OpenVPN client.

  The OpenVPN client is enabled by default.
- The mode used by the OpenVPN server, either routing (TUN), or bridging (TAP).
- The firewall zone to be used by the OpenVPN client.
- The IP address of the OpenVPN server.
- Certificates and keys:
  - The **CA certificate** (usually in a ca.crt file).
  - The **Public key** (for example, client.crt)
  - The **Private key** (for example, client.key).

Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.
- Additional OpenVPN parameters.

See Configure SureLink active recovery for OpenVPN for information about OpenVPN active recovery.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

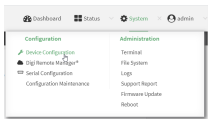
   b. Click the **Device ID**.

   c. Click **Settings**.

   d. Click to expand **Config**.

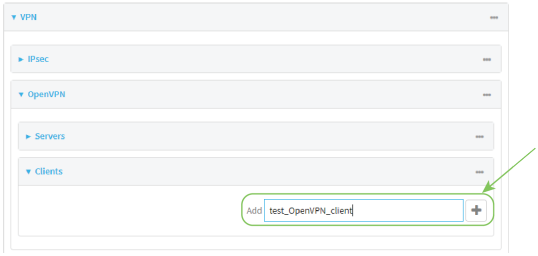
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

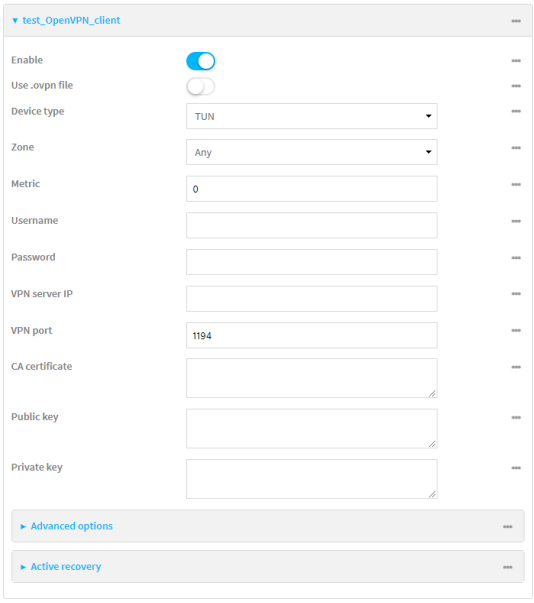
   

   The **Configuration** window is displayed.
3. Click **VPN** > **OpenVPN** > **Clients**.

4. For **Add**, type a name for the OpenVPN client and click ⁄.



The new OpenVPN client configuration is displayed.



5. The OpenVPN client is enabled by default. To disable, toggle off **Enable**.
6. The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually, click **Use .ovpn file** to disable.
7. For **Device type**, select the mode used by the OpenVPN server, either **TUN** or **TAP**.
8. For **Zone**, select the firewall zone for the OpenVPN client.
9. (Optional) Select the **Metric** for the OpenVPN client. If multiple active routes match a destination, the route with the lowest metric will be used.
10. (Optional) For **Username** and **Password**, type the login credentials as configured on the OpenVPN server.
11. For **VPN server IP**, type the IP address of the OpenVPN server.
12. (Optional) Set the **VPN port** used by the OpenVPN server. The default is **1194**.
13. Paste the contents of the **CA certificate** (usually in a ca.crt file), the **Public key** (for example, client.crt), and the **Private key** (for example, client.key) into their respective fields. The contents will be hidden when the configuration is saved.
14. (Optional) Click to expand **Advanced Options** to manually set additional OpenVPN parameters.

a. Click **Enable** to enable the use of additional OpenVPN parameters.
b. Click **Override** if the additional OpenVPN parameters should override default options.
c. For **OpenVPN parameters**, type the additional OpenVPN parameters. For example, to override the configuration by using a configuration file, enter **--config filename**, for example, **--config /etc/config/openvpn_config**.

15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> add vpn openvpn client name
(config vpn openvpn client name)>
```

   where *name* is the name of the OpenVPN server.

   The OpenVPN client is enabled by default. To disable the client, type:

```
(config vpn openvpn client name)> enable false
(config vpn openvpn client name)>
```

4. The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually:

```
(config vpn openvpn client name)> use_file false
(config vpn openvpn client name)>
```

5. Set the mode used by the OpenVPN server:

```
(config vpn openvpn client name)> device_type value
(config vpn openvpn client name)>
```

   where *value* is either **tun** or **tap**. The default is **tun**.

6. Set the firewall zone for the OpenVPN client:

```
(config vpn openvpn client name)> zone value
(config vpn openvpn client name)>
```

   To view a list of available zones:

```
(config vpn openvpn client name)> zone ?

Zone: The zone for the openvpn client interface.
```

```
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:

(config vpn openvpn client name)>
```

7. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

```
(config vpn openvpn client name)> metric value
(config vpn openvpn client name)>
```

   where *value* is an interger between **0** and **65535**. The default is **0**.

8. (Optional) Set the login credentials as configured on the OpenVPN server:

```
(config vpn openvpn client name)> username value
(config vpn openvpn client name)> password value
(config vpn openvpn client name)>
```

9. Set the IP address of the OpenVPN server:

```
(config vpn openvpn client name)> server ip_address
(config vpn openvpn client name)>
```

10. (Optional) Set the port used by the OpenVPN server:

```
(config vpn openvpn client name)> port port
(config vpn openvpn client name)>
```

    The default is **1194**.

11. Paste the contents of the CA certificate (usually in a ca.crt file) into the value of the **cacert** parameter:

```
(config vpn openvpn client name)> cacert value
(config vpn openvpn client name)>
```

12. Paste the contents of the public key (for example, client.crt) into the value of the **public_cert** parameter:

```
(config vpn openvpn client name)> public_cert value
(config vpn openvpn client name)>
```

13. Paste the contents of the private key (for example, client.key) into the value of the **private_key** parameter:

```
(config vpn openvpn client name)> private_key value
(config vpn openvpn client name)>
```

14. (Optional) Set additional OpenVPN parameters.
    a. Enable the use of additional OpenVPN parameters:

    ```
    (config vpn openvpn client name)> advanced_options enable true
    (config vpn openvpn client name)>
    ```

    b. Configure whether the additional OpenVPN parameters should override default options:

    ```
    (config vpn openvpn client name)> advanced_options override true
    (config vpn openvpn client name)>
    ```

    c. Set the additional OpenVPN parameters:

    ```
    (config vpn openvpn client name)> advanced_options extra parameters
    (config vpn openvpn client name)>
    ```

15. Save the configuration and apply the change.

    ```
    (config)> save
    Configuration saved.
    >
    ```

16. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure SureLink active recovery for OpenVPN

You can configure the IX10 device to regularly probe OpenVPN client connections to determine if the connection has failed and take remedial action.

Required configuration items

- A valid OpenVPN client configuration. See Configure an OpenVPN client by using an .ovpn file or Configure an OpenVPN client without using an .ovpn file for configuration instructions.
- Enable OpenVPN SureLink.
- The behavior of the IX10 device upon OpenVPN failure: either
  - Restart the OpenVPN interface
  - Reboot the device.

Additional configuration items

- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.
- The number of probe failures before the OpenVPN connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe failures before considering it to have failed.

To configure the IX10 device to regularly probe the OpenVPN connection:

Web

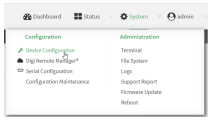
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

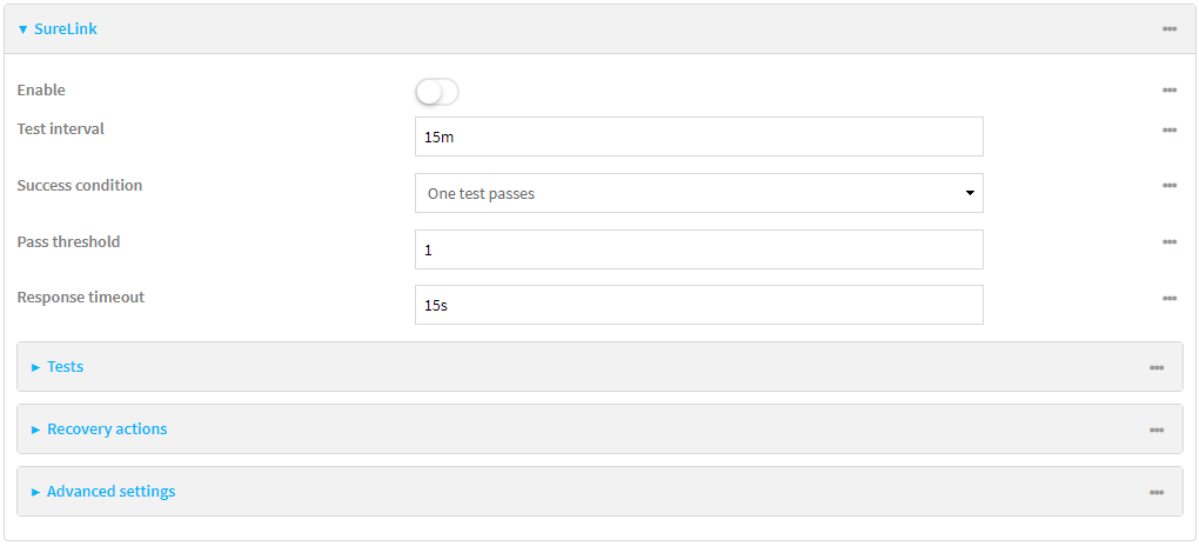
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **OpenVPN** > **Clients**.
4. Create a new OpenVPN client or select an existing one:
   - To create a new OpenVPN client, see Configure an OpenVPN client by using an .ovpn file or Configure an OpenVPN client without using an .ovpn file.
   - To edit an existing OpenVPN client, click to expand the appropriate client.
5. After creating or selecting the OpenVPN client, click **SureLink**.



6. **Enable** SureLink.
7. (Optional) Change the **Test interval** between connectivity tests.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Interval** to ten minutes, enter **10m** or **600s**.

   The default is 15 minutes.
8. (Optional) If more than one test target is configured, for **Success condition**, select either:
   - **One test passes**: Only one test needs to pass for Surelink to consider an interface to be up.
   - **All test pass**: All tests need to pass for SureLink to consider the interface to be up.
9. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
10. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

    The default is 15 seconds.
11. Click to expand **Tests**.

    By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

    a. Click .

    New tests are enabled by default. To disable, click to toggle off **Enable**.

    b. Type a **Label** for the test.

    c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.

    d. Select the **Test type**.

    Available test types:

    - **Ping test**: Uses ICMP to determine connectivity.

      If **Ping test** is selected, complete the following:

      - **Ping target:** The type of target for the ping, one of:
        - **Hostname or IP address** of an external server.
          - **Ping host**: hostname or IP address of the server.
        - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.

    - The **Interface address**.
    - The **Interface DNS** server.
  - **Ping payload size:** The number of bytes to send as part of the ping payload.
- **DNS test**: Performs a DNS query to the named DNS server.

  If **DNS test** is selected, complete the following:
  - **DNS server**: The IP address of the DNS server.
- **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **HTTP test** is selected, complete the following:
  - **Web server**: The URL of the web server.
- **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **Test the interface status** is selected, complete the following:
  - **Down time**: The amount of time that the interface is down before the test can be considered to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Down time** to ten minutes, enter **10m** or **600s**.
  - **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.
- **Custom test**: Tests the interface with custom commands.

  If **Custom test** is selected, complete the following:
  - The **Commands to run to test**.
- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

  If **TCP connection test** is selected, complete the following:
  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.
- **Test another interface's status**: Tests the status of another interface.

  If **Test another interface's status** is selected, complete the following:

- **Test interface**: The interface to test.
- **IP version**: The type of IP connection, one of:
  - **Any**: Either the IPv4 or IPv6 connection must be up.
  - **Both**: Both the IPv4 or IPv6 connection must be up.
  - **IPv4**: The IPv4 connection must be up.
  - **IPv6**: The IPv6 connection must be up.
- **Expected status**: The status required for the test to past.
  - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
  - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

e. Repeat for each additional test.

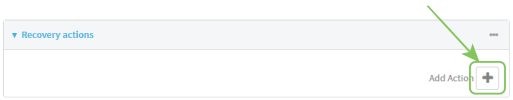
12. Add recovery actions:

a. Click to expand **Recovery actions**.

By default, there are two preconfigured recovery actions:

- **Update routing**: Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
- **Restart interface**.

b. Click ♑



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

c. Type a **Label** for the recovery action.

d. For **Recovery type**, select **Reboot device**.

e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

- **Change default gateway**: Increases the interface's metric to change the default gateway.

  If **Change default gateway** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Increase metric to change active default gateway**: Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Restart interface**.

  If **Restart interface** is selected, complete the following:

- **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
- **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Reset modem**: This recovery action is available for WWAN interfaces only.

  If **Reset modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Switch to alternate SIM**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **Switch to alternate SIM** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Reboot device**.

  If **Reboot device** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- Execute custom **Recovery commands**.

  If **Recovery commands** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
  - The **Commands to run to recovery connectivity**.
  - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Powercycle the modem**. This recovery action is available for WWAN interfaces only.

  If **Powercycle the modem** is selected, complete the following:

  - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.

- **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

f. Repeat for each additional recovery action.

13. (Optional) Configure advanced SureLink parameters:
    a. Click to expand **Advanced settings**.
    b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

    The default is 300 seconds.
    c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

    For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

    The default is 300 seconds.
    d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.
14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new OpenVPN client, or edit an existing one:
   - To create a new OpenVPN client, see Configure an OpenVPN client by using an .ovpn file or Configure an OpenVPN client without using an .ovpn file.
   - To edit an existing OpenVPN client, change to the OpenVPN client's node in the configuration schema. For example, for an OpenVPN client named **openvpn_client1**, change to the **openvpn_client1** node in the configuration schema:

```
(config)> vpn openvpn client openvpn_client1
(config vpn openvpn client openvpn_client1)>
```

4. Enable SureLink:

```
(config vpn openvpn client openvpn_client1)> surelink enable true
(config vpn openvpn client openvpn_client1)>
```

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

   To add additional tests:

   a. Add a test:

```
(config vpn openvpn client openvpn_client1)> add surelink tests end
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

   b. New tests are enabled by default. To disable:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> enable false
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

   c. Create a label for the test:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> label string
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

   d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ipv6 true
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

   e. Set the test type:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> test value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

   where *value* is one of:

   - **ping**: Uses ICMP to determine connectivity.

     If **ping** is selected, complete the following:

     - Set the **ping_method**:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ping_method value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

       where *value* is one of:

       - **hostname**: The hostname or IP address of an external server.
         - Set **ping_host** to the hostname or IP address of the server:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ping_host
hostname/IP_address
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **interface_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
- **interface_address**.
- **interface_dns**: The interface's DNS server.

- Set the number of bytes to send as part of the ping payload:

```
(config vpn openvpn client openvpn_client1 openvpn client openvpn_client1 surelink tests 1)> ping_size int
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **dns**: Performs a DNS query to the named DNS server.

  If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> dns_server IP_address
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

  If **http** is set, set the URL of the web server.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> http url
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **dns_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

  If **interface_up** is set, complete the following:

  - Set the amount of time that the interface is down before the test can be considered to have failed.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> interface_down_time value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number*{w|d|h|m|s}**.

    For example, to set **interface_down_time** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> interface_down_time 600s
(config)>
```

  - Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> interface_timeout
value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> interface_timeout 600s
(config)>
```

- **custom_test**: Tests the interface with custom commands.

  If **custom_test** is set, set the commands to run to perform the test:

```
(config vpn openvpn client openvpn_client1  surelink tests 1)> custom_test_commands
"string"
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **tcp_connection**: Tests that the interface can reach a destination port on the configured host.

  If **tcp_connection** is selected, complete the following:

  - Set the hostname or IP address of the host to create a TCP connection to:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> tcp_host
hostname/IP_address
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

  - Set the TCP port to create a TCP connection to.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> tcp_port port
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **other**: Tests the status of another interface.

  If **other** is selected, complete the following:

  - Set the interface to test.
    i. Use the **?** to determine available interfaces:
    ii. Set the interface. For example:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> other_interface
/network/interface/eth1
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

  - Set the type of IP connection:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> other_ip_version value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

where *value* is one of:

- **any**: Either the IPv4 or IPv6 connection must be up.
- **both**: Both the IPv4 or IPv6 connection must be up.
- **ipv4** The IPv4 connection must be up.
- **ipv6**: The IPv6 connection must be up.

- The status required for the test to past.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> other_status value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

6. Add recovery actions:

a. Type **...** to return to the root of the configuration:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ...
(config)>
```

b. Add a recovery action:

```
(config)> add vpn openvpn client openvpn_client1 surelink actions end
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

c. New actions are enabled by default. To disable:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> enable false
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

d. Create a label for the action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> label string
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

e. Set the type of recovery action to **reboot_device**:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> action reboot_device
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

f. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed. The command varies depending on whether the interface is a WAN or WWAN:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> modem_action value
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- WAN interfaces:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> action value
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- WWAN interfaces:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> modem_action value
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

where *value* is one of:

- **update_routing_table**: Increases the interface's metric to change the default gateway.

  If **update_routing_table** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

    ```
    (config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
    (config vpn openvpn client openvpn_client1 surelink actions 0)>
    ```

    The default is **3**.

  - Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

    ```
    (config vpn openvpn client openvpn_client1 surelink actions 0)> metric_adjustment_
    modem int
    (config vpn openvpn client openvpn_client1 surelink actions 0)>
    ```

    The default is **100**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

    ```
    (config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
    (config vpn openvpn client openvpn_client1 surelink actions 0)>
    ```

- **restart_interface**.

  If **restart_interface** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

  The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- **reset_modem**: This recovery action is available for WWAN interfaces only.

  If **reset_modem** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- **switch_sim**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

  If **switch_sim** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- **modem_power_cycle**: This recovery action is available for WWAN interfaces only.

  If **modem_power_cycle** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- **reboot_device**.

  If **reboot_device** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

    The default is **3**.

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- **custom_action**: Execute custom recovery commands.

  If **custom_action** is selected, complete the following:

  - Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

    The default is **3**.

  - Set the commands to run to attempt to recovery connectivity.

```
(config network interface my_wan surelink actions 0)> custom_action_commands_
modem "string"
(config network interface my_wan surelink actions 0)>
```

  - Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

g. Repeat for each additional recovery action.

7. Optional SureLink configuration parameters:

a. Type **...** to return to the root of the configuration:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> ...
(config)>
```

b. Set the test interval between connectivity tests:

```
(config)> vpn openvpn client openvpn_client1 surelink interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn openvpn client openvpn_client1 surelink interval 600s
(config)>
```

The default is **15m**.

c. If more than one test target is configured, set the success condition:

```
(config)> vpn openvpn client openvpn_client1 surelink success_condition value
(config)>
```

where *value* is either:

- **one**: Only one test needs to pass for Surelink to consider an interface to be up.
- **all**: All tests need to pass for SureLink to consider the interface to be up.

d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

```
(config)> vpn openvpn client openvpn_client1 surelink pass_threshold int
(config)>
```

The default is **1**.

e. Set the amount of time that the device should wait for a response to a test attempt before considering it to have failed:

```
(config)> vpn openvpn client openvpn_client1 surelink timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn openvpn client openvpn_client1 surelink timeout 600s
(config)>
```

The default is **15s**.

f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

```
(config)> vpn openvpn client openvpn_client1 surelink advanced delayed_start value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **delayed_start** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn openvpn client openvpn_client1 surelink advanced delayed_start 600s
(config)>
```

The default is **300s**.

g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

```
(config)> vpn openvpn client openvpn_client1 surelink advanced backoff_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **backoff_interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn openvpn client openvpn_client1 surelink advanced backoff_interval 600s
(config)>
```

The default is 300 seconds.

h. The **interface_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

```
(config)> vpn openvpn client openvpn_client1 surelink advanced interface_gateway
hostname/IP_address
(config)>
```

8. Save the configuration and apply the change.

```
(config vpn openvpn client openvpn_client1 connection_monitor target 0)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See Show SureLink status and statistics for information about showing Surelink status for OpenVPN clients.

Show OpenVPN server status and statistics

You can view status and statistics for OpenVPN servers from either the web interface or the command line:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status** > **OpenVPN** > **Servers**.

   The **OpenVPN Servers** page appears.

2. To view configuration details about an OpenVPN server, click the ✸ (configuration) icon in the upper right of the OpenVPN server's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To display details about all configured OpenVPN servers, type the following at the prompt:

```
> show openvpn server all

Server         Enable  Type  Zone     IP Address      Port
---------------- ------ ---- -------- ---------------- ----
OpenVPN_server1 true   tun   internal 192.168.30.1/24  1194
OpenVPN_server2 false  tun   internal 192.168.40.1/24  1194

>
```

3. To display details about a specific server:

```
> show openvpn server name OpenVPN_server1

Server             : OpenVPN_server1
Enable             : true
Type               : tun
Zone               : internal
IP Address         : 192.168.30.1/24
Port               : 1194
Use File           : true
Metric             : 0
Protocol           : udp
First IP           : 80
Last IP            : 99

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show OpenVPN client status and statistics

You can view status and statistics for OpenVPN clients from either web interface or the command line:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status** > **OpenVPN** > **Clients**.

   The **OpenVPN Clients** page appears.

2. To view configuration details about an OpenVPN client, click the ✷ (configuration) icon in the upper right of the OpenVPN client's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To display details about all configured OpenVPN clients, type the following at the prompt:

```
> show openvpn client all

Client         Enable  Status    Username  Use File  Zone
-------------- ------ -------   --------- -------- --------
OpenVPN_Client1 true   connected         true     internal
OpenVPN_Client2 true   pending           true     internal

>
```

3. To display details about a specific client:

```
> show openvpn client name OpenVPN_client1

Client          : OpenVPN_client1
Enable           : true
Status          : up
Username            : user1
IP address         : 123.122.121.120
Remote           : 120.121.122.123
MTU             : 1492
Zone            : internal
IP Address          : 192.168.30.1/24
Port            : 1194
Use File         : true
Metric          : 0
Protocol         : udp
Port            : 1194
Type            : tun

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is an IP packet encapsulation protocol that allow for networks and routes to be advertized from one network device to another. You can use GRE to encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an IP network.

Configuring a GRE tunnel

Configuring a GRE tunnel involves the following items:

Required configuration items

- A GRE loopback endpoint interface.
- GRE tunnel configuration:
  - Enable the GRE tunnel.

    The GRE tunnels are enabled by default.
  - The local endpoint interface.
  - The IP address of the remote device/peer.

Additional configuration items

- A GRE key.
- Enable the device to respond to keepalive packets.

Task One: Create a GRE loopback endpoint interface

Web

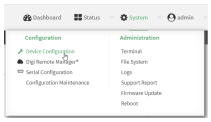
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. For **Add Interface**, type a name for the GRE loopback endpoint interface and click .
5. **Enable** the interface.

   New interfaces are enabled by default. To disable, toggle off **Enable**.
6. For **Interface type**, select **Ethernet**.
7. For **Zone**, select **Internal**.
8. For **Device**, select **Ethernet: Loopback**.
9. Click to expand **IPv4**.
10. For **Address**, enter the IP address and subnet mask of the local GRE endpoint, for example **10.10.1.1/24**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the GRE endpoint interface. For example, to add an interface named **gre_endpoint**:

```
(config)> add network interface gre_interface
(config network interface gre_interface)>
```

4. Set the interface zone to **internal**:

```
(config network interface gre_interface)> zone internal
(config network interface gre_interface)>
```

5. Set the interface device to **loopback**:

```
(config network interface gre_interface)> device /network/device/loopback
(config network interface gre_interface)>
```

6. Set the IP address and subnet mask of the local GRE endpoint. For example, to set the local GRE endpoint's IP address and subnet mask to **10.10.1.1/24:**

```
(config network interface gre_interface)> ipv4 address 10.10.1.1/24
(config network interface gre_interface)>
```

7. Save the configuration and apply the change.

```
(config network interface gre_interface)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Task Two: Configure the GRE tunnel

Web

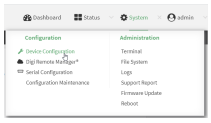
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **IP Tunnels**.
4. For **Add IP tunnel**, type a name for the GRE tunnel and click .
5. **Enable** the tunnel.

   New tunnels are enabled by default. To disable, toggle off **Enable**.
6. For **Mode**, select one of the following options:
   - **GRE**: Standard GRE point-to-point protocol.
   - **mGRE**: multipoint GRE protocol.
   - **GRETAP**: Ethernet over GRE.
7. For **Local endpoint**, select the GRE endpoint interface created in Task One.

8. If **GRE** is selected for the **Mode**, for **Remote endpoint**, type the IP address of the GRE endpoint on the remote peer.
9. If **GRETAP** is selected for **Mode**, for **Local endpoint**, select the interface.
10. (Optional) For **Key**, enter a key that will be inserted in GRE packets created by this tunnel. It must match the key set by the remote endpoint. Allowed value is an integer between 0 and 4294967295, or an IP address.
11. (Optional) **Enable keepalive reply** to enable the device to reply to Cisco GRE keepalive packets.
12. (Optional) **Enable open routing** to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel.
13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the GRE endpoint tunnel. For example, to add a tunnel named **gre_example**:

```
(config)> add vpn iptunnel gre_example
(config vpn iptunnel gre_example)>
```

   GRE tunnels are enabled by default. To disable:

```
(config vpn iptunnel gre_example)> enable false
(config vpn iptunnel gre_example)>
```

4. Set the mode:

```
(config vpn iptunnel gre_example)> type value
(config vpn iptunnel gre_example)>
```

   where *value* is either:

   - **gre**: Standard GRE point-to-point protocol.
   - **mgre**: multipoint GRE protocol.
   - **GRETAP**: Ethernet over GRE
5. Set the local endpoint to the GRE endpoint interface created in Task One, for example:

```
(config vpn iptunnel gre_example)> local /network/interface/gre_endpoint
(config vpn iptunnel gre_example)>
```

6. If **type** is set to **gre**, set the IP address of the GRE endpoint on the remote peer:

```
(config vpn iptunnel gre_example)> remote ip_address
(config vpn iptunnel gre_example)>
```

7. (Optional) Set a key that will be inserted in GRE packets created by this tunnel.

   The key must match the key set by the remote endpoint.

```
(config vpn iptunnel gre_example)> key value
(config vpn iptunnel gre_example)>
```

   where value is an integer between 0 and 4294967295, or an IP address.

8. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

```
(config vpn iptunnel gre_example)> keepalive true
(config vpn iptunnel gre_example)>
```

9. (Optional) Enable the device to allow packets destined for an address which is not explicitly in the routing table to exit the IP tunnel:

```
(config vpn iptunnel gre_example)> open_routing true
(config vpn iptunnel gre_example)>
```

10. Save the configuration and apply the change.

```
(config vpn iptunnel gre_example)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show GRE tunnels

To view information about currently configured GRE tunnels:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **Status** > **IP tunnels**.

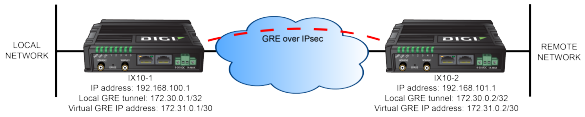
   The **IP Tunnels** page appears.

2. To view configuration details about a GRE tunnel, click the ✷ (configuration) icon in the upper right of the tunnel's status pane.

Example: GRE tunnel over an IPSec tunnel

The IX10 device can be configured as an advertised set of routes through an IPSec tunnel. This allows you to leverage the dynamic route advertisement of GRE tunnels through a secured IPSec tunnel.

The example configuration provides instructions for configuring the IX10 device with a GRE tunnel through IPsec.



IX10-1 configuration tasks

1. Create an IPsec tunnel named **ipsec_gre1** with:
   - A pre-shared key.
   - **Remote endpoint** set to the public IP address of the IX10-2 device.
   - A policy with:
     - **Local network** set to the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**.
     - **Remote network** set to the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**.
2. Create an IPsec endpoint interface named **ipsec_endpoint1**:
   a. **Zone** set to **Internal**.
   b. **Device** set to **Ethernet: Loopback**.
   c. IPv4 Address set to the IP address of the local GRE tunnel, **172.30.0.1/32**.
3. Create a GRE tunnel named **gre_tunnel1**:
   a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec_endpoint1**.
   b. Remote endpoint set to the IP address of the GRE tunnel on IX10-2, **172.30.0.2**.
4. Create an interface named **gre_interface1** and add it to the GRE tunnel:
   a. **Zone** set to **Internal**.
   b. **Device** set to **IP tunnel: gre_tunnel1**.
   c. IPv4 Address set to a virtual IP address on the GRE tunnel, **172.31.0.1/30**.

IX10-2 configuration tasks

1. Create an IPsec tunnel named **ipsec_gre2** with:
   - The same pre-shared key as the **ipsec_gre1** tunnel on IX10-1.
   - **Remote endpoint** set to the public IP address of IX10-1.
   - A policy with:
     - **Local network** set to the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**.
     - **Remote network** set to the IP address of the remote GRE tunnel, **172.30.0.1/32**.

2. Create an IPsec endpoint interface named **ipsec_endpoint2**:
   a. **Zone** set to **Internal**.
   b. **Device** set to **Ethernet: Loopback**.
   c. IPv4 Address set to the IP address of the local GRE tunnel, **172.30.0.2/32**.
3. Create a GRE tunnel named **gre_tunnel2**:
   a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec_endpoint2**.
   b. Remote endpoint set to the IP address of the GRE tunnel on IX10-1, **172.30.0.1**.
4. Create an interface named **gre_interface2** and add it to the GRE tunnel:
   a. **Zone** set to **Internal**.
   b. **Device** set to **IP tunnel: gre_tunnel2**.
   c. IPv4 Address set to a virtual IP address on the GRE tunnel, **172.31.0.2/30**.

Configuration procedures

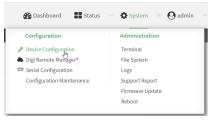
Configure the IX10-1 device
Task one: Create an IPsec tunnel

Web

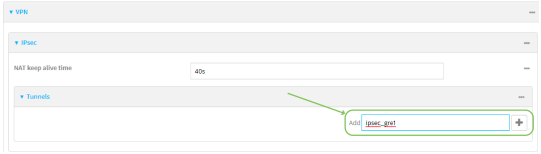
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

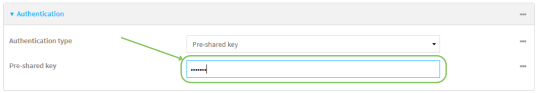
   Local Web UI:
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

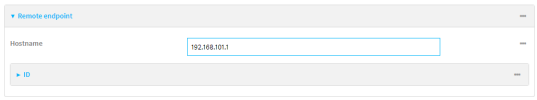
   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec** > **Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec_gre1** and click .



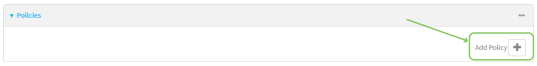
5. Click to expand **Authentication**.
6. For **Pre-shared key**, type **testkey**.



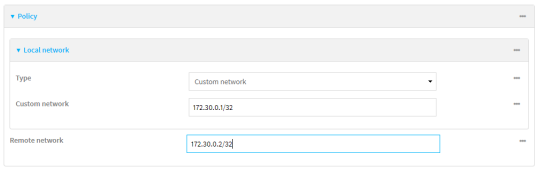
7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the IX10-2 device.



9. Click to expand **Policies**.
10. For **Add Policy**, click to add a new policy.



11. Click to expand **Local network**.
12. For **Type**, select **Custom network**.
13. For **Address**, type the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**.
14. For **Remote network**, type the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**.



15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add an IPsec tunnel named **ipsec_gre1**:

```
(config)> add vpn ipsec tunnel ipsec_gre1
(config vpn ipsec tunnel ipsec_gre1)>
```

4. Set the pre-shared key to **testkey**:

```
(config vpn ipsec tunnel ipsec_gre1)> auth secret testkey
(config vpn ipsec tunnel ipsec_gre1)>
```

5. Set the remote endpoint to public IP address of the IX10-2 device:

```
(config vpn ipsec tunnel ipsec_gre1)> remote hostname 192.168.101.1
(config vpn ipsec tunnel ipsec_gre1)>
```

6. Add a policy:

```
(config vpn ipsec tunnel ipsec_gre1)> add policy end
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

7. Set the local network policy type to **custom**:

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> local type custom
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

8. Set the local network address to the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**:

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> local custom 172.30.0.1/32
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

9. Set the remote network address to the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**:

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> remote network 172.30.0.2/32
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

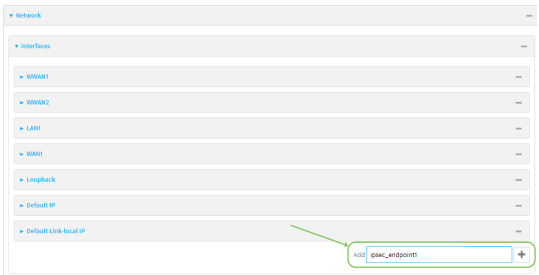
10. Save the configuration and apply the change.

```
(config ipsec tunnel ipsec_gre1 policy 0)> save
Configuration saved.
>
```

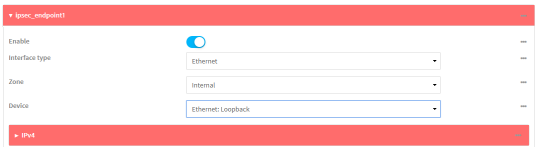
Task two: Create an IPsec endpoint interface

Web

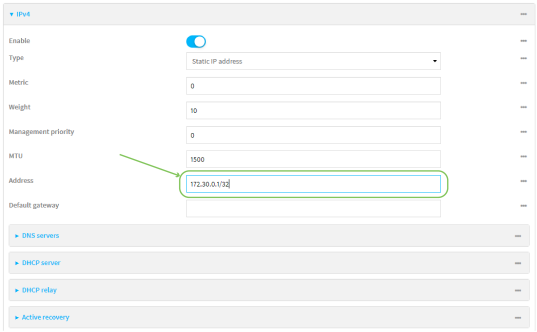
1. Click **Network** > **Interface**.
2. For **Add Interface**, type **ipsec_endpoint1** and click ⅋



3. For **Zone**, select **Internal**.
4. For **Device**, select **Ethernet: loopback**.



5. Click to expand **IPv4**.
6. For **Address**, type the IP address of the local GRE tunnel, **172.30.0.1/32**.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **ipsec_endpoint1**:

```
(config)> add network interface ipsec_endpoint1
(config network interface ipsec_endpoint1)>
```

3. Set the zone to **internal**:

```
(config network interface ipsec_endpoint1)> zone internal
(config network interface ipsec_endpoint1)>
```

4. Set the device to **/network/device/loopback**:

```
(config network interface ipsec_endpoint1)> device /network/device/loopback
(config network interface ipsec_endpoint1)>
```

5. Set the IPv4 address to the IP address of the local GRE tunnel, **172.30.0.1/32**:

```
(config network interface ipsec_endpoint1)> ipv4 address 172.30.0.1/32
(config network interface ipsec_endpoint1)>
```

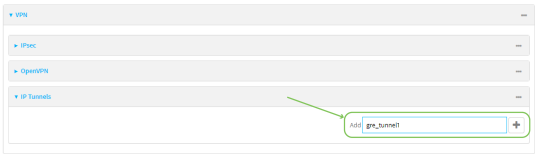
6. Save the configuration and apply the change.

```
(config vpn ipsec tunnel ipsec_endpoint1 policy 0)> save
Configuration saved.
>
```

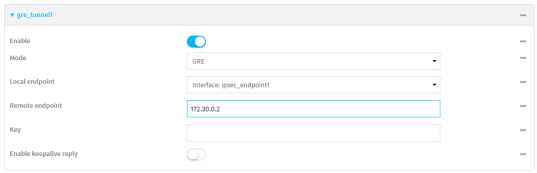
Task three: Create a GRE tunnel

Web

1. Click **VPN** > **IP Tunnels**.
2. For **Add IP Tunnel**, type **gre_tunnel1** and click ⨁.



3. For **Local endpoint**, select the IPsec endpoint interface created in Task two (**Interface: ipsec_endpoint1**).
4. For **Remote endpoint**, type the IP address of the GRE tunnel on IX10-2, **172.30.0.2**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add a GRE tunnel named **gre_tunnel1**:

```
(config)> add vpn iptunnel gre_tunnel1
(config vpn iptunnel gre_tunnel1)>
```

3. Set the local endpoint to the IPsec endpoint interface created in Task two (**/network/interface/ipsec_endpoint1**):

```
(config vpn iptunnel gre_tunnel1)> local /network/interface/ipsec_endpoint1
(config vpn iptunnel gre_tunnel1)>
```

4. Set the remote endpoint to the IP address of the GRE tunnel on IX10-2, **172.30.0.2**:

```
(config vpn iptunnel gre_tunnel1)> remote 172.30.0.2
(config vpn iptunnel gre_tunnel1)>
```

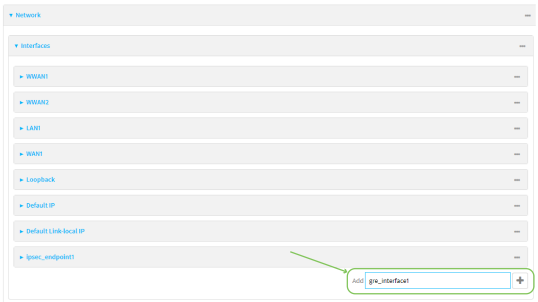
5. Save the configuration and apply the change.

```
(config vpn iptunnel gre_tunnel1)> save
Configuration saved.
>
```

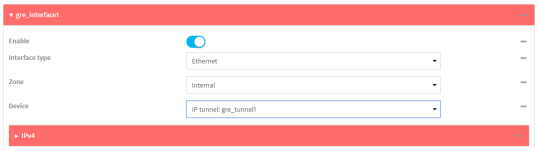
Task four: Create an interface for the GRE tunnel device

Web

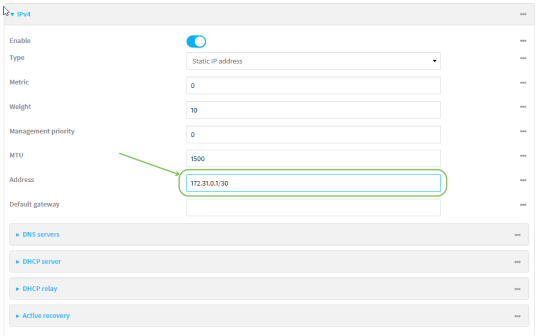
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **gre_interface1** and click .



3. For **Zone**, select **Internal**.
4. For **Device**, select the GRE tunnel created in Task three (**IP tunnel: gre_tunnel1**).



5. Click to expand **IPv4**.
6. For **Address**, type **172.31.0.1/30** for a virtual IP address on the GRE tunnel.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **gre_interface1**:

```
(config)> add network interface gre_interface1
(config network interface gre_interface1)>
```

3. Set the zone to **internal**:

```
(config network interface gre_interface1)> zone internal
(config network interface gre_interface1)>
```

4. Set the device to the GRE tunnel created in Task three (**/vpn/iptunnel/gre_tunnel1**):

```
(config network interface gre_interface1)> device /vpn/iptunnel/gre_tunnel1
(config network interface gre_interface1)>
```

5. Set **172.31.0.1/30** as the virtual IP address on the GRE tunnel:

```
(config network interface gre_interface1)> ipv4 address 172.31.0.1/30
(config network interface gre_interface1)>
```

6. Save the configuration and apply the change.

```
(config network interface gre_interface1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the IX10-2 device
Task one: Create an IPsec tunnel

Web

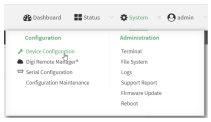
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

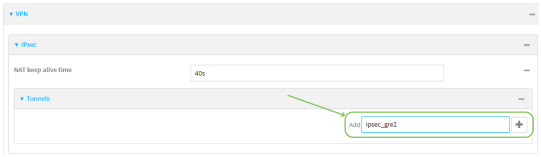
   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

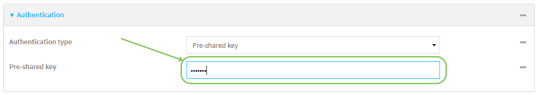


The **Configuration** window is displayed.

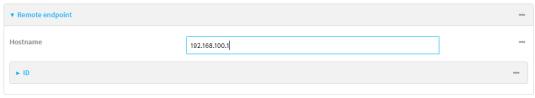
3. Click **VPN** > **IPsec** > **Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec_gre2** and click .



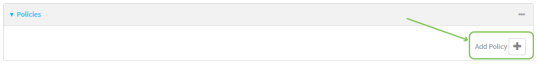
5. Click to expand **Authentication**.
6. For **Pre-shared key**, type the same pre-shared key that was configured for the IX10-1 (**testkey**).



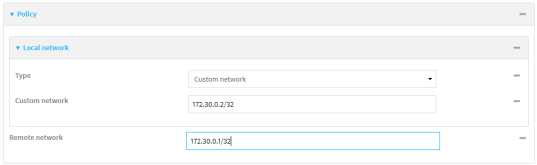
7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the IX10-1 device.



9. Click to expand **Policies**.
10. For **Add Policy**, click to add a new policy.



11. Click to expand **Local network**.
12. For **Type**, select **Custom network**.
13. For **Address**, type the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**.
14. For **Remote network**, type the IP address and subnet of the remote GRE tunnel, **172.30.0.1/32**.



15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add an IPsec tunnel named **ipsec_gre2**:

```
(config)> add vpn ipsec tunnel ipsec_gre2
(config vpn ipsec tunnel ipsec_gre2)>
```

4. Set the pre-shared key to the same pre-shared key that was configured for the IX10-1 (**testkey**):

```
(config vpn ipsec tunnel ipsec_gre2)> auth secret testkey
(config vpn ipsec tunnel ipsec_gre2)>
```

5. Set the remote endpoint to public IP address of the IX10-1 device:

```
(config vpn ipsec tunnel ipsec_gre2)> remote hostname 192.168.100.1
(config vpn ipsec tunnel ipsec_gre2)>
```

6. Add a policy:

```
(config vpn ipsec tunnel ipsec_gre2)> add policy end
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

7. Set the local network policy type to **custom**:

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> local type custom
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

8. Set the local network address to the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**:

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> local custom 172.30.0.2/32
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

9. Set the remote network address to the IP address and subnet of the remote GRE tunnel, **172.30.0.1/32**:

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> remote network 172.30.0.1/32
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

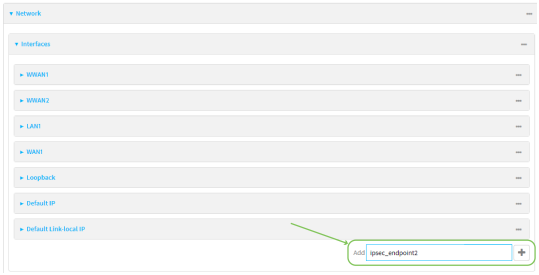
10. Save the configuration and apply the change.

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> save
Configuration saved.
>
```

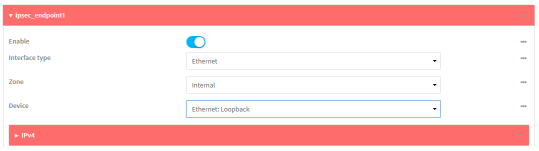
Task two: Create an IPsec endpoint interface

Web

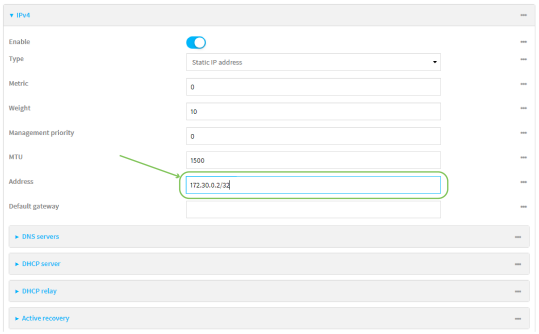
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **ipsec_endpoint2** and click .



3. For **Zone**, select **Internal**.
4. For **Device**, select **Ethernet: loopback**.



5. Click to expand **IPv4**.
6. For **Address**, type the IP address of the local GRE tunnel, **172.30.0.2/32**.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **ipsec_endpoint2**:

```
(config)> add network interface ipsec_endpoint2
(config network interface ipsec_endpoint2)>
```

3. Set the zone to **internal**:

```
(config network interface ipsec_endpoint2)> zone internal
(config network interface ipsec_endpoint2)>
```

4. Set the device to **/network/device/loopback**:

```
(config network interface ipsec_endpoint2)> device /network/device/loopback
(config network interface ipsec_endpoint2)>
```

5. Set the IPv4 address to the IP address of the local GRE tunnel, **172.30.0.2/32**:

```
(config network interface ipsec_endpoint2)> ipv4 address 172.30.0.2/32
(config network interface ipsec_endpoint2)>
```

6. Save the configuration and apply the change.

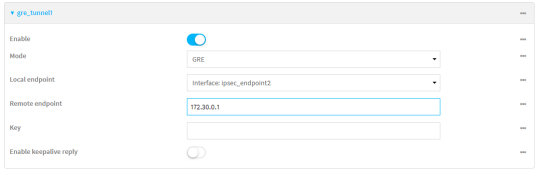
```
(config vpn ipsec tunnel ipsec_endpoint2)> save
Configuration saved.
>
```

Task three: Create a GRE tunnel

Web

1. Click **VPN** > **IP Tunnels**.
2. For **Add IP Tunnel**, type **gre_tunnel2** and click ⨁.

3. For **Local endpoint**, select the IPsec endpoint interface created in Task two (**Interface: ipsec_endpoint2**).
4. For **Remote endpoint**, type the IP address of the GRE tunnel on IX10-1, **172.30.0.1**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add a GRE tunnel named **gre_tunnel2**:

```
(config)> add vpn iptunnel gre_tunnel2
(config vpn iptunnel gre_tunnel2)>
```

3. Set the local endpoint to the IPsec endpoint interface created in Task two (**/network/interface/ipsec_endpoint2**):

```
(config vpn iptunnel gre_tunnel2)> local /network/interface/ipsec_endpoint2
(config vpn iptunnel gre_tunnel2)>
```

4. Set the remote endpoint to the IP address of the GRE tunnel on IX10-1, **172.30.0.1**:

```
(config vpn iptunnel gre_tunnel2)> remote 172.30.0.1
(config vpn iptunnel gre_tunnel2)>
```

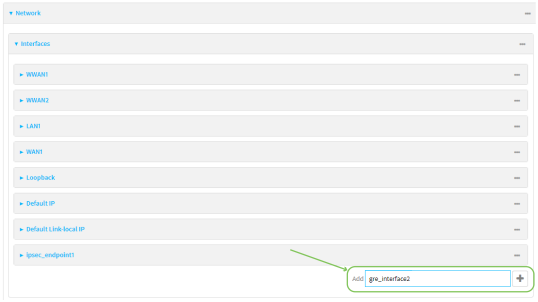
5. Save the configuration and apply the change.

```
(config vpn iptunnel gre_tunnel2)> save
Configuration saved.
>
```

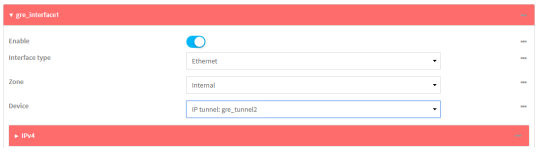
Task four: Create an interface for the GRE tunnel device

Web

1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **gre_interface2** and click .

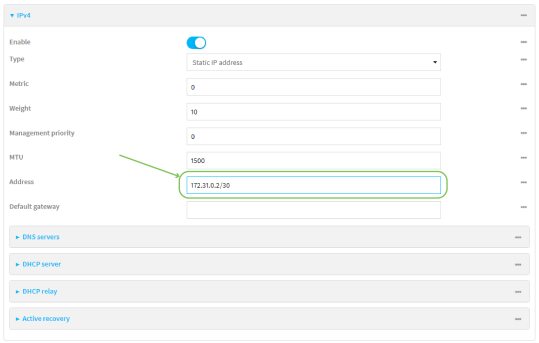


3. For **Zone**, select **Internal**.
4. For **Device**, select the GRE tunnel created in Task three (**IP tunnel: gre_tunnel2**).



5. Click to expand **IPv4**.

6. For **Address**, type **172.31.0.2/30** for a virtual IP address on the GRE tunnel.



7. Click **Apply** to save the configuration and apply the change.

Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **gre_interface2**:

```
(config)> add network interface gre_interface2
(config network interface gre_interface2)>
```

3. Set the zone to **internal**:

```
(config network interface gre_interface2)> zone internal
(config network interface gre_interface2)>
```

4. Set the device to the GRE tunnel created in Task three (**/vpn/iptunnel/gre_tunnel2**):

```
(config network interface gre_interface2)> device /vpn/iptunnel/gre_tunnel2
(config network interface gre_interface2)>
```

5. Set **172.31.0.2/30** as the virtual IP address on the GRE tunnel:

```
(config network interface gre_interface2)> ipv4 address 172.31.0.2/30
(config network interface gre_interface2)>
```

6. Save the configuration and apply the change.

```
(config network interface gre_interface2)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Dynamic Multipoint VPN (DMVPN)

Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of a virtual private network (VPN), using a multi spoke-to-hub network in which the network addresses of the spoke routers do not need to be known, and therefore do not need to be configured in the hub router.

One advantage to this form of VPN is a scalable network in which the size of the hub configuration is minimized. When one spoke of the network needs to send traffic to another spoke, a direct transfer is possible without having to add any load onto the hub. This is achieved by the creation of a dynamic GRE tunnel directly to the other spoke. The network address of the target spoke is resolved with the use of Next Hop Resolution Protocol (NHRP).

This section contains the following topics:

Configure a DMVPN spoke 460

Configure a DMVPN spoke

To configure a DMVPN spoke:

Web

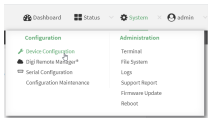
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

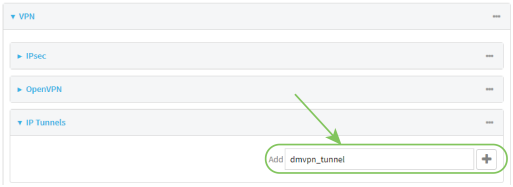
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

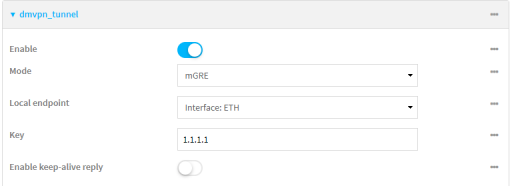
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Create an IP tunnel.
   a. Click **VPN** > **IP Tunnels**.
   b. In **Add IP tunnel**, type the name of the tunnel and click .

   c. For **Mode**, select **mGRE**.
   d. For **Local endpoint**, select the interface that will serve as the local endpoint of the tunnel.
   e. For **Key**, type a four-octet value that matches the key on the remote endpoint.

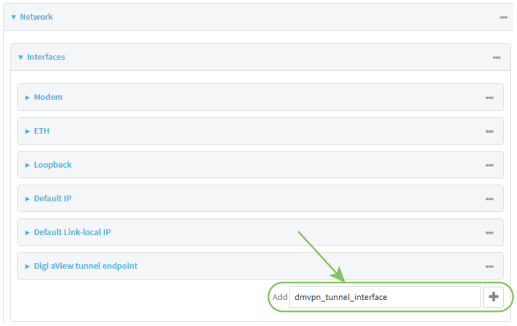
f. (Optional) **Enable keep-alive reply** to enable the device to reply to Cisco GRE keep-alive packets.

g. (Optional) **Enable open routing** to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel.

4. Assign an IP address to the IP tunnel:

a. Click **Network** > **Interfaces**.

b. For **Add Interface**, type a name for the interface and click .

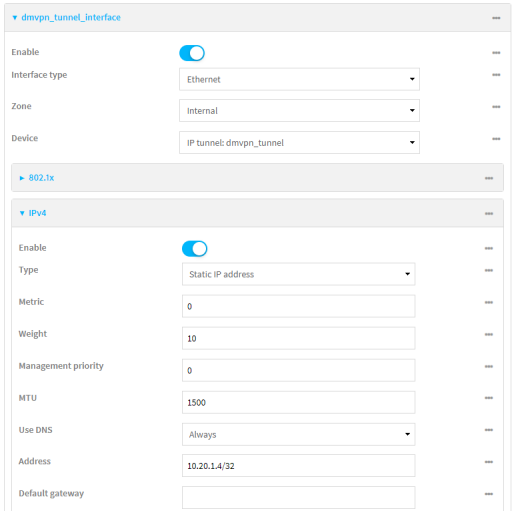


c. For **Zone**, select **Internal**.

d. For **Device**, select the IP tunnel created above.

e. Click to expand **IPv4**.

f. For **Address**, type the IP address and netmask of the tunnel. The netmask must be set to **/32**.



5. Configure **NHRP**:

a. Click **Network** > **Routing Services**.

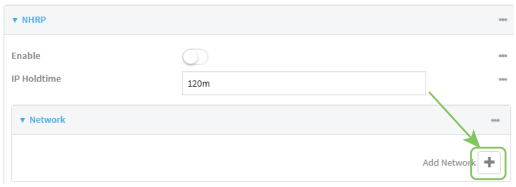
b. **Enable** routing services.

c. Click to expand **NHRP**.

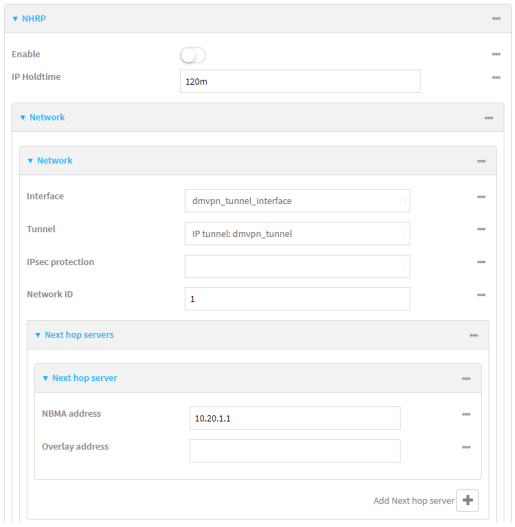
d. **Enable** NHRP.

e. Click to expand Network.

f. Click to add a network.



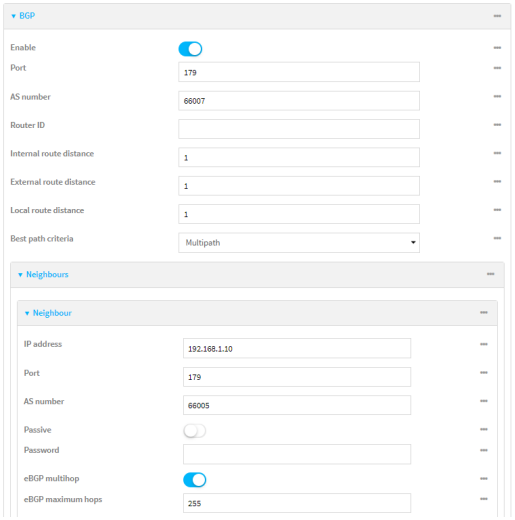
g. For **Interface**, select the interface created above.
h. For **Tunnel**, select the IP tunnel created above.
i. Click to expand **Next hop servers**.
j. Click to add a server.
k. For **NBMA address**, type the hostname or IP address of the node that will be the next hop server.



6. To enable redirection of packets between spokes, configure OSPF routing:
   a. Click **Network** > **Routes** > **Routing services** > **OSPF**.
   b. **Enable** OSPF.
   c. For **ABR behavior**, choose the Area Border Router for the network.
   d. For **Reference bandwidth**, type the link bandwidth.
   e. **Enable** the Opaque-LSA standard.
   f. **Enable** the RFC1583 standard.
7. Configure the overlay connection:
   a. Click **Network** > **Routing services** > **BGP**.
   b. **Enable** BGP.
   c. For **AS number**, type the autonomous system number for this device.
   d. For **Best path criteria**, select **Multipath**.
   e. Click to expand **Neighbours**.
   f. Click to add a neighbour.

g. For **IP address**, type the IP address of the hub.

h. Click to toggle on **eBGP multihop**.



8. Repeat to add additional spokes.
9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create an IP tunnel.

   a. Add an IP tunnel. For example, to add a tunnel named **dmvpn_tunnel**:

```
(config)> add vpn iptunnel dmvpn_tunnel
(config vpn iptunnel dmvpn_tunnel)>
```

   b. Set the type to multipoint:

```
(config vpn iptunnel dmvpn_tunnel)> type multipoint
(config vpn iptunnel dmvpn_tunnel)>
```

   c. Set the local interface:

      i. Use the **?** to determine available interfaces:

      ii. Set the interface. For example:

```
(config vpn iptunnel dmvpn_tunnel)> local /network/interface/eth1
(config vpn iptunnel dmvpn_tunnel)>
```

d. Set the key to a four-octet value that matches the key on the remote endpoint. For example:

```
(config vpn iptunnel dmvpn_tunnel)> key 1.1.1.1
(config vpn iptunnel dmvpn_tunnel)>
```

e. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

```
(config vpn iptunnel dmvpn_tunnel)> keepalive true
(config vpn iptunnel dmvpn_tunnel)>
```

f. (Optional) Enable the device to allow packets destined for an address which is not explicitly in the routing table to exit the IP tunnel:

```
(config vpn iptunnel dmvpn_tunnel)> open_routing true
(config vpn iptunnel dmvpn_tunnel)>
```

4. Assign an IP address to the IP tunnel:
   a. Type **...** to return to the top level of the configuration schema:

```
(config vpn iptunnel dmvpn_tunnel)> ...
(config)>
```

   b. And a network interface. For example, to add an interface named dmvpn_tunnel_ interface:

```
(config)> add network interface dmvpn_tunnel_interface
(config network interface dmvpn_tunnel_interface)>
```

   c. Set the zone to **internal**:

```
(config network interface dmvpn_tunnel_interface)> zone internal
(config network interface dmvpn_tunnel_interface)>
```

   d. Set the device to the IP tunnel created above:

```
(config network interface dmvpn_tunnel_interface)> device /vpn/iptunnel/dmvpn_tunnel
(config network interface dmvpn_tunnel_interface)>
```

   e. Set the IP address and netmask of the tunnel. The netmask must be set to **/32**. For example, to set the IP address to **10.20.1.4/32**:

```
(config network interface dmvpn_tunnel_interface)> ipv4 address 10.20.1.4/32
(config network interface dmvpn_tunnel_interface)>
```

5. Configure NHRP:
   a. Type **...** to return to the top level of the configuration schema:

```
(config network interface dmvpn_tunnel_interface)> ...
(config)>
```

b. Enable routing services:

```
(config)> network route service enable true
(config)>
```

c. Enable NHRP:

```
(config)> network route service nhrp enable true
(config)>
```

d. Add an NHRP network:

```
(config)> add network route service nhrp network end
(config network route service nhrp network 0)>
```

e. Set the interface to the interface that was created above:

```
(config network route service nhrp network 0)> interface dmvpn_tunnel_interface
(config network route service nhrp network 0)>
```

f. Set the tunnel to the IP tunnel created above:

```
(config network route service nhrp network 0)> tunnel /vpn/iptunnel/dmvpn_tunnel
(config network route service nhrp network 0)>
```

g. Add a net hop server:

```
(config network route service nhrp network 0)> add nhs end
(config network route service nhrp network 0 nhs 0)>-
```

6. Set the hostname or IP address of the node that will be the next hop server:

```
(config network route service nhrp network 0 nhs 0)> nbma hostname/IP_address
(config network route service nhrp network 0 nhs 0)>
```

7. Configure OSPF routing:

```
(config network route service ospf)
(config)>
```

8. Configure the overlay connection using BGP:
   a. Type **...** to return to the top level of the configuration schema:

```
(config network interface dmvpn_tunnel_interface)> ...
(config)>
```

   b. Enable BGP:

```
(config)> network route service bgp enable true
(config)>
```

   c. Set the autonomous system number for this device. For example, to set the autonomous system number to 66007:

```
(config)> network route service bgp asn 66007
(config)>
```

d. Set the best path criteria to multipath:

```
(config)> network route service bgp as_path multipath-relax
(config)>
```

e. Add a neighbour:

```
(config)> add network route service bgp neighbour end
(config network route service bgp neighbour 0)>
```

f. Set **ip** to the IP address of the hub. For example:

```
(config network route service bgp neighbour 0)> ip 10.20.1.1
(config network route service bgp neighbour 0)>
```

g. Enable eBGP multihop:

```
(config network route service bgp neighbour 0)> ebgp_multihop true
(config network route service bgp neighbour 0)>
```

9. Repeat to add additional spokes.
10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

L2TP

Your IX10 device supports PPP-over-L2TP (Layer 2 Tunneling Protocol).

Configure a PPP-over-L2TP tunnel

Your IX10 device supports PPP-over-L2TP (Layer 2 Tunneling Protocol). The tunnel endpoints are known as L2TP Access Concentrators (LAC) and L2TP Network Servers (LNS). Each endpoint terminates the PPP session.

Required configuration items

- For L2TP access concentrators:
  - The hostname or IP address of the L2TP network server.
  - The firewall zone for the tunnel.

- For L2TP network servers:
  - The IP address of the L2TP access concentrator.
  - The local IP address assigned to the L2TP virtual network interface.
  - The IP address assigned to the remote peer.
  - The firewall zone for the tunnel.

Additional configuration items

- The UDP port that L2TP servers will listen on, if other than the deafult of **1701**.
- Access control for the L2TP tunnel.
- For L2TP access concentrators:
  - L2TP network server port.
  - The username and password of the L2TP server.
  - The metric for the tunnel.
  - Enable custom PPP configuration options for the tunnel.
    - Whether to override the default configuration and only use the custom options.
    - Optional configuration data in the format of a pppd options file.
- For L2TP network servers:
  - The Authentication method.
  - The metric for the tunnel.
  - Enable custom PPP configuration options for the tunnel.
    - Whether to override the default configuration and only use the custom options.
    - Optional configuration data in the format of a pppd options file.

Web

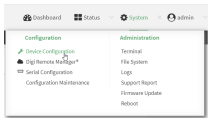
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN** > **L2TP**.
4. (Optional) Type the **UDP listening port** that L2TP servers will listen on, if other than the default of **1701**.
5. Set the access control for L2TP tunnels:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the service-type.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the service-type.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.
        See Firewall configuration for information about firewall zones.
     d. Click again to allow access through additional firewall zones.
6. To add an L2TP access concentrator:
   a. Click to expand **L2TP access concentrators**.
   b. For **Add L2TP access concentrator**, type a name for the LAC and click .
   c. LACs are enabled by default. To disable, toggle off **Enable**.
   d. For **L2TP network server**, type the hostname or IP address of the L2TP network server.

e. (Optional) Type the **L2TP network server port** to use to connect to the server, if other than the default of **1701**.
f. (Optional) Type the **Username** to use to log into the server.
g. (Optional) Type the **Password** to use to log into the server.
h. (Optional) Type the **Metric** for the tunnel, if other than the default of **1**.
i. Select a firewall **Zone** for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.
j. (Optional): Custom PPP configuration:
    i. **Enable** custom PPP configuration.
    ii. Enable **Override** if the custom configuration should override the default configuration and only use the custom options.
    iii. For **Configuration file**, paste or type the configuration data in the format of a pppd options file.

7. To add an L2TP network server:
    a. Click to expand **L2TP network servers**.
    b. For **Add L2TP network server**, type a name for the LNS and click .
    c. LNSs are enabled by default. To disable, toggle off **Enable**.
    d. For **L2TP access concentrator**, type the IP addressof the L2TP access concentrator that this server will allow connections from. This can also be:
        - A range of IP addresses, using the format x.x.x.x-y.y.y.y, for example **192.168.188.1-192.168.188.254**.
        - The keyword **any**, which means that the server will accept connections from any IP address.
    e. For **Local IP address**, type the IP address of the L2TP virtual network interface.
    f. For **Remote IP address**, type the IP address to assign to the remote peer.
    g. (Optional) For **Authentication method**, select one of the following:
        - **None**: No authentication is required.
        - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
        - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
        - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

        If **Automatic**, **CHAP**, or **PAP** is selected, enter the **Username** and **Password** required to authenticate.

        The default is **None**.
    h. (Optional) For **Authentication method**, select the authentication method, one of:
        - **None**: No authentication is required.
        - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
        - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
        - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

- **MS-CHAPv2**: Uses the Microsoft version of the Challenge Handshake Authentication Profile (CHAP) to authenticate.
- If **Automatic**, **CHAP**, **PAP**, or **MS-CHAPv2** is selected, enter the **Username** and **Password** required to authenticate.
- The default is **None**.

i. (Optional) Type the **Metric** for the tunnel, if other than the default of **1**.

j. Select a firewall **Zone** for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.

k. (Optional): Custom PPP configuration:

i. **Enable** custom PPP configuration.

ii. Enable **Override** if the custom configuration should override the default configuration and only use the custom options.

iii. For **Configuration file**, paste or type the configuration data in the format of a pppd options file.

8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Set the UDP listening port that L2TP servers will listen on:

```
(config)> vpn l2tp port value
(config)>
```

   where *value* is an integer between **1** and **65535**. The default is **1701**.

4. Set the access control for L2TP tunnels:

   - To limit access to specified IPv4 addresses and networks:

```
(config)> add vpn l2tp acl address end value
(config)>
```

     Where *value* can be:

     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add vpn l2tp acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add vpn l2tp acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add vpn l2tp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.
```

```
Additional Configuration
------------------------------------------------------------------------------
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup

(config)>
```

Repeat this step to include additional firewall zones.

5. To add an L2TP access concentrator:
   a. Add an LAC:

```
(config)> add vpn l2tp lac name
(config add vpn l2tp lac name)>
```

   where *name* is the name of the LAC. For example, to add an LAC named lac_tunnel:

```
(config)> add vpn l2tp lac lac_tunnel
(config vpn l2tp lac lac_tunnel)>
```

   LACs are enabled by default. To disable:

```
(config vpn l2tp lac lac_tunnel)> enable false
(config vpn l2tp lac lac_tunnel)>
```

   b. Set the hostname or IP address of the L2TP network server:

```
(config vpn l2tp lac lac_tunnel)> lns hostname
(config vpn l2tp lac lac_tunnel)>
```

   c. (Optional) Set the UDP port to use to connect to the L2TP network server:

```
(config vpn l2tp lac lac_tunnel)> port int
(config vpn l2tp lac lac_tunnel)>
```

   where *int* is an integer between **1** and **65535**. The default is **1701**.

   d. (Optional) Set the username to use to log into the server:

```
(config vpn l2tp lac lac_tunnel)> username username
(config vpn l2tp lac lac_tunnel)>
```

   e. (Optional) Set the password to use to log into the server:

```
(config vpn l2tp lac lac_tunnel)> password password
(config vpn l2tp lac lac_tunnel)>
```

f. (Optional) Set the metric for the tunnel:

```
(config vpn l2tp lac lac_tunnel)> metric int
(config vpn l2tp lac lac_tunnel)>
```

where *int* is an integer between **0** and **65535**. The default is **1**.

g. Set the firewall zone for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.

i. Use the **?** to determine available zones:

```
(config vpn l2tp lac lac_tunnel)> zone ?

Zone: The firewall zone assigned to this tunnel. This can be used by packet
filtering rules and access control lists to restrict network traffic on this
tunnel.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:

(config vpn l2tp lac lac_tunnel)>
```

ii. Set the zone:

```
(config vpn l2tp lac lac_tunnel)> zone zone
(config vpn l2tp lac lac_tunnel)>
```

h. (Optional): Custom PPP configuration:

i. Enable custom PPP configuration:

```
(config vpn l2tp lac lac_tunnel)> custom enable true
(config vpn l2tp lac lac_tunnel)>
```

ii. Enable overriding, if the custom configuration should override the default configuration and only use the custom options:

```
(config vpn l2tp lac lac_tunnel)> custom override true
(config vpn l2tp lac lac_tunnel)>
```

iii. Paste or type the configuration data in the format of a pppd options file:

```
(config vpn l2tp lac lac_tunnel)> custom config_file data
(config vpn l2tp lac lac_tunnel)>
```

6. To add an L2TP network server:
   a. Add an LNS:

```
(config)> add vpn l2tp lns name
(config add vpn l2tp lac name)>
```

   where *name* is the name of the LNS. For example, to add an LNS named lns_server:

```
(config)> add vpn l2tp lns lns_server
(config vpn l2tp lns lns_server)>
```

   LACs are enabled by default. To disable:

```
(config vpn l2tp lns lns_server)> enable false
(config vpn l2tp lns lns_server)>
```

   b. Set the IP address of the L2TP access concentrator that this server will allow connections from:

```
(config vpn l2tp lns lns_server)> lac IP_address
(config vpn l2tp lns lns_server)>
```

   This can also be:
   - A range of IP addresses, using the format x.x.x.x-y.y.y.y, for example **192.168.188.1-192.168.188.254**.
   - The keyword **any**, which means that the server will accept connections from any IP address.

   c. Set the IP address of the L2TP virtual network interface:

```
(config vpn l2tp lns lns_server)> local_address IP_address
(config vpn l2tp lns lns_server)>
```

   d. Set the IP address to assign to the remote peer:

```
(config vpn l2tp lns lns_server)> remote_address IP_address
(config vpn l2tp lns lns_server)>
```

   e. (Optional) Set the authentication method:

```
(config vpn l2tp lns lns_server)> auth method
(config)>
```

   where *method* is one of the following:
   - **none**: No authentication is required.
   - **auto**: The device will attempt to connect using CHAP first, and then PAP.
   - **chap**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
   - **pap**: Uses the Password Authentication Profile (PAP) to authenticate.
   - **mschapv2**: Uses the Microsoft version of the Challenge Handshake Authentication Profile (CHAP) to authenticate.

If **auto**, **chap**, **pap** or **mschapv2** is selected, enter the **Username** and **Password** required to authenticate:

```
(config vpn l2tp lns lns_server)> username username
(config vpn l2tp lns lns_server)> password password
(config vpn l2tp lns lns_server)>
```

The default is **none**.

f. (Optional) Set the metric for the tunnel:

```
(config vpn l2tp lns lns_server)> metric int
(config vpn l2tp lns lns_server)>
```

where *int* is an integer between **0** and **65535**. The default is **1**.

g. Set the firewall zone for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.

   i. Use the **?** to determine available zones:

```
(config vpn l2tp lns lns_server)> zone ?

Zone: The firewall zone assigned to this tunnel. This can be used by packet
filtering rules and access control lists to restrict network traffic on this
tunnel.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:

(config vpn l2tp lns lns_server)>
```

   ii. Set the zone:

```
(config vpn l2tp lns lns_server)> zone zone
(config vpn l2tp lns lns_server)>
```

h. (Optional): Custom PPP configuration:

   i. Enable custom PPP configuration:

```
(config vpn l2tp lac lns lns_server)> custom enable true
(config vpn l2tp lns lns_server)>
```

   ii. Enable overriding, if the custom configuration should override the default configuration and only use the custom options:

```
(config vpn l2tp lns lns_server)> custom override true
(config vpn l2tp lns lns_server)>
```

iii. Paste or type the configuration data in the format of a pppd options file:

```
(config vpn l2tp lns lns_server)> custom config_file data
(config vpn l2tp lns lns_server)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

L2TP with IPsec

L2TP is commonly used in conjunction with IPsec in transport mode (to provide security).

Your IX10 supoorts L2TP with IPsec by configuring a transport-mode IPsec tunnel between the two endpoints, and then an L2TP tunnel with its LNS and LAC configured the same as the IPsec tunnel's endpoints. See Configure an IPsec tunnel for information about configuring an IPsec tunnel.

Note The IX10 does not currently support the configuration of IPsec protocol/port traffic selectors. This means that you cannot restrict traffic on the IPsec tunnel to L2TP traffic (typically UDP port 1701).

While multiple L2TP clients are supported on the IX10 by configuring a separate LNS for each client, multiple clients behind a Network Address Translation (NAT) device are not supported, because they will all appear to have the same IP address.

Show L2TP tunnel status

Web

Show the status of L2TP access connectors from the WebUI

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TP** > **Access Connectors**.

   The **L2TP Access Connectors** page appears.

2. To view configuration details about an L2TP access connector, click the ✱ (configuration) icon in the upper right of the tunnel's status pane.

Show the status of L2TP network servers from the WebUI

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TP** > **Network Servers**.

   The **L2TP Network Servers** page appears.
2. To view configuration details about an L2TP network server, click the ✸ (configuration) icon in the upper right of the tunnel's status pane.

Command line

Show the status of L2TP access connectors from the Admin CLI

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured L2TP access connectors, type the following at the prompt:

```
> show l2tp lac

Name      Enabled  Status  Device
--------- -------  ------ -----------
lac_test1 true     up     test_device0
lac_test2 true     pending
>
```

3. To display details about a specific tunnel:

```
> show l2tp lac name lac_test2

lac_test2 L2TP Access Concentrator Status
-------------------------------------
Enabled       : true
Status        : pending

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show the status of L2TP network servers from the Admin CLI

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured L2TP access connectors, type the following at the prompt:

```
> show l2tp lns

 Name      Enabled  Status  Device
 --------- -------  ------  -----------
 lns_test1 true     up      test_device0
 lns_test2 true     pending

>
```

3. To display details about a specific tunnel:

```
> show l2tp lns name lns_test2

 lns_test2 L2TP Access Concentrator Status
 -------------------------------------
 Enabled       : true
 Status        : pending

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

L2TPv3 Ethernet

Your IX10 device supports Layer 2 Tunneling Protocol Version 3 (L2TPv3) static unmanaged Ethernet tunnels.

Configure an L2TPv3 tunnel

Your IX10 device supports Layer 2 Tunneling Protocol Version 3 (L2TPv3) static unmanaged Ethernet tunnels.

Required configuration items

- A name for the L2TPv3 tunnel.
- Enable the tunnel.
- The remote endpoint IP address.
- The local endpoint IP address.
- The session ID.
- The peer session ID.

Additional configuration items

- Encapsulation type. If UDP is selected:
  - The ID for the tunnel.
  - The ID of the peer's tunnel.
  - Determine whether to enable UDP checksum.
- The session cookie.

- The peer session cookie.
- The Layer2SpecificHeader type.
- The Sequence numbering control.

Web

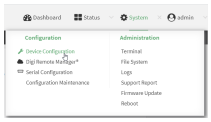
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **L2TPv3 ethernet**.
4. For **Add L2TPv3 ethernet tunnel**, type a name for the tunnel and click .
5. For **Remote endpoint**, type the IPv4 address of the remote endpoint.
6. For **Local endpoint**, select the interface that will be the local endpoint.
7. For **Tunnel ID**, type the tunnel identifier for this tunnel. This must match the value for **Peer tunnel ID** on the remote peer. Allowed value is any integer between 1 and 4294967295.
8. For **Peer tunnel ID**, type the **Tunnel ID** of the remote peer.
9. (Optional) For **Encapsulation type**, select either **UDP** or **IP**. If **UDP** is selected:
   a. For **UDP source port**, type the number of the source UDP port to be used for the tunnel.
   b. For **UDP destination port**, type the number of the destination UDP port to be used for the tunnel.
   c. (Optional) Click to enable **UDP checksum** to calculate and check the UDP checksum.
10. Click to expand **Sessions**.
    a. For **Add Sesssion**, type a name for a session carried by the parent tunnel and click .
    b. For **Session ID**, type the session identifier for this session. This must match the value for **Peer session ID** on the remote peer. Allowed value is any integer between 1 and 4294967295.
    c. For **Peer session ID**, type the **Session ID** of the remote peer.

d. (Optional) For **Cookie**, type the cookie value to be assigned to the session. Allowed value is 8 or 16 hex digits.
e. (Optional) For **Peer cookie**, type the **Cookie** value of the remote peer.
f. For **Layer2SpecificHeader type**, select the Layer2Specific header type. This must match what is configured on the remote peer.
g. For **Sequence numbering control**, determine the sequence number control to prevent or detect out of order packets. Allowed values are:
   - **None**: No sequence numbering.
   - **Send**: Add a sequence number to each outgoing packet.
   - **Receive**: Reorder packets if they are received out of order.
   - **Both**: Add a sequence number to each outgoing packet, and reorder packets if they are received out of order.

   The default is **None**.
h. Repeat for additional sessions.

11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a L2TPv3 Ethernet tunnel. For example, to add a tunnel named **L2TPv3_example**:

```
(config)> add vpn l2tpv3 L2TPv3_example
(config vpn l2tpeth L2TPv3_example)>
```

   The tunnel is enabled by default. To disable:

```
(config vpn l2tpeth L2TPv3_example)> enable false
(config vpn l2tpeth L2TPv3_example)>
```

4. Set the IPv4 address of the remote endpoint:

```
(config vpn l2tpeth L2TPv3_example)> remote IP_address
(config vpn l2tpeth L2TPv3_example)>
```

5. Set the interface of the local endpoint:
   i. Use the **?** to determine available interfaces:
   ii. Set the interface. For example:

```
(config vpn l2tpeth L2TPv3_example)> local /network/interface/eth1
(config vpn l2tpeth L2TPv3_example)>
```

6. Set the tunnel identifier for this tunnel. This must match the value for peer tunnel ID on the remote peer.

```
(config vpn l2tpeth L2TPv3_example)> tunnel_id value
(config vpn l2tpeth L2TPv3_example)>
```

   where *value* is any integer between 1 and 4294967295.

7. Set the tunnel ID of the remote peer:

```
(config vpn l2tpeth L2TPv3_example)> peer_tunnel_id value
(config vpn l2tpeth L2TPv3_example)>
```

   where *value* is any integer between 1 and 4294967295.

8. (Optional) Set the encapsulation type:

```
(config vpn l2tpeth L2TPv3_example)> encapsulation  value
(config vpn l2tpeth L2TPv3_example)>
```

   where *value* is either **udp** or **ip**. The default is **upd**.

   If **udp** is set:

   a. Set the source UDP port to be used for the tunnel:

```
(config vpn l2tpeth L2TPv3_example)> udp_source_port port
(config vpn l2tpeth L2TPv3_example)>
```

   b. Set the destination UDP port to be used for the tunnel.

```
(config vpn l2tpeth L2TPv3_example)> udp_destination_port port
(config vpn l2tpeth L2TPv3_example)>
```

   c. (Optional) To calculate and check the UDP checksum:

```
(config vpn l2tpeth L2TPv3_example)> udp_checksum true
(config vpn l2tpeth L2TPv3_example)>
```

9. Add a session carried by the parent tunnel:

```
(config vpn l2tpeth L2TPv3_example)> add session session_example
(config vpn l2tpeth L2TPv3_example session_example)>
```

10. Set the session identifier for this session. This must match the value for peer session ID on the remote peer.

```
(config vpn l2tpeth L2TPv3_example session_example)> session_id value
(config vpn l2tpeth L2TPv3_example session_example)>
```

    where *value* is any integer between 1 and 4294967295.

11. Set the session ID of the remote peer:

```
(config vpn l2tpeth L2TPv3_example session_example)> peer_session_id value
(config vpn l2tpeth L2TPv3_example session_example)>
```

    where *value* is any integer between 1 and 4294967295.

12. (Optional) Set the cookie value to be assigned to the session.

```
(config vpn l2tpeth L2TPv3_example session_example)> cookie value
(config vpn l2tpeth L2TPv3_example session_example)>
```

Allowed *value* is 8 or 16 hex digits.

13. (Optional) Set the cookie value of the remote peer:

```
(config vpn l2tpeth L2TPv3_example session_example)> peer cookie value
(config vpn l2tpeth L2TPv3_example session_example)>
```

Allowed *value* is 8 or 16 hex digits.

14. Set the Layer2Specific header type. This must match what is configured on the remote peer.

```
(config vpn l2tpeth L2TPv3_example session_example)> l2spec_type value
(config vpn l2tpeth L2TPv3_example session_example)>
```

where *value* is either **none** or **default**. The default is **default**.

15. Set the sequence number control to prevent or detect out of order packets.

```
(config vpn l2tpeth L2TPv3_example session_example)> seq value
(config vpn l2tpeth L2TPv3_example session_example)>
```

where *value* is one of:

- **none**: No sequence numbering.
- **send**: Add a sequence number to each outgoing packet.
- **recv**: Reorder packets if they are received out of order.
- **both**: Add a sequence number to each outgoing packet, and reorder packets if they are received out of order.

  The default is **none**.

16. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

17. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show L2TPV3 tunnel status

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TPv3 Ethernet**.

   The **L2TPv3 Ethernet** page appears.

2. To view configuration details about an L2TPV3 tunnel, click the ✸ (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured L2TPv3 Ethernet tunnels, type the following at the prompt:

```
> show l2tpeth

Tunnel Session    Enabled  Device      Status
----------------- -------  ----------- ------
test/session/test true     le_test_test up

>
```

3. To display details about a specific tunnel:

```
> show l2tpeth name /vpn/l2tpeth/test/session/test

test/session/test Tunnel Session Status
---------------------------------------
Enabled             : true
Status              : up


Local IP            : 4.3.2.1
Remote IP           : 10.10.10.1
Tunnel ID           : modem
Peer Tunnel ID      : 10.10.10.1 === 4.3.2.1
Session ID          : 255
Peer Session ID     : 1476
Lifetime (Actual)   : 600

Device              : le_test_test
RX Packets          : 2,102
RX Bytes            : 462
TX Packets          : 2,787
TX Byptes           : 3,120

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

MACsec

MACsec (Media Access Control Security) is a 802.1ae (Layer2) VPN protocol that can be used to create a secure MACsec tunnel over a wired Ethernet LAN. The MACsec uses keys to provide multiple authentications between hosts in a network.

A MACsec tunnel must be tied to a physical interface. You cannot create a MACsec tunnel for a bridge.

Security modes

Two security modes are available for a MACsec tunnel.

- **Automatic**: Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
- **Manual**: Uses connectivity association key information that is manually entered in the **CAK** and **CKN** fields.

Configure a MACsec tunnel

Your IX10 device supports MACsec (Layer 2 Tunneling Protocol).

Required configuration items

- The local network device to connect to the peer device.
- When using **Manual** mode, the connectivity association key and key name.

Web

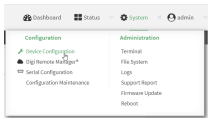
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **VPN** > **MACsec**.

4. For **Add MACsec tunnel**, click ⅋
5. Click **Enable**.
6. For **Local endpoint**, select the local network device you want to use to connect to the peer device.
7. For **Security mode**, select your desired mode.
   - **Automatic**: Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
   - **Manual**: Uses connectivity association key information that is manually entered in the **CAK** and **CKN** fields.
8. If you selected **Manual**, additional required fields display.
   a. For **CAK**, enter the connectivity associated key. The key format is 16 hex digits.
   b. For **CKN**, enter the connectivity associated key name. The key format is 32 hex digits.
9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Name the tunnel. At the config prompt, type:

```
(config)> add vpn macsec name
(config)>
```

   where *name* is a string.
4. Enable the tunnel:

```
(config vpn macsec tunnel1) enable true
(config vpn macsec tunnel1)>
```

5. Specify the local endpoint:

```
(config vpn macsec tunnel1) local value
(config vpn macsec tunnel1)>
```

   where *value* is one of the available options.
6. Specify the security mode:

```
(config vpn macsec tunnel1) type value
(config vpn macsec tunnel1)>
```

   where *value* is one of the following:

- **automatic**: Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
- **manual**: Uses connectivity association key information that is manually entered.

7. If you specified the **manual** security mode, enter the connectivity association key and key name.
   a. Specify the connectivity association key:

   ```
   (config vpn macsec tunnel1) association cak value
   (config  vpn macsec tunnel1)>
   ```

   where *value* is the association key. The key format is 16 hex digits.
   b. Specify the connectivity association key name:

   ```
   (config vpn macsec tunnel1) association ckn value
   (config  vpn macsec tunnel1)>
   ```

   where *value* is the association key name. The key format is 32 hex digits.
8. Save the configuration and apply the change.

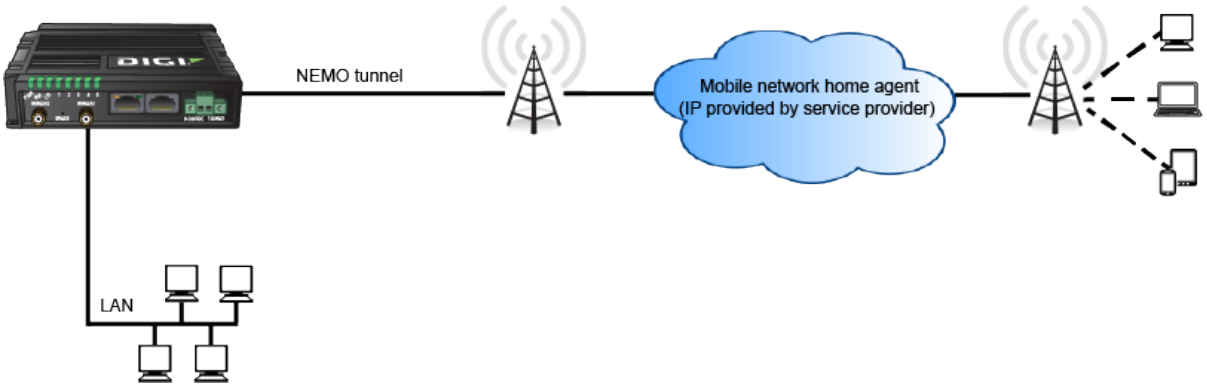
   ```
   (config)> save
   Configuration saved.
   >
   ```

9. Type **exit** to exit the Admin CLI.
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

NEMO

Network Mobility (NEMO) is a mobile networking technology that provides access to one or more Local Area Networks (LANs) on your device. NEMO creates a tunnel between the home agent on the mobile private network and the IX10 device, isolating the connection from internet traffic and advertising the IP subnets of the LANs for remote access and device management.

Dynamic Mobile Network Routing (DMNR) is the implementation of NEMO for Verizon Wireless Private Networks. DMNR support requires the use of Verizon SIM cards that have DMNR enabled.



Configure a NEMO tunnel

Configuring an NEMO tunnel with a remote device involves configuring the following items:

Required configuration items

- Enable the NEMO tunnel.

  The NEMO tunnel is enabled by default.
- The IP address of the NEMO virtual network interface.
- The firewall zone of the NEMO tunnel.
- The IP address of the NEMO home agent server. This is provided by your cellular carrier.
- The home agent's authentication key. This is provided by your cellular carrier.
- Home agent registration lifetime. This is provided by your cellular carrier.
- The local network interfaces that will be advertised on NEMO.

Additional configuration items

- The home agent Software Parameter Index (SPI).
- Path MTU discovery.

  Path MTU discovery is enabled by default. If it is disabled, identify the MTU.
- Care of address: the local network interface that is used to communicate with the peer.
  - If set to **Interface**, identify the local interface to be used. Generally, this will be the Wirelesss WAN (**Modem**).
  - If set to **IP address**, enter the IP address.
- The local network of the GRE endpoint negotiated by NEMO.
  - If the local network is set to Interface, identify the local interface to be used.

Web

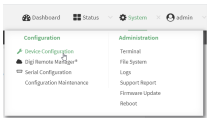
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN** > **NEMO**.

   The NEMO tunnel is enabled by default. To disable, toggle off **Enable**.

4. For **Home IP address**, type the IPv4 address of the NEMO virtual network interface.
5. For **Zone**, select **Internal**.

   The Internal firewall zone configures the IX10 device to trust traffic going to the tunnel and allows it through the network.

6. For **Home agent server IP** address, type the IPv4 address of the NEMO home agent. This is provided by your cellular carrier.
7. For **Key**, type the key used to authenticate to the home agent. This is provided by your cellular carrier.
8. For **Home agent SPI**, type the Security Parameter Index (SPI) value, which is used in the authentication extension when registering. This should be normally left at the default setting of **256** unless your service provider indicates a different value.
9. For **Home agent registration lifetime, in seconds**, type the number of seconds number of seconds until the authorization key expires. This is provided by your cellular carrier.
10. For **MTU discovery**, leave enabled to determine the maximum transmission unit (MTU) size.

    If disabled, for **MTU**, type the MTU size. The default MTU size for LANs on the IX10 device is 1500. The MTU size of the NEMO tunnel will be smaller, to take into account the required headers.

11. Click to expand **Care of address** to configure the local WAN interface of the internet facing network.
    a. For **Type**, select the method to determine the local network interface that is used to communicate with the peer.
       - If **Default route** is selected, the network interface that is used will be the same as the default route.
       - If **Interface** is selected, specify the local network interface.
       - If **IP address** is selected, type the IP address.

       The default is **Default route**.

12. Click to expand **GRE tunnel local endpoint**.
    a. For **Type**, select the local endpoint of the GRE endpoint negotiated by NEMO.
       - If **Default route** is selected, the network interface that is used will be the same as the default route.
       - If **Interface** is selected, specify the local network interface.

       The default is **Default route**.

13. Click to expand **Local networks**.
    a. For **Add Interface**, click to add a local network to use as a virtual NEMO network interface.

    b. For **Interface**, select the local interface to use as a virtual NEMO network interface. Generally, this will be the a Local Area Network (LAN).
    c. (Optional) Repeat for additional interfaces.
14. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a NEMO tunnel. For example, to add a NEMO tunnel named **nemo_example**:

```
(config)> add vpn nemo nemo_example
(config vpn nemo nemo_example)>
```

   The NEMO tunnel is enabled by default. To disable:

```
(config vpn nemo nemo_example)> enable false
(config vpn nemo nemo_example)>
```

4. Set the IPv4 address of the NEMO virtual network interface:

```
(config vpn nemo nemo_example)> home_address IPv4_address
(config vpn nemo nemo_example)>
```

5. Set the IPv4 address of the NEMO home agent. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> home_agent IPv4_address
(config vpn nemo nemo_example)>
```

6. Set the key used to authenticate to the home agent. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> key value
(config vpn nemo nemo_example)>
```

7. Set the the number of seconds number of seconds until the authorization key expires. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> lifetime integer
(config vpn nemo nemo_example)>
```

Allowed values are any integer between 1 and 65535.

8. MTU discovery is enabled by default, which allows the device to determine the maximum transmission unit (MTU) size. To disable:

```
(config vpn nemo nemo_example)> mtu_discovery false
(config vpn nemo nemo_example)>
```

If disabled, set the MTU size. The default MTU size for LANs on the IX10 device is 1500. The MTU size of the NEMO tunnel will be smaller, to take into account the required headers.

```
(config vpn nemo nemo_example)> mtu integer
(config vpn nemo nemo_example)>
```

Allowed values are any integer between 68 and 1476.

9. Set the Security Parameter Index (SPI) value, which is used in the authentication extension when registering. This should be normally left at the default setting of **256** unless your service provider indicates a different value.

```
(config vpn nemo nemo_example)> spi integer
(config vpn nemo nemo_example)>
```

Allowed values are any integer between 256 and 4294967295.

10. Set the firewall zone for the NEMO tunnel to internal:

```
(config vpn nemo nemo_example)> zone internal
(config vpn nemo nemo_example)>
```

The Internal firewall zone configures the IX10 device to trust traffic going to the tunnel and allows it through the network.

11. Configure the Care-of-Address, the local WAN interface of the internet facing network.
    a. Set the method to determine the Care-of-Address:

```
(config vpn nemo nemo_example)> coaddress type value
(config vpn nemo nemo_example)>
```

where *value* is one of:

- **defaultroute**: Uses the same network interface as the default route.
- **interface**

  If **interface** is used, set the interface:

  i. Use the **?** to determine available interfaces:

  ii. Set the interface. For example:

```
(config vpn nemo nemo_example)> coaddress interface eth1
(config vpn nemo nemo_example)>
```

- **ip**

  If **ip** is used, set the IP address:

```
(config vpn nemo nemo_example)> coaddress address IP_address
(config vpn nemo nemo_example)>
```

The default is **defaultroute**.

12. Set the GRE tunnel local endpoint:
    a. Set the method to determine the GRE tunnel local endpoint:

```
(config vpn nemo nemo_example)> tun_local type value
(config vpn nemo nemo_example)>
```

    where *value* is one of:
    - **defaultroute**: Uses the same network interface as the default route.
    - **interface**

      If **interface** is used, set the interface.
      i. Use the **?** to determine available interfaces:
      ii. Set the interface. For example:

```
(config vpn nemo nemo_example)> tun_local interface eth1
(config vpn nemo nemo_example)>
```

    The default is **defaultroute**.
13. Configure one or more local networks to use as a virtual NEMO network interface. Generally, this will be a Local Area Network (LAN):
    a. Add a local network to use as a virtual NEMO network interface:

```
(config vpn nemo nemo_example)> add network end eth
(config vpn nemo nemo_example)>
```

    b. (Optional) Repeat for additional interfaces.
14. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

15. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show NEMO status

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status** > **NEMO**.

   The **NEMO** page appears.
2. To view configuration details about an NEMO tunnel, click the ✸ (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured NEMO tunnels, type the following at the prompt:

```
> show nemo

NEMO  Enable  Status  Address  Agent   CoAddress
----  ------  ------  -------  -------  ----------
demo  false
test  true    up     1.2.3.4  4.3.2.1  10.10.10.1

>
```

3. To display details about a specific tunnel:

```
> show nemo name test

test NEMO Status
----------------
Enabled              : true
Status               : up
Home Agent           : 4.3.2.1
Care of Address      : 10.10.10.1
Interface            : modem
GRE Tunnel           : 10.10.10.1 === 4.3.2.1
Metric               : 255
MTU                  : 1476
Lifetime (Actual)    : 600

Local Network  Subnet        Status
-------------  ------------  ----------
lan1           192.168.2.1/24  Advertized
LAN2           192.168.3.1/24  Advertized


>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

WireGuard VPN

WireGuard is a VPN[1] is a protocol that operates at the network layer to provide communication between devices over a public network. It encrypts and encapsulates traffic to protect information.

1virtual private network

WireGuard supports full networking capabilities including standard, policy-based, and static routes, as well as firewalls. In addition to having IPs inside the tunnel, like IPSec and OpenVPN, you can use this WireGuard tunnel for policy-based routing: send only certain traffic through the tunnel or use it for static routes to send routing and networking through regardless of the source IP. You can also have multiple tunnels.

There are two modes available when configuring a WireGuard VPN:

- **Client mode**: Configure the IX10 device to act as a client, so it establishes an outbound WireGuard VPN tunnel to a remote server.
- **Server mode**: Configure the IX10 device to act as a server, so one or more remote devices can establish an inbound WireGuard VPN tunnel to the device.

Configure the WireGuard VPN

Your IX10 device supports using WireGuard VPN. You can configure the device for either client or server mode. For client mode, your IX10 is establishing an outbound WireGuard VPN connection to the WireGuard server. For server mode, your IX10 is acting as a WireGuard server and accepts incoming WireGuard VPN connections from one or more client devices. Regardless of how you configure the device, you will need to to create a Wireguard tunnel and corresponding interface.

Before you begin

Decide whether you want your device to establish an outbound WireGuard VPN connection or if you want it to act as a WireGuard server. Each mode requires different information.

For client mode	**For server mode**
You need the following information from the WireGuard server: ■ Private key ■ Remote endpoint address or hostname ■ Remote endpoint port ■ Remote endpoint public key ■ Preshared key (optional) ■ Local and remote IP addresses	You need the following information: ■ Client public key **Note** This key can come from the client device or you can generate it from the Digi device's Admin CLI console using the `wireguard generate [tunnel_name] [client_name]` command after configuring the Wireguard server settings on the Digi device. ■ Pre-shared key (optional) ■ Local and remote IP addresses

Web

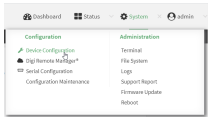
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

1. To create a WireGuard tunnel, navigate to **VPN** > **WireGuard** > **WireGuard tunnel**.
2. Click to add a new WireGuard tunnel.
3. Type a name for the tunnel.
4. Click **OK**.

   The settings for your new tunnel appear.

Tunnel setting	UI configuration
Enable	The new tunnel is enabled by default. It can be disabled if the tunnel is being set up for future use or if you want to stop the tunnel while testing other configuration changes.

Tunnel setting	UI configuration
Peers	a. Click to add a new peer. ▪ If this IX10 is the WireGuard client, then only add one peer. The peer is the remote Wireguard server to which it connects. ▪ If this IX10 is the WireGuard server, add one or more peers. The peer(s) are the remote WireGuard clients that will connect to this device. b. Configure the settings for the new peer (s). If the new peer is to act as the WireGuard server, make sure to configure the following settings: ▪ [Remote] Public key ▪ [Remote] Pre-shared key (optional) ▪ [Remote] Allowed addresses: Only traffic destined for an IP address added here is sent to this peer. ▪ [Remote] Endpoint address ▪ [Remote] Endpoint port If the new peer is to act as a remote WireGuard client, make sure to configure the following settings: ▪ [Client] Public key ▪ [Client] Pre-shared key (optional) ▪ [Local and Remote] Allowed addresses
Device managed private key	Enable to allow the IX10 to generate its own public and private keys. If this setting is enabled, it triggers the IX10 to automatically generate a private key and corresponding public key. This private and public key is used to establish the encrypted communication between the client and peer via the Wireguard tunnel. To see the public key, navigate to **Status** > **VPN** > **WireGuard**.

Tunnel setting	UI configuration
Private key	Type the private key for the Wireguard tunnel, if the **Device managed private key** setting is disabled.
Endpoint port	The WireGuard connection value of **51820** is populated by default.

5. Modify the settings.
6. To create the WireGuard interface, navigate to **Network** > **Interfaces** > **Interface**.
7. Click to add a new interface.
8. Type a name for the interface.
9. Click **OK**.
10. The settings for your new interface appear.

Tunnel setting	UI configuration
Enable	The new interface is enabled by default. It can be disabled if it is being set up for future use or if you want to stop using the interface while testing other configuration changes.
Zone	Select **External**.
Device	Select the device the interface will use, which is the new WireGuard tunnel you created.
IPv4	a. Click **IPv4** to expand the settings menu. b. For **Address**, type the IP address and netmask assigned to this interface (SYNTAX: IPv4_address/netmask). For example, `10.200.200.1/24`. c. Click to expand **DNS servers**. d. Click to add a new DNS server. e. For DNS Server, type the IP address of the DNS server (SYNTAX: IPv4_address). For example, `10.200.200.1`.

11. Click **Apply** to save the new configuration settings.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Save the configuration and apply the change.

```
(config vpn iptunnel gre_example)> save
Configuration saved.
>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

5. At the command line, type **VPN** to enter configuration mode for VPN:

```
 > config vpn
(config vpn)>
```

6. Type **wireguard** to enter configuration mode for WireGuard.

```
 > config vpn wireguard
(config vpn wireguard)>
```

7. The table below lists the required settings for creating and configuring a client WireGuard tunnel.

Configuration	Description

add	Add a new WireGuard tunnel.
	`> config vpn wireguard add *name*`
	`(config)>`
	Where *name* is the name of the new WireGuard tunnel.
	For example, *newtunnel1*.

enable	The WireGuard tunnel is enabled by default.
	You may want to temporarily disable the tunnel while it is being set up, for future use, or if you want to stop the tunnel while testing other configuration changes.
	To disable:
	`(config)> vpn wireguard *name* enable false`
	`(config)>`
	To enable:
	`(config)> vpn wireguard *name* enable true`
	`(config)>`

peer	a. Determine if the IX10 will act as a client or server.

- If this IX10 is the WireGuard client, then only add one peer. The peer is the remote Wireguard server to which it connects.
- If this IX10 is the WireGuard server, add one or more peers. The peer(s) are the remote WireGuard clients that will connect to this device.

b. Create the peer(s).

```
(config)> vpn wireguard name add peer
(config)>
```

For a peer that acts as the remote Wireguard server, configure the following settings:

- [Remote] Device managed public key

```
(config vpn wireguard [name])> generate

Parameters
----------------------------------------
tunnel          Tunnel Name (Required)
peer            Peer (Required)
```

- [Remote] Public key

```
(config)> vpn wireguard name peer public_key
(config)>
```

- [Remote] Pre-shared key (optional)

```
(config)> vpn wireguard name peer psk
(config)>
```

- [Remote] Allowed addresses: Only traffic destined for an IP address added here will be sent to this peer.

```
(config)> vpn wireguard name peer overlay
(config)>
```

- [Remote] Endpoint address

```
(config)> vpn wireguard name peer endpoint
(config)>
```

- [Remote] Endpoint port

```
(config)> vpn wireguard name peer port
(config)>
```

For a peer(s) that acts as the remote WireGuard client, configure the following settings:

- [Client] Public key

	(config)> vpn wireguard *name* peer public_key (config)> ■ [Client] Pre-shared key (optional) (config)> vpn wireguard *name* peer psk (config)> ■ [Local and Remote] Allowed addresses
autogenerate	Enable to allow the IX10 to generate its own public and private keys. If this setting is enabled, it triggers the IX10 to automatically generate a private key and corresponding public key. To enable: > config vpn wireguard add *name* autogenerate true (config)> To disable: > config vpn wireguard add *name* autogenerate false (config)>
port	The WireGuard connection value of **51820** is populated by default. (config)> vpn wireguard *name* port (config)>
private-key	Type the private key for the Wireguard tunnel, if the **Device managed private key** setting is disabled. > config vpn wireguard add *name* private key *value* (config)> With *value* being a 32-byte string encoded in base 64.

8. The table below lists the required settings for creating and configuring a new interface.

Configuration	Description
add	Add a new interface. > (config network interface) > add *name* (config)> Where *name* is the name of the new interface. For example, `add newWGtunnel1`.
enable	The interface is enabled by default. You may want to temporarily disable the tunnel while it is being set up, for future use, or if you want to stop the tunnel while testing other configuration changes.

	To disable:
	`(config network interface ) > name enable false`
	`(config)>`
	To enable:
	`(config network interface) > name enable true`
	`(config)>`
	Where *name* is the name of the new interface.

zone	Set the zone to external.
	`(config network interface [name]) > zone external`
	`(config)>`

device	Add the network device used by this interface. `(config network interface [name]) > device /vpn/wireguard/[name]` For example, `device /vpn/wireguard/newWGtunnel1`.

IPv4	a. Add the address and netmask assigned to this interface.
	`config network interface [name] ipv4) > address IPv4_[IPaddress]/[netmask]`
	For example, `ipv4_10.200.200.1/24`.
	b. Add the IP address of the DNS server.
	`(config network interface [name] ipv4) > dns`
	`(config network interface [name] ipv4 dns) > ipv4_[address].`
	Address is the IP address of the DNS server.
	For example, `ipv4_10.200.200.1`.

Services

This chapter contains the following topics:

Allow remote access for web administration and SSH 502
Configure the web administration service 505
Configure SSH access 515
Use SSH with key authentication 522
Configure telnet access 525
Configure DNS 530
Simple Network Management Protocol (SNMP) 537
Location information 544
Modbus gateway 570
System time synchronization 588
Network Time Protocol 593
Configure a multicast route 600
Enable service discovery (mDNS) 602
Use the MQTT broker service 605
Use the iPerf service 616
Configure the ping responder service 621

Allow remote access for web administration and SSH

By default, only devices connected to the IX10's LAN have access to the device via web administration and SSH. To enable these services for access from remote devices:

- The IX10 device must have a publicly reachable IP address.
- The **External** firewall zone must be added to the web administration or SSH service. See Firewall configuration for information on zones.
- See Set the idle timeout for IX10 users for information about setting the inactivity timeout for the web administration and SSH services.

To allow web administration or SSH for the External firewall zone:

Add the External firewall zone to the web administration service

Web

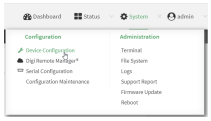
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

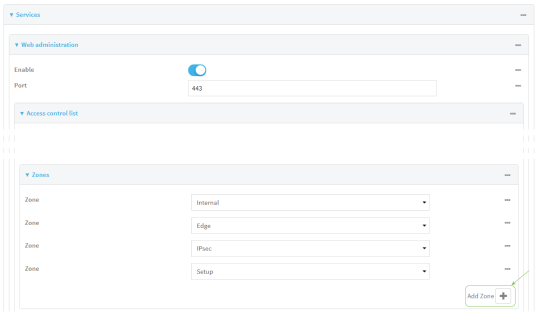
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

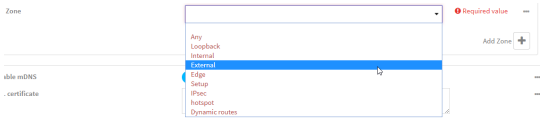
   

   The **Configuration** window is displayed.
3. Click **Services** > **Web administration** > **Access Control List** > **Zones**.

4. For **Add Zone**, click .



5. Select **External**.



6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the external zone to the web administration service:

```
(config)> add service web_admin acl zone end external
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Add the External firewall zone to the SSH service

Web

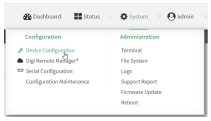
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

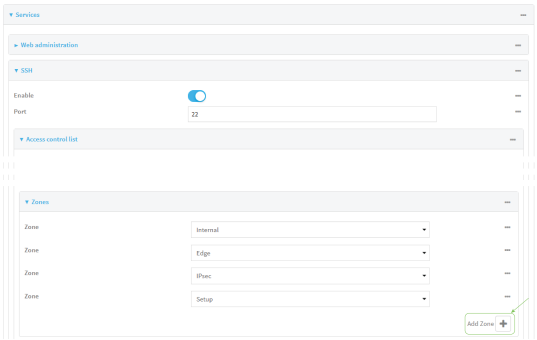
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

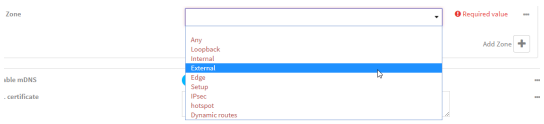
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Configuration** > **Services** > **SSH** > **Access Control List** > **Zones**.
4. For **Add Zone**, click .

5. Select **External**.

6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the **External** zone to the SSH service:

```
(config)> add service ssh acl zone end external
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the web administration service

The web administration service allows you to monitor and configure the IX10 device by using the WebUI, a browser-based interface.

By default, the web administration service is enabled and uses the standard HTTPS port, 443. The default access control for the service uses the **Internal** firewall zone, which means that only devices connected to the IX10's LAN can access the WebUI. If this configuration is sufficient for your needs, no further configuration is required. See Allow remote access for web administration and SSH for information about configuring the web administration service to allow access from remote devices.

Required configuration items

- The web administration service is enabled by default.
- Configure access control for the service.

Additional configuration items

- Port to use for web administration service communication.
- Multicast DNS (mDNS) support.
- An SSL certificate to use for communications with the service.
- Support for legacy encryption protocols.

See Set the idle timeout for IX10 users for information about setting the inactivity timeout for the web administration services.

Enable or disable the web administration service

The web administration service is enabled by default. To disable the service, or enable it if it has been disabled:

Web

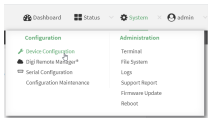
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Web administration**.
4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable or disable the web administration service:
   - To enable the service:

```
(config)> service web_admin enable true
(config)>
```

- To disable the sevice:

```
(config)> service web_admin enable false
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the service

Web

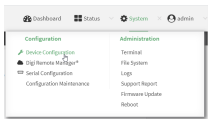
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Web administration**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click ♑.
     c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the web administration service.

d. Click again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click
  c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the web administration service.
  d. Click again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click again to allow access through additional firewall zones.

6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
7. For **SSL certificate**, if you have your own signed SSL certificate, paste the certificate and private key. If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
   - The SSL certificate and private key must be in PEM format.
   - The private key can use one of the following algorithms:
     - RSA
     - DSA
     - ECDSA
     - ECDH

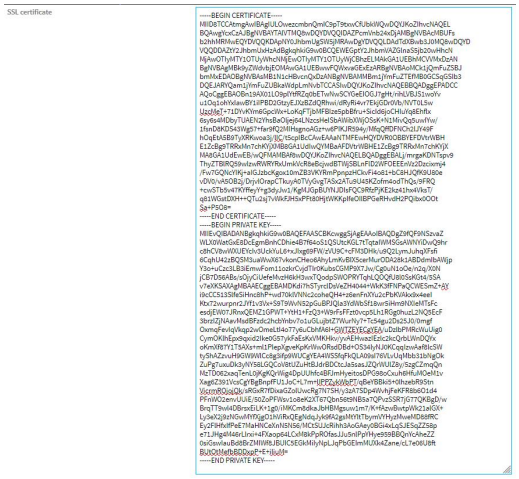
     Note Password-protected certificate keys are not supported.

Example:

a. Generate the SSL certificate and private key, for example:

```
# openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
```

b. Paste the contents of **certificate.pem** and **key.pem** into the **SSL certificate** field. The contents of the **certificate.pem** must be first. For example:



8. **View** is set to **Auto** by default and normally should not be changed.
9. **Legacy port redirection** is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed. To disable legacy port redirection, click to expand **Legacy port redirection** and deselect **Enable**.
10. For **Minimum TLS version**, select the minimum TLS version that can be used by client to negotiate the HTTPS session.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config)> add service web_admin acl address end value
     (config)>
     ```

     Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the web administratrion service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service web_admin acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the web administratrion service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service web_admin acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
------------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service web_admin acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

4. (Optional) If you have your own signed SSL certificate, if you have your own signed SSL certificate, set the certificate and private key by pasting their contents into the **service web_admin cert** command. Enclose the certificate and private key contents in quotes (**"**).

```
(config)> service web_admin cert "ssl-cert-and-private-key"
(config)>
```

   - If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
   - The SSL certificate and private key must be in PEM format.
   - The private key can use one of the following algorithms:
     - RSA
     - DSA
     - ECDSA
     - ECDH

     Note Password-protected certificate keys are not supported.

   Example

   a. Generate the SSL certificate and private key, for example:

```
# openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
```

   b. Paste the contents of **certificate.pem** and **key.pem** into the **service web_admin cert** command. Enclose the contents of **certificate.pem** and **key.pem** in quotes. For example:

```
(config)> service web_admin cert "-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgIULOwezcmbnQmIC9pT9txwCfUbkWQwDQYJKoZIhvcNAQEL
```

BQAwgYcxCzAJBgNVBAYTAlVTMQ8wDQYDVQQIDAZPcmVnb24xDjAMBgNVBAcMBUFs

b2hhMRMwEQYDVQQKDApNY0JhbmUgSW5jMRAwDgYDVQQLDAdTdXBwb3J0MQ8wDQYD
VQQDDAZtY2JhbmUxHzAdBgkqhkiG9w0BCQEWEGptY2JhbmVAZGlnaS5jb20wHhcN
MjAwOTIyMTY1OTUyWhcNMjEwOTIyMTY1OTUyWjCBhzELMAkGA1UEBhMCVVMxDzAN
BgNVBAgMBk9yZWdvbjEOMAwGA1UEBwwFQWxvaGExEzARBgNVBAoMCk1jQmFuZSBJ
bmMxEDAOBgNVBAsMB1N1cHBvcnQxDzANBgNVBAMMBm1jYmFuZTEfMB0GCSqGSIb3
DQEJARYQam1jYmFuZUBkaWdpLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAOBn19AX01LO9plYtfRZq0bETwNwSCYGeEIOGJ7gHt/rihLVBJS1woYv
u1Oq1ohYxIawBY1iIPBD2GtzyEJXzBZdQRhwi/dRyRi4vr7EkjGDr0Vb/NVT0L5w
UzcMeT+71DYvKYm6GpcWx+LoKqFTjbMFBIze5pbBfru+Sicld6joCHIuYq8Ehflx
6sy6s4MDbyTUAEN2YhsBaOljej64LNzcsHeISbAWibXWjOSsK+N1MivQq5uwIYw/
1fsnD8KDS43Wg57+far9fQ2MIHsgnoAGz+w6PIKJR594y/MfqQffDFNCh2lJY49F
hOqEtA5B9TyXRKwoa3j/IIC/t5cpIBcCAwEAAaNTMFEwHQYDVR0OBBYEFDVtrWBH
E1ZcBg9TRRxMn7chKYjXMB8GA1UdIwQYMBaAFDVtrWBHE1ZcBg9TRRxMn7chKYjX
MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBALj/mrgaKDNTspv9
ThyZTBlRQ59wIzwRWRYRxUmkVcR8eBcjwdBTWjSBLnFID2WFOEEEnVz2Dzcixmj4
/Fw7GQNcYIKj+aIGJzbcKgox10mZB3VKYRmPpnpzHCkvFi4o81+bC8HJQfK9U80e
vDV0/vA5OB2j/DrjvlOrapCTkuyA0TVyGvgTASx2ATu9U45KZofm4odThQs/9FRQ
+cwSTb5v47KYffeyY+g3dyJw1/KgMJGpBUYNJDIsFQC9RfzPjKE2kz41hx4VksT/
q81WGstDXH++QTu2sj7vWkFJH5xPFt80HjtWKKpIfeOIIBPGeRHvdH2PQibx0OOt
Sa+P5O8=
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDgZ9fQF9NSzvaZ
WLX0WatGxE8DcEgmBnhCDhie4B7f64oS1QSUtcKGL7tTqtaIWMSGsAWNYiDwQ9hr
c8hCV8wWXUEYcIv3UckYuL6+xJIxg69FW/zVU9C+cFM3DHk/u9Q2LymJuhqXFsfi
6CqhU42zBQSM3uaWwX67vkonCHeo6AhyLmKvBIX5cerMurODA28k1ABDdmIbAWjp
Y3o+uCzc3LB3iEmwFom11ozkrCvjdTIr0KubsCGMP9X7Jw/Cg0uN1oOe/n2q/X0N
jCB7D56ABs/sOjyCiUefeMvzH6kH3wxTQodpSWOPRYTqhLQOQfU8l0SsKGt4/5SA
v7eXKSAXAgMBAAECggEBAMDKdi7hSTyrclDsVeZH4044+WkK3fFNPaQCWESmZ+AY
i9cCC513SlfeSiHnc8hP+wd70klVNNc2coheQH4+z6enFnXYu2cPbKVAkx9x4eeI
Ktx72wurpnr2JYf1v3Vx+S9T9WvN52pGuBPJQla3YdWbSf18wr5iHm9NXIeMTsFc
esdjEW07JRnxQEMZ1GPWT+YtH1+FzQ3+W9rFsFFzt0vcp5Lh1RGg0huzL2NQ5EcF
3brzIZjNAavMsdBFzdc2hcbYnbv7o1uGLujbtZ7WurNy7+Tc54gu2Ds25J0/0mgf
OxmqFevIqVkqp2wOmeLtl4o77y6uCbhfA6I+GWTZEYECgYEA/uDzlbPMRcWuUig0
CymOKlhEpx9qxid2Ike0G57ykFaEsKxVMKHkv/yvAEHwazIEzlc2kcQrbLWnDQYx
oKmXf87Y1T5AXs+ml1PlepXgveKpKrWwORsdDBd+OS34lyNJ0KCqqIzwAaf8lcSW
tyShAZzvuH9GW9WlCc8g3ifp9WUCgYEA4WSSfqFkQLA09sI76VLvUqMbb31bNgOk
ZuPg7uxuDk3yNY58LGQCoV8tUZuHtBJdrBDCtcJa5sasJZQrWUlZ8y/5zgCZmqQn
MzTD062xaqTenL0jKgKQrWig4DpUUhfc4BFJmHyeitosDPG98oCxuh6HfuMOeM1v
Xag6Z391VcsCgYBgBnpfFU1JoC+L7m+IlPPZykWbPT/qBeYBBki5+0lhzebR9Stn
VicrmROjojQk/sRGxR7fDixaGZolUwcRg7N7SH/y3zA7SDp4WvhjFeKFR8b6O1d4
PFnWO2envUUiE/50ZoPFWsv1o8eK2XT67Qbn56t9NB5a7QPvzSSR7jG77QKBgD/w
BrqTT9wl4DBrsxEiLK+1g0/iMKCm8dkaJbHBMgsuw1m7/K+fAzwBwtpWk21alGX+
Ly3eX2j9zNGwMYfXjgO1hViRxQEgNdqJyk9fA2gsMtYltTbymVYHyzMweMD88fRC
Ey2FlHfxIfPeE7MaHNCeXnN5N56/MCtSUJcRihh3AoGAey0BGi4xLqSJESqZZ58p
e71JHg4M46rLlrxi+4FXaop64LCxM8kPpROfasJJu5nlPpYHye959BBQnYcAheZZ

```
0siGswlauBd8BrZMIWf8JBUIC5EGkMilyNpLJqPbGEImMUXk4Zane/cL7e06U8ft
BUtOtMefbBDDxpP+E+iliuM=
-----END PRIVATE KEY-----"
(config)>
```

5. (Optional) Configure Multicast DNS (mDNS):

   mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

   - To enable the mDNS protocol:

     ```
     (config)> service web_admin mdns enable true
     (config>
     ```

   - To disable the mDNS protocl:

     ```
     (config)> service web_admin mdns enable false
     (config)>
     ```

6. (Optional) Set the port number for this service.

   The default setting of 443 normally should not be changed.

   ```
   (config)> service web_admin port 444
   (config)>
   ```

7. (Optional) Set the minimum TLS version that can be used by client to negotiate the HTTPS session:

   ```
   (config)> service web_admin legacy_encryption value
   (config)>
   ```

   where *value* is one of:

   - **TLS-1_1**
   - **TLS-1_2**
   - **TLS-1_3**

   The default is **TLS-1_2**.

8. (Optional) Disable legacy port redirection.

   Legacy port redirection is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed.

   To disable legacy port redirection:

   ```
   (config)> service web_admin legacy enable false
   (config)>
   ```

9. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure SSH access

The IX10's default configuration has SSH access enabled, and allows SSH access to the device from authorized users within the **Internal** firewall zone. If this configuration is sufficient for your needs, no further configuration is required. See Allow remote access for web administration and SSH for information about configuring the SSH service to allow access from remote devices.

Required configuration items

- Enable SSH access.
- Configure access control for the SSH service.

Additional configuration items

- Port to use for communications with the SSH service.
- Multicast DNS (mDNS) support.
- A private key to use for communications with the SSH service.
- Create custom SSH configuration settings.

See Set the idle timeout for IX10 users for information about setting the inactivity timeout for the SSH service.

Enable or disable the SSH service

The SSH service is enabled by default. To disable the service, or enable it if it has been disabled:

Web

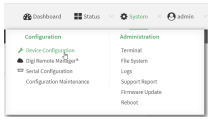
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **Services** > **SSH**.
4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable or disable the SSH service:
   - To enable the service:

```
(config)> service ssh enable true
(config)>
```

   - To disable the sevice:

```
(config)> service ssh enable false
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the service

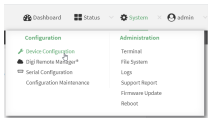
Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services** > **SSH**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's SSH service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the SSH service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's SSH service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the SSH service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.

d. Click again to allow access through additional firewall zones.

6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
7. For **Private key**, type the private key in PEM format. If **Private key** is blank, the device will use an automatically-generated key.
8. To create custom SSH configuration settings:
   a. Click to expand **Custom configuration**.
   b. Click **Enable**.
   c. For **Override**:
      - If **Override** is enabled, entries in **Configuration file** will be used in place of the standard SSH configuration.
      - If **Override** is not enabled, entries in **Configuration file** will be added to the standard SSH configuration.
   d. For **Configuration file**, type configuration settings in the form of an OpenSSH sshd_config file.

      For example, to enable the diffie-helman-group-sha-14 key exchange algorithm:
      i. Click **Enable** to enable SSH custom configuration.
      ii. Leave **Override** disabled.
      iii. For **Configuration file**, type the following:

```
KexAlgorithms +diffie-hellman-group14-sha1
```

9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

```
(config)> add service ssh acl address end value
(config)>
```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the SSH service.

     Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service ssh acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the SSH service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service ssh acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
------------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service ssh acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.
```

```
Additional Configuration
--------------------------------------------------------------------------------
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup

(config)>
```

Repeat this step to include additional firewall zones.

4. (Optional) Set the private key in PEM format. If not set, the device will use an automatically-generated key.

```
(config)> service ssh key key.pem
(config)>
```

5. (Optional) Configure Multicast DNS (mDNS)

   mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

   - To enable the mDNS protocol:

```
(config)> service ssh mdns enable true
(config>
```

   - To disable the mDNS protocl:

```
(config)> service ssh mdns enable false
(config)>
```

6. (Optional) Set the port number for this service.

   The default setting of 22 normally should not be changed.

```
(config)> service ssh port 24
(config)>
```

7. To create custom SSH configuration settings:

   a. Enable custom configurations:

```
(config)> service ssh custom enable true
(config)>
```

   b. To override the standard SSH configuration and only use the **config_file** parameter:

```
(config)> service ssh custom override true
(config)>
```

- If **override** is set to **true**, entries in **Configuration file** will be used in place of the standard SSH configuration.
- If **override** is set to **false**, entries in **Configuration file** will be added to the standard SSH configuration.

  The default is **false**.

c. Set the configuration settings:

```
(config)> service ssh custom config_file value
(config)>
```

where *value* is one or more entires in the form of an OpenSSH sshd_config file. For example, to enable the diffie-helman-group-sha-14 key exchange algorithm:

```
(config)> service ssh custom config_file "KexAlgorithms +diffie-hellman-group14-sha1"
(config)>
```

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Use SSH with key authentication

Rather than using passwords, you can use SSH keys to authenticate users connecting via SSH, SFTP, or SCP. SSH keys provide security and scalability:

- **Security**: Using SSH keys for authentication is more secure than using passwords. Unlike a password that can be guessed by an unauthorized user, SSH key pairs provide more sophisticated security. A public key configured on the IX10 device is paired with a private key on the user's PC. The private key, once generated, remains on the user's PC.
- **Scalability**: SSH keys can be used on more than one IX10 device.

Generating SSH key pairs

On a Microsoft Windows PC, you can generate SSH key pairs using a terminal emulator application, such as **PuTTY** or **Tera Term**.

On a Linux host, an SSH key pair is usually created automatically in the user's **.ssh** directory. The private and public keys are named **id_rsa** and **id_rsa.pub**. If you need to generate an SSH key pair, you can use the **ssh-keygen** application.

For example, the following entry generates an RSA key pair in the user's **.ssh** directory:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa
```

The private key file is named **id_rsa** and the public key file is named **id_rsa.pub**. (The **.pub** extension is automatically appended to the name specified for the private key output file.)

Required configuration items

- Name for the user
- SSH public key for the user

Additional configuration items

- If you want to access the IX10 device using SSH over a WAN interface, configure the access control list for the SSH service to allow SSH access for the **External** firewall zone.

Web

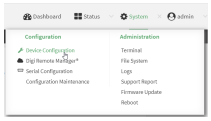
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication** > **Users**.
4. Select an existing user or create a new user. See User authentication for information about creating a new user.
5. Click **SSH keys**.
6. In **Add SSH key**, enter a name for the SSH key and click .
7. Enter the public SSH key by pasting or typing a public encryption key that this user can use for passwordless SSH login.
8. Click **Apply** to save the configuration and apply the change.

Command line

You can add configure passwordless SSH login for an existing user or include the support when creating a new user. See User authentication for information about creating a new user. These instructions assume an existing user named **temp_user**.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add an SSH key for the user by using the ssh_key command and pasting or typing a public encryption key:

```
(config)> add auth user maria ssh_key key_name key
(config)>
```

   where:

   - *key_name* is a name for the key.
   - *key* is a public SSH key, which you can enter by pasting or typing a public encryption key that this user can use for passwordless SSH login
4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure telnet access

By default, the telnet service is disabled.

Note Telnet is an insecure protocol and should only be used for backward-compatibility reasons, and only if the network connection is otherwise secured.

Required configuration items

- Enable telnet access.
- Configure access control for the telnet service.

Additional configuration items

- Port to use for communications with the telnet service.
- Multicast DNS (mDNS) support.

See Set the idle timeout for IX10 users for information about setting the inactivity timeout for the telnet service.

Enable the telnet service

The telnet service is disabled by default. To enable the service:

Web

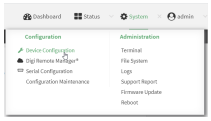
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **telnet**.

4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the telnet service:

```
(config)> service telnet enable true
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the service

Web

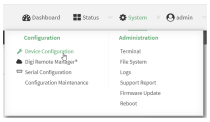
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services** > **telnet**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's telnet service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the telnet service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's telnet service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the telnet service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
     d. Click again to allow access through additional firewall zones.

6. Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

```
(config)> add service telnet acl address end value
(config)>
```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the telnet service.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

```
(config)> add service telnet acl address6 end value
(config)>
```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the telnet service.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service telnet acl interface end value
(config)>
```

     Where *value* is an interface defined on your device.

     Display a list of available interfaces:

     Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?
```

```
Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service telnet acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

4. (Optional) Configure Multicast DNS (mDNS)

   mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is disabled by default. To enable:

```
(config)> service telnet mdns enable true
(config>
```

5. (Optional) Set the port number for this service.

The default setting of 23 normally should not be changed.

```
(config)> service telnet port 25
(config)>
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure DNS

The IX10 device includes a caching DNS server which forwards queries to the DNS servers that are associated with the network interfaces, and caches the results. This server is used within the device, and cannot be disabled. Use the access control list to restrict external access to this server.

Required configuration items

- Configure access control for the DNS service.

Additional configuration items

- Whether the device should cache negative responses.
- Whether the device should always perform DNS queries to all available DNS servers.
- Whether to prevent upstream DNS servers from returning private IP addresses.
- Additional DNS servers, in addition to the ones associated with the device's network interfaces.
- Specific host names and their IP addresses.

  The device is configured by default with the hostname **digi.device**, which corresponds to the **192.168.210.1** IP address.

To configure the DNS server:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

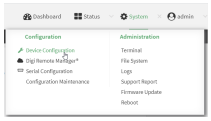
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

   b. Click the **Device ID**.

c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services** > **DNS**.
4. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's DNS service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the DNS service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's DNS service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the DNS service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.

d. Click again to allow access through additional firewall zones.

5. (Optional) **Cache negative responses** is enabled by default. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable, click to toggle off **Cache negative responses**.
6. (Optional) **Query all servers** is enabled by default. This option is useful when only some DNS servers will be able to resolve hostnames. To disable, click to toggle off **Query all servers**.
7. (Optional) **Rebind protection**, if enabled, prevents upstream DNS servers from returning private IP addresses. To enable, click **Rebind protection**.
8. (Optional) **Allow localhost rebinding** is enabled by default if **Rebind protection** is enabled. This is useful for Real-time Black List (RBL) servers.
9. (Optional) Type the IP address of the **Fallback server**. This is a DNS server to be used in the absence of any other server. The default is **8.8.8.8**.
10. (Optional) To add additional DNS servers:
    a. Click **DNS servers**.
    b. For **Add Server**, click .
    c. (Optional) Enter a label for the DNS server.
    d. For **DNS server**, enter the IP address of the DNS server.
    e. **Domain** restricts the device's use of this DNS server based on the domain. If no domain are listed, then all queries may be sent to this server.
11. (Optional) To add host names and their IP addresses that the device's DNS server will resolve:
    a. Click **Additional DNS hostnames**.
    b. For **Add Host**, click .
    c. Type the **IP address** of the host.
    d. For **Name**, type the hostname.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

```
(config)> add service dns acl address end value
(config)>
```

   Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service dns acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service dns acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service dns acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

4. (Optional) Cache negative responses

   By default, the device's DNS server caches negative responses. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable:

   ```
   (config)> service dns cache_negative_responses false
   (config>
   ```

5. (Optional) Query all servers

   By default, the device's DNS server queries all available DNS servers. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable:

   ```
   (config)> service dns query_all_servers false
   (config>
   ```

6. (Optional) Rebind protection

   By default, rebind protection is disabled. If enabled, this prevents upstream DNS servers from returning private IP addresses. To enable:

   ```
   (config)> service dns stop_dns_rebind false
   (config)>
   ```

7. (Optional) Allow localhost rebinding

   By default, localhost rebinding is enabled by default if rebind protection is enabled. This is useful for Real-time Black List (RBL) servers. To disable:

   ```
   (config)> service dns rebind_localhost_ok false
   (config)>
   ```

8. (Optional) Fallback server

   Configure the IP address of the DNS server to be used in the absence of any other server. The default is **8.8.8.8**.

```
(config)> service dns fallback_server value
(config)>
```

9. (Optional) Add additional DNS servers
   a. Add a DNS server:

```
(config)> add service dns server end
(config service dns server 0)>
```

   b. Set the IP address of the DNS server:

```
(config service dns server 0)> address ip-addr
(config service dns server 0)>
```

   c. To restrict the device's use of this DNS server based on the domain, use the **domain** command. If no domain are listed, then all queries may be sent to this server.

```
(config service dns server 0)> domain domain
(config service dns server 0)>
```

   d. (Optional) Set a label for this DNS server:

```
(config service dns server 0)> label label
(config service dns server 0)>
```

10. (Optional) Add host names and their IP addresses that the device's DNS server will resolve
    a. Add a host:

```
(config)> add service dns host end
(config service dns host 0)>
```

    b. Set the IP address of the host:

```
(config service dns host 0)> address ip-addr
(config service dns host 0)>
```

    c. Set the host name:

```
(config service dns host 0)> name host-name
(config service dns host 0)>
```

11. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show DNS server

You can display status for DNS servers. This command is available only at the Admin CLI.

Command line

Show DNS information

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show dns command at the system prompt:

```
> show dns

Interface  Label  Server                  Domain
---------  -----  ----------------------  ------
eth1              192.168.3.1
eth1              fd00:2704::1
eth1              fe80::227:4ff:fe2b:ae12
eth1              fe80::227:4ff:fe44:105b
eth1              fe80::240:ffff:fe80:23b0

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for remotely managing and monitoring network devices. Network administrators can use the SNMP architecture to manage nodes, including servers, workstations, routers, switches, hubs, and other equipment on an IP network, manage network performance, find and solve network problems, and plan for network growth.

The IX10 device supports both SNMPv3 and SNMPv2c in read-only mode. Both are disabled by default. SNMPv1 is not supported.

SNMP Security

By default, the IX10 device automatically blocks SNMP packets from being received over WAN and LAN interfaces. As a result, if you want a IX10 device to receive SNMP packets, you must configure the SNMP access control list to allow the device to receive the packets. See Configure Simple Network Management Protocol (SNMP).

Standard and custom Management Information Bases (MIB)

The standard MIB defines the properties and access permissions for various managed objects so that you can query standard information about a device, like *system contact* or *system location* via SNMP monitoring. The custom MIB defines the unique properties and access permissions not found in the standard MIB. To view the MIB list, see Download MIBs.

Dynamic SNMP

To expose a specific device property for SNMP monitoring that is not included in the standard MIB - properties like *serial number*, *system firmware version*, *hardware model name*, and *dynamic properties* - you can query the runtime database for the property value and then add a Dynamic SNMP. The device property is added to the custom MIB.

Configure Simple Network Management Protocol (SNMP)

Required configuration items

- Enable SNMP.
- Firewall configuration using access control to allow remote connections to the SNMP agent.
- The user name and password used to connect to the SNMP agent.

Additional configuration items

- The port used by the SNMP agent.
- Authentication type (either MD5 or SHA1).
- Privacy protocol (either DES or AES128).
- Privacy passphrase, if different that the SNMP user password.
- Enable Multicast DNS (mDNS) support.

To configure the SNMP agent on your IX10 device:

Web

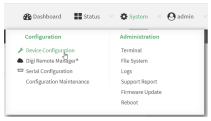
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **SNMP**.
4. Click **Enable**.
5. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's SNMP agent. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the SNMP agent.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's SNMP agent. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the SNMP agent.
     d. Click again to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click .
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click .
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
  See Firewall configuration for information about firewall zones.
  d. Click again to allow access through additional firewall zones.

6. Type the **Username** used to connect to the SNMP agent.
7. Type the **Password** used to connect to the SNMP agent.
8. (Optional) For **Port**, type the port number. The default is **161**.
9. (Optional) Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
10. (Optional) Select the **Authentication type**, either **MD5** or **SHA1**. The default is **MD5**.
11. (Optional) Type the **Privacy passphrase**. If not set, the password, entered above, is used.
12. (Optional) Select the **Privacy protocol**, either **DES** or **AES128**. The default is **DES**.
13. (Optional) Add **Dynamic SNMP Properties** to expose specific details about your device for SNMP monitoring that are not included in the standard MIB. To query the runtime database to find the device property you want to expose to SNMP, see Use digidevice runtime to access the runtime database.
    a. Click .
    b. For **Property**, type the device property (e.g., "system.cpu_temp" or "system.name").
    c. Click again to add another dynamic SNMP property.
14. (Optional) Enable read-only access to SNMP version 2c.
    a. Click **Enable version 2c access** to enable read-only access to SNMP version 2c.
    b. The **Community Name** field displays. The default name is **public**. You can change the name if needed.
15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the SNMP agent:

```
(config)> service snmp enable true
(config)>
```

4. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config)> add service snmp acl address end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the SNMP service.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

     ```
     (config)> add service snmp acl address6 end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the SNMP service.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

     ```
     (config)> add service snmp acl interface end value
     (config)>
     ```

     Where *value* is an interface defined on your device.

     Display a list of available interfaces:

     Use **... network interface ?** to display interface information:

     ```
     (config)> ... network interface ?

     Interfaces

     Additional Configuration
     ------------------------------------------
     setupip          Setup IP
     setuplinklocalip      Setup Link-local IP
     ```

```
eth             ETH
loopback        Loopback
modem           Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service snmp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

5. Set the name of the user that will be used to connect to the SNMP agent.

```
(config)> service snmp username name
(config)>
```

6. Set the password for the user that will be used to connect to the SNMP agent:

```
(config)> service snmp password pwd
(config)>
```

7. (Optional) Set the port number for the SNMP agent. The default is **161**.

```
(config)> service snmp port port
(config)>
```

8. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. For the SNMP agent, mDNS is disabled by default. To enable:

```
(config)> service snmp mdns enable true
(config>
```

9. (Optional) Set the authentication type. Allowed values are **MD5** or **SHA1**. The default is **MD5**.

```
(config)> service snmp auth_type SHA1
(config)>
```

10. (Optional) Set the privacy passphrase. If not set, the password, entered above, is used.

```
(config)> service snmp privacy pwd
(config)>
```

11. (Optional) Set the privacy protocol, either **DES** or **AES128**. The default is **DES**.

```
(config)> service snmp privacy_protocol AES128
(config)>
```

12. (Optional) Add **Dynamic SNMP Properties** to expose specific details about your device for SNMP monitoring that are not included in the standard MIB.

```
(config) service snmp runt> add end value
(config)>
```

Where *value* can be any element in the runtime table you want to expose to SNMP monitoring (for example, "system.cpu_temp" or "system.name").

13. (Optional) Enable read-only access to to SNMP version 2c.

```
(config)> service snmp enable 2c true
(config)>
```

The community name is set to **public** by default. You can change it if desired.

```
(config)> service snmp community_name <name>
(config)>
```

Where *name* is the new community name.

14. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

15. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Download MIBs

This procedure is available from the WebUI only.

Required configuration items

- Enable SNMP.

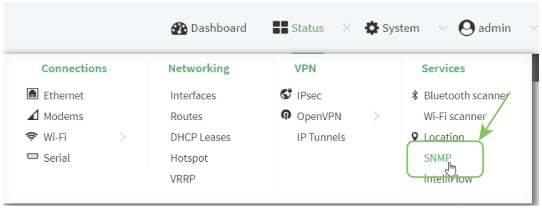
To download a .zip archive of the SNMP MIBs supported by this device:

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. Enable SNMP.

   See Configure Simple Network Management Protocol (SNMP) for information about enabling and configuring SNMP support on the IX10 device.
3. On the main menu, click **Status**. Under **Services**, click **SNMP**.

   Note If you have recently enabled SNMP and the SNMP option is not visible, refresh your browser.



   The **SNMP** page is displayed.

4. Click **Download**.

Location information

Your IX10 device can be configured to use the following location sources:

- The modem's internal Global Navigation Satellite System (GNSS) module that provides information about the current location of the device.
- User-defined static location.
- Location messages forwarded to the device from other location-enabled devices.

You can also configure your IX10 device to forward location messages, either from the IX10 device or from external sources, to a remote host. Additionally, the device can be configured to use a geofence, to allow you to determine actions that will be taken based on the physical location of the device.

This section contains the following topics:

Enable modem GNSS support 545
Configure the device to use a user-defined static location 547
Configure the device to accept location messages from external sources 549
Forward location information to a remote host 551
Configure geofencing 558
Show location information 569

Enable modem GNSS support

Web

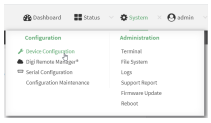
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

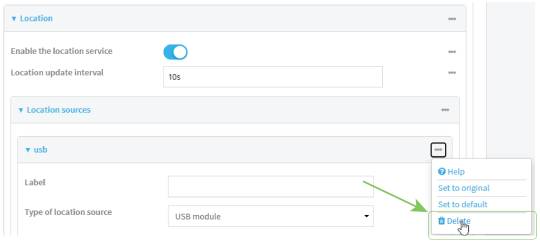
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Location** > **Location sources** > **modem**.
4. (Optional) Type a **Label** for the Modem GNSS location source.
5. For **Type of location source**, leave the selection at **Modem GNSS**.
6. Click **Enable the location source** to disable the GNSS receiver, or to enable it if it has been disabled.
7. Alternatively, you can also delete the **modem** location source:
   a. Click the menu icon (**...**) next to the **modem** location source.
   b. Click **Delete**.



8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable or disable the modem GNSS module:

   a. Use the show command to determine the index number of the modem GNSS location source:

```
(config)> show service location source
0
    enable true
    no label
    type modem
(config)>
```

   b. Use the index number to enable or disable the module:

   - To enable the module:

```
(config)> service location source 0 enable true
(config)>
```

   - To disable the module:

```
(config)> service location source 0 enable false
(config)>
```

   Alternatively, you can use the index number to delete the USB location source:

```
(config)> del service location 0
(config)>
```

4. (Optional) Set a label for this location source:

```
(config)> service location source 0 label "label"
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the device to use a user-defined static location

You can configured your IX10 device to use a user-defined static location.

Web

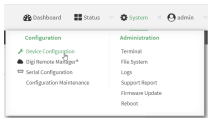
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Location** > **Location sources**.
4. Click to add a location source.
5. (Optional) Type a **Label** for this location source.
6. For **Type of location source**, select **User-defined location**.
7. The location source is enabled by default. Click **Enable the location source** to disable the location source, or to enable it if it has been disabled.
8. For **Latitude**, type the latitude of the device. Allowed values are **-90** and **90**, with up to six decimal places.
9. For **Longitude**, type the longitude of the device. Allowed values are **-180** and **180**, with up to six decimal places.
10. For **Altitude**, type the altitude of the device. Allowed values are an integer followed by **m** or **km**, for example, **100m** or **1km**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a location source:

```
(config)> add service location source end
(config service location source )>
```

The location source is enabled by default. To disable:

```
(config service location source )> enable false
(config service location source )>
```

4. (Optional) Set a label for this location source:

```
(config service location source )> label "label"
(config)>
```

5. Set the **type** of location source to **user_defined**:

```
(config service location source )> type user_defined
(config service location source )>
```

6. Set the latitude of the device:

```
(config service location source  coordinates latitude int
(config service location source )>
```

where *int* is any integer between **-90** and **90**, with up to six decimal places.

7. Set the longitude of the device:

```
(config service location source  coordinates longitude int
(config service location source )>
```

where *int* is any integer between **-180** and **180**, with up to six decimal places.

8. Set the altitude of the device:

```
(config service location source  coordinates altitude alt
(config service location source )>
```

Where *alt* is an integer followed by **m** or **km**, for example, **100m** or **1km**.

9. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the device to accept location messages from external sources

You can configure the IX10 device to accept NMEA and TAIP messages from external sources. For example, location-enabled devices connected to the IX10 device can forward their location information to the device, and then the IX10 device can serve as a central repository for this location information and forward it to a remote host. See Forward location information to a remote host for information about configuring the IX10 device to forward location messages.

This procedure configures a UDP port on the IX10 device that will be used to listen for incoming messages.

Required configuration items

- The location server must be enabled.
- UDP port that the IX10 device will listen to for incoming location messages.
- Access control list configuration to provide access to the port through the firewall.

To configure the device to accept location messages from external sources:

Web

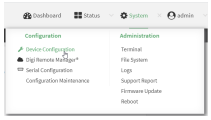
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Location** > **Location sources**.
4. Click to add a location source.
5. (Optional) Type a **Label** for this location source.
6. For **Type of location source**, select **Server**.
7. For **Location server port**, type the number of the UDP port that will receive incoming location messages.
8. Click **Access control list** to configure access control:

- To limit access to specified IPv4 addresses and networks:
  a. Click **IPv4 Addresses**.
  b. For **Add Address**, click .
  c. For **Address**, enter the IPv4 address or network that can access the device's location server UDP port. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the location server UDP port.
  d. Click again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click .
  c. For **Address**, enter the IPv6 address or network that can access the device's location server UDP port. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the location server UDP port.
  d. Click again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click .
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click .
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click again to allow access through additional firewall zones.

9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a location source:

```
(config)> add service location source end
(config service location source )>
```

4. (Optional) Set a label for this location source:

```
(config service location source )> label "label"
(config service location source )>
```

5. Set the **type** of location source to **server**:

```
(config service location source )> type server
(config service location source )>
```

6. Set the UDP port that will receive incoming location messages.

```
(config service location source )> server port port
(config service location source )>
```

7. Click **Access control list** to configure access control:
8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

2. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Forward location information to a remote host

You can configure location clients on the IX10 device that forward location messages in either NMEA or TAIP format to a remote host.

Required configuration items

- Enable the location service.
- The hostname or IP address of the remote host to which the location messages will be forwarded.
- The communication protocol, either TCP or UDP.
- The destination port on the remote host to which the messages will be forwarded.
- Message protocol type of the messages being forwarded, either NMEA or TAIP.

Additional configuration items

- Additional remote hosts to which the location messages will be forwarded.
- Location update interval, which determines how often the device will forward location information to the remote hosts.
- A description of the remote hosts.
- Specific types of NMEA or TAIP messages that should be forwarded.

- If the message protocol is NMEA, configure a talker ID to be used for all messages.
- Text that will be prepended to the forwarded message.
- A vehicle ID that is used in the TAIP ID message and can also be prepended to the forwarded message.

Configure the IX10 device to forward location information:

Web

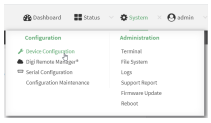
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Location** > **Destination servers**.
4. For **Add destination server**, click .
5. (Optional) For **Label**, type a description of the location destination server.
6. For **Destination server**, enter the hostname or IP address of the remote host to which location messages will be sent.
7. For **Destination server port**, enter the UDP or TCP port on the remote host to which location messages will be sent.
8. For **Communication protocol**, select either **UDP** or **TCP**.
9. For **Forward interval multiplier**, select the number of **Location update intervals** to wait before forwarding location data to this server. See Configure the location service for more information about setting the **Location update interval**.
10. For **NMEA filters**, select the filters that represent the types of messages that will be forwarded. By default, all message types are forwarded.
    - To remove a filter:
      a. Click the down arrow (⩤) next to the appropriate message type.
      b. Click **Delete**.

- To add a message type:
  a. For **Add NMEA filter** or **Add TAIP filter**, click .
  b. Select the filter type. Allowed values are:
     - **GGA**: Reports time, position, and fix related data.
     - **GLL**: Reports position data: position fix, time of position fix, and status.
     - **GSA**: Reports GPS DOP and active satellites.
     - **GSV**: Reports the number of SVs in view, PRN, elevation, azimuth, and SNR.
     - **RMC**: Reports position, velocity, and time.
     - **VTG**: Reports direction and speed over ground.

11. For **TAIP filters**, select the filters that represent the types of messages that will be forwarded. By default, all message types are forwarded.
    - To remove a filter:
      a. Click the down arrow () next to the appropriate message type.
      b. Click **Delete**.
    - To add a message type:
      a. For **Add NMEA filter** or **Add TAIP filter**, click .
      b. Select the filter type. Allowed values are:
         - **AL**: Reports altitude and vertical velocity.
         - **CP**: Compact position: reports time, latitude, and longitude.
         - **ID**: Reports the vehicle ID.
         - **LN**: Long navigation: reports the latitude, longitude, and altitude, the horizontal and vertical speed, and heading.
         - **PV**: Position/velocity: reports the latitude, longitude, and heading.
12. For **Outgoing message type**, select either **NMEA** or **TAIP** for the type of message that the device will forward to a remote host.

    (Optional) If **NMEA** is selected:

    a. Select a **Talker ID**.

       The talker ID is a two-character prefix in the NMEA message that identifies the source type. The talker ID set here will override the talker ID from all sources, and all forwarded sentences will use the configured ID. The default setting is **Default**, which means that the talker ID provided by the source will be used.

    b. Determine the **Behavior when fix is invalid**:
       - **None**: No messages are sent.
       - **Empty**: Send messages with empty fields.
       - **Last fix**: Send messages with information from the last valid fix.
13. (Optional) For **Prepend text**, enter text to prepend to the forwarded message. Two variables can be included in the prepended text:
    - **%s**: Includes the IX10 device's serial number in the prepended text.
    - **%v**: Includes the vehicle ID in the prepended text.

    For example, to include both the device's serial number and vehicle ID in the prepend message, you can enter the following in the **Prepend** field:

```
__|%s|__|%v|__
```

14. Type a four-digit alphanumeric **Vehicle ID** that will be included with to location messages. If no vehicle ID is configured, this setting defaults to 0000.
15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a remote host to which location messages will be sent:

```
(config)> add service location forward end
(config service location forward 0)>
```

4. Set the hostname or IP address of the remote host to which location messages will be sent:

```
(config service location forward 0)> server host
(config service location forward 0)>
```

5. Set the communication protocol to either **upd** or **tcp**:

```
(config service location forward 0)> protocol protocol
(config service location forward 0)>
```

6. Set the TCP or UDP port on the remote host to which location messages will be sent:

```
(config service location forward 0)> server_port 8000
(config service location forward 0)>
```

7. Set the number of **Location update intervals** to wait before forwarding location data to this server. See Configure the location service for more information about setting the **Location update interval**.

```
(config service location forward 0)> interval_multiplier int
(config service location forward 0)>
```

8. Set the protocol type for the messages. Allowed values are **taip** or **nmea**; the default is **taip**:

```
(config service location forward 0)> type nmea
(config service location forward 0)>
```

   (Optional) If the protocol type is set to **nmea**:

   a. Configure a **Talker ID**.

The talker ID is a two-character prefix in the NMEA message that identifies the source type. The talker ID set here will override the talker ID from all sources, and all forwarded sentences will use the configured ID.

i. Use the **?** to determine available talker IDs:

```
(config service location forward 0)> talker_id ?

Talker ID: Setting a talker ID will override the talker ID from all remote
sources, and all forwarded sentences from remote sources will use the configured
ID.
Format:
  Default
  GA
  GB
  GI
  GL
  GN
  GP
  GQ
Default value: Default
Current value: Default

(config service location forward 0)>
```

ii. Set the talker ID:

```
(config service location forward 0)> talker_id value
(config service location forward 0)>
```

The default setting is **Default**, which means that the talker ID provided by the source will be used.

b. Determine the behavior when fix is invalid:

```
(config service location forward 0)> no_fix value
(config service location forward 0)>
```

where *value* is one of:

- **none**: No messages are sent.
- **empty**: Send messages with empty fields.
- **last_fix**: Send messages with information from the last valid fix.

The default is **empty**.

9. (Optional) Set the text to prepend to the forwarded message. Two variables can be included in the prepended text:
   - **%s**: Includes the IX10 device's serial number in the prepended text.
   - **%v**: Includes the vehicle ID in the prepended text.

```
(config service location forward 0)> prepend __|%s|__|%v|__
(config service location forward 0)>
```

10. (Optional) Set the vehicle ID.

Allowed value is a four digit alphanumerical string (for example, 01A3 or 1234). If no vehicle ID is configured, this setting defaults to 0000.

```
(config service location forward 0)> vehicle-id 1234
(config service location forward 0)>
```

11. (Optional) Provide a description of the remote host:

```
(config service location forward 0)> label "Remote host 1"
(config service location forward 0)>
```

12. (Optional) Specify types of messages that will be forwarded. Allowed values vary depending on the message protocol type. By default, all message types are forwarded.
    - If the message protocol type is NMEA:

      Allowed values are:

      - **gga**: Reports time, position, and fix related data.
      - **gll**: Reports position data: position fix, time of position fix, and status.
      - **gsa**: Reports GPS DOP and active satellites.
      - **gsv**: Reports the number of SVs in view, PRN, elevation, azimuth, and SNR.
      - **rmc**: Reports position, velocity, and time.
      - **vtg**: Reports direction and speed over ground.

      To remove a message type:

      a. Use the **show** command to determine the index number of the message type to be deleted:

      ```
      (config service location forward 0)> show filter_nmea
      0 gga
      1 gll
      2 gsa
      3 gsv
      4 rmc
      5 vtg
      (config service location forward 0)>
      ```

      b. Use the index number to delete the message type. For example, to delete the **gsa** (index number 2) message type:

      ```
      (config service location forward 0)> del filter_nmea 2
      (config service location forward 0)>
      ```

      To add a message type:

      a. Change to the **filter_nmea** node:

      ```
      (config service location forward 0)> filter_nmea
      (config service location forward 0 filter_nmea)>
      ```

      b. Use the **add** command to add the message type. For example, to add the **gsa** message type:

```
(config service location forward 0 filter_nmea)> add gsa end
(config service location forward 0 filter_nmea)>
```

- If the message protocol type is TAIP:

  Allowed values are:

  - **al**: Reports altitude and vertical velocity.
  - **cp**: Compact position: reports time, latitude, and longitude.
  - **id**: Reports the vehicle ID.
  - **ln**: Long navigation: reports the latitude, longitude, and altitude, the horizontal and vertical speed, and heading.
  - **pv**: Position/velocity: reports the latitude, longitude, and heading.

  To remove a message type:

  a. Use the **show** command to determine the index number of the message type to be deleted:

  ```
  (config service location forward 0)> show filter_taip
  0 al
  1 cp
  2 id
  3 ln
  4 pv
  (config service location forward 0)>
  ```

  b. Use the index number to delete the message type. For example, to delete the **id** (index number 2) message type:

  ```
  (config service location forward 0)> del filter_taip 2
  (config service location forward 0)>
  ```

  To add a message type:

  a. Change to the **filter_taip** node:

  ```
  (config service location forward 0)> filter_taip
  (config service location forward 0 filter_taip)>
  ```

  b. Use the **add** command to add the message type. For example, to add the **id** message type:

  ```
  (config service location forward 0 filter_taip)> add id end
  (config service location forward 0 filter_taip)>
  ```

13. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

14. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure geofencing

Geofencing is a mechanism to create a virtual perimeter that allows you configure your IX10 device to perform actions when entering or exiting the perimeter. For example, you can configure a device to factory default if its location service indicates that it has been moved outside of the geofence.

Multiple geofences can be defined for one device, allowing for a complex configuration in which different actions are taken depending on the physical location of the device.

Required configuration items

- Location services must be enabled.
- The geofence must be enabled.
- The boundary type of the geofence, either circular or polygonal.
  - If boundary type is circular, the latitude and longitude of the center point of the circle, and the radius.
  - If boundary type is polygonal, the latitude and longitude of the polygon's vertices (a vertex is the point at which two sides of a polygon meet). Three vertices will create a triangular polygon; four will create a square, etc. Complex polygons can be defined.
- Actions that will be taken when the device's location triggers a geofence event. You can define actions for two types of events:
  - Actions taken when the device enters the boundary of the geofence, or is inside the boundary when the device boots.
  - Actions taken when the device exits the boundary of the geofence, or is outside the boundary when the device boots.

  For each event type:
  - Determine if the action(s) associated with the event type should be performed when the device boots inside or outside of the geofence boundary.
  - The number of update intervals that should take place before the action(s) are taken.

  Multiple actions can be configured for each type of event. For each action:
  - The type of action, either a factory erase or executing a custom script.
  - If a custom script is used:
    - The script that will be executed.
    - Whether to log output and errors from the script.
    - The maximum memory that the script will have available.
    - Whether the script should be executed within a sandbox that will prevent the script from affecting the system itself.

Additional configuration items

- Update interval, which determines the amount of time that the geofence should wait between polling for updated location data.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

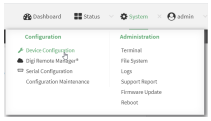
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

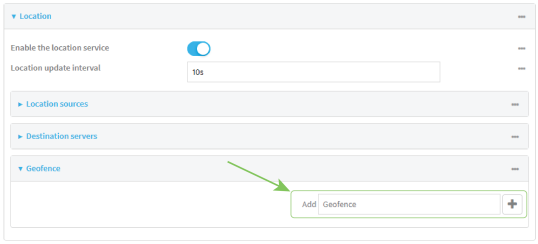
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **Services** > **Location** > **Geofence**.
4. For **Add Geofence**, type a name for the geofence and click .

   The geofence is enabled by default. To disable, toggle off **Enable**.

5. For **Update interval**, type the amount of time that the geofence should wait between polling for updated location data. The default is one minute.

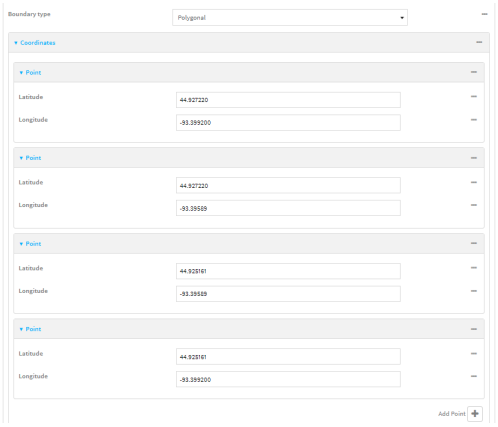
   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Update interval** to ten minutes, enter **10m** or **600s**.

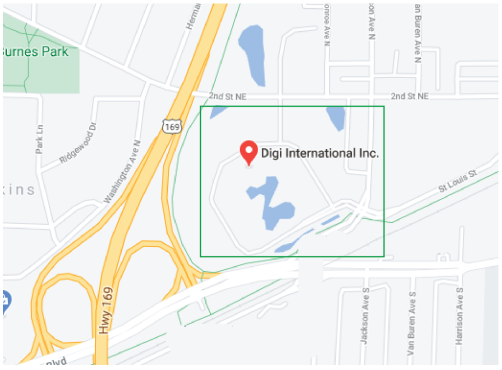
6. For **Boundary type**, select the type of boundary that the geofence will have.
   - If **Circular** is selected:
     a. Click to expand **Center**.
     b. Type the **Latitude** and **Longitude** of the center point of the circle. Allowed values are:
        - For **Latitude**, any integer between **-90** and **90**, with up to six decimal places.
        - For **Longitude**, any integer between **-180** and **180**, with up to six decimal places.
     c. For **Radius**, type the radius of the circle. Allowed values are an integer followed by **m** or **km**, for example, **100m** or **1km**.

- If **Polygonal** is selected:
  a. Click to expand **Coordinates**.
  b. Click to add a point that represents a vertex of the polygon. A vertex is the point at which two sides of a polygon meet.
  c. Type the **Latitude** and **Longitude** of one of the vertices of the polygon. Allowed values are:
     - For **Latitude**, any integer between **-90** and **90**, with up to six decimal places.
     - For **Longitude**, any integer between **-180** and **180**, with up to six decimal places.
  d. Click again to add an additional point, and continue adding points to create the desired polygon.

  For example, to configure a square polygon around the Digi headquarters, configure a polygon with four points:



  This defines a square-shaped polygon equivalent to the following:



7. Define actions to be taken when the device's location triggers a geofence event:
   - To define actions that will be taken when the device enters the geofence, or is inside the geofence when it boots:

a. Click to expand **On entry**.

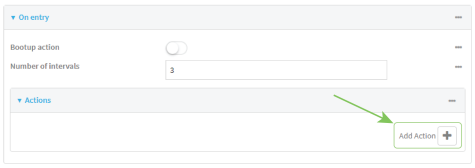
b. (Optional) Enable **Bootup action** to configure the device to perform the **On entry** actions if the device is inside the geofence when it boots.

c. For **Number of intervals**, type or select the number of **Update Intervals** that must take place prior to performing the **On entry** actions.

For example, if the **Update interval** is **1m** (one minute) and the **Number of intervals** is **3**, the **On entry** actions will not be performed until the device has been inside the geofence for three minutes.

d. Click to expand **Actions**.

e. Click to create a new action.



f. For Action type, select either:

- **Factory erase** to erase the device configuration when the action is triggered.
- **Custom script** to execute a custom script when the action is triggered.

If **Custom script** is selected:

i. Click to expand **Custom script**.

ii. For **Commands**, type the script that will be executed when the action is triggered. If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

iii. Enable **Log script output** to log the output of the script to the system log.

iv. Enable **Log script errors** to log errors from the script to the system log.

v. (Optional) For **Maximum memory**, type the maximum amount of system memory that will be available for the script and it spawned processes.

Allowed values are any integer followed by one of the following: **b|bytes|KB|k|MB|M|GB|G|TB|T**.

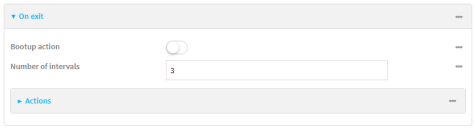
For example. the allocate one megabyte of memory to the script and its spawned processes, type **1MB** or **1M**.

vi. **Sandbox** is enabled by default. This prevents the script from adversely affecting the system. If you disable **Sandbox**, the script may render the system unusable.

vii. Repeat for any additional actions.

- To define actions that will be taken when the device exits the geofence, or is outside the geofence when it boots:

a. Click to expand **On exit**.



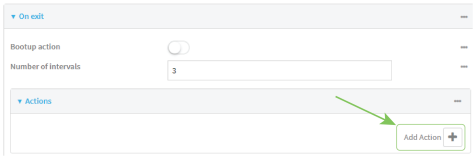
b. (Optional) Enable **Bootup action** to configure the device to perform the **On exit** actions if the device is inside the geofence when it boots.

c. For **Number of intervals**, type or select the number of **Update Intervals** that must take place prior to performing the **On exit** actions.

For example, if the **Update interval** is **1m** (one minute) and the **Number of intervals** is **3**, the **On entry** actions will not be performed until the device has been inside the geofence for three minutes.

d. Click to expand **Actions**.

e. Click to create a new action.



f. For Action type, select either:

- **Factory erase** to erase the device configuration when the action is triggered.
- **Custom script** to execute a custom script when the action is triggered.

If **Custom script** is selected:

i. Click to expand **Custom script**.

ii. For **Commands**, type the script that will be executed when the action is triggered. If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

iii. Enable **Log script output** to log the output of the script to the system log.

iv. Enable **Log script errors** to log errors from the script to the system log.

v. (Optional) For **Maximum memory**, type the maximum amount of system memory that will be available for the script and it spawned processes.

Allowed values are any integer followed by one of the following: **b|bytes|KB|k|MB|M|GB|G|TB|T**.

For example. the allocate one megabyte of memory to the script and its spawned processes, type **1MB** or **1M**.

vi. **Sandbox** is enabled by default. This prevents the script from adversely affecting the system. If you disable **Sandbox**, the script may render the system unusable.

vii. Repeat for any additional actions.

8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```

3. Add a geofence:

   ```
   (config)> add service location geofence name
   (config service location geofence name)>
   ```

   where *name* is a name for the geofence. For example:

   ```
   (config)> add service location geofence test_geofence
   (config service location geofence test_geofence)>
   ```

   The geofence is enabled by default. To disable:

   ```
   (config service location geofence test_geofence)> enable false
   (config service location geofence test_geofence)>
   ```

4. Set the amount of time that the geofence should wait between polling for updated location data:

   ```
   (config service location geofence test_geofence)> update_interval value
   (config service location geofence test_geofence)>
   ```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **update_interval** to ten minutes, enter either **10m** or **600s**:

   ```
   (config service location geofence test_geofence)> update_interval 600s
   (config service location geofence test_geofence)>
   ```

   The default is **1m** (one minute).

5. Set the boundary type for the geofence:

   ```
   (config service location geofence test_geofence)> boundary value
   (config service location geofence test_geofence)>
   ```

   where *value* is either **circular** or **polygonal**.

   - If **boundary** is set to **circular** :

     a. Set the latitude and longitude of the center point of the circle:

     ```
     (config service location geofence test_geofence)> center latitude int
     (config service location geofence test_geofence)> center longitude int
     (config service location geofence test_geofence)>
     ```

     where *int* is:

- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

b. Set the radius of the circle:

```
(config service location geofence test_geofence)> radius radius
(config service location geofence test_geofence)>
```

where *radius* is an integer followed by **m** or **km**, for example, **100m** or **1km**.

- If **boundary** is set to **polygonal**:

a. Set the coordinates of one vertex of the polygon. A vertex is the point at which two sides of a polygon meet.

i. Add a vertex:

```
(config service location geofence test_geofence)> add coordinates end
(config service location geofence test_geofence coordinates 0)>
```

ii. Set the latitude and longitude of the vertex:

```
(config service location geofence test_geofence coordinates 0)> latitude int
(config service location geofence test_geofence coordinates 0)> longitude int
(config service location geofence test_geofence coordinates 0)>
```

where *int* is:

- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

iii. Configure additional vortices:

```
(config service location geofence test_geofence coordinates 0)> ..
(config service location geofence test_geofence coordinates)> add end
(config service location geofence test_geofence coordinates 1)> latitude int
(config service location geofence test_geofence coordinates 1)> longitude int
(config service location geofence test_geofence coordinates 1)>
```

where *int* is:

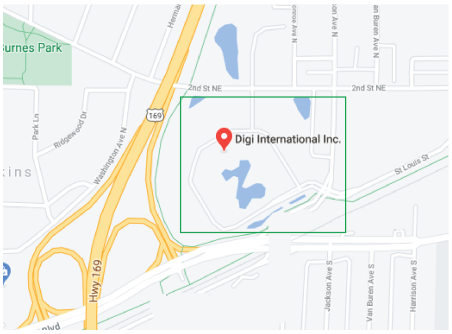
- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

Repeat for each vortex of the polygon.
For example, to configure a square polygon around the Digi headquarters, configure a polygon with four points:

```
(config service location geofence test_geofence)> add coordinates end
(config service location geofence test_geofence coordinates 0)> latitude 44.927220
```

```
(config service location geofence test_geofence coordinates 0)> longitude -
93.399200
(config service location geofence test_geofence coordinates 0)> ..
(config service location geofence test_geofence coordinates)> add end
(config service location geofence test_geofence coordinates 1)> latitude 44.927220
(config service location geofence test_geofence coordinates 1)> longitude -
93.39589
(config service location geofence test_geofence coordinates 1)> ..
(config service location geofence test_geofence coordinates)> add end
(config service location geofence test_geofence coordinates 2)> latitude 44.925161
(config service location geofence test_geofence coordinates 2)> longitude -
93.39589
(config service location geofence test_geofence coordinates 2)> ..
(config service location geofence test_geofence coordinates)> add end
(config service location geofence test_geofence coordinates 3)> latitude 44.925161
(config service location geofence test_geofence coordinates 3)> longitude -
93.399200
(config service location geofence test_geofence coordinates 3)>
```

This defines a square-shaped polygon equivalent to the following:



6. Define actions to be taken when the device's location triggers a geofence event:
   - To define actions that will be taken when the device enters the geofence, or is inside the geofence when it boots:
     a. (Optional) Configure the device to preform the actions if the device is inside the geofence when it boots:

```
(config)> service location geofence test_geofence on_entry bootup true
(config)>
```

     b. Set the number of update_intervals that must take place prior to performing the actions:

```
(config)> service location geofence test_geofence on_entry num_intervals int
(config)>
```

        For example, if the update interval is **1m** (one minute) and the **num_intervals** is set to **3**, the actions will not be performed until the device has been inside the geofence for three minutes.

     c. Add an action:

i. Type **...** to return to the root of the configuration:

```
(config service location geofence test_geofence coordinates 3)> ...
(config)>
```

ii. Add the action:

```
(config)> add service location geofence test_geofence on_entry action end
(config service location geofence test_geofence on_entry action 0)>
```

d. Set the type of action:

```
(config service location geofence test_geofence on_entry action 0)> type value
(config service location geofence test_geofence on_entry action 0)>
```

where *value* is either:

- **factory_erase**—Erases the device configuration when the action is triggered.
- **script**—Executes a custom script when the action is triggered.

factory_erase or **script**.

If **type** is set to **script**:

i. Type or paste the script, closed in quote marks:

```
(config service location geofence test_geofence on_entry action 0)> commands
"script"
(config service location geofence test_geofence on_entry action 0)>
```

If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

ii. To log the output of the script to the system log:

```
(config service location geofence test_geofence on_entry action 0)> syslog_stdout
true
(config service location geofence test_geofence on_entry action 0)>
```

iii. To log the errors from the script to the system log:

```
(config service location geofence test_geofence on_entry action 0)> syslog_stderr
true
(config service location geofence test_geofence on_entry action 0)>
```

iv. (Optional) Set the maximum amount of system memory that will be available for the script and it spawned processes:

```
(config service location geofence test_geofence on_entry action 0)> max_memory
value
(config service location geofence test_geofence on_entry action 0)>
```

where *value* is any integer followed by one of the following: **b|bytes|KB|k|MB|M|GB|G|TB|T**.

For example. the allocate one megabyte of memory to the script and its spawned processes:

```
(config service location geofence test_geofence on_entry action 0)> max_memory
1MB
(config service location geofence test_geofence on_entry action 0)>
```

v. A sandbox is enabled by default to prevent the script from adversely affecting the system. To disable the sandbox:

```
(config service location geofence test_geofence on_entry action 0)> sandbox false
(config service location geofence test_geofence on_entry action 0)>
```

If you disable the sandbox, the script may render the system unusable.

vi. Repeat for any additional actions.

- To define actions that will be taken when the device exits the geofence, or is outside the geofence when it boots:

a. (Optional) Configure the device to preform the actions if the device is outside the geofence when it boots:

```
(config)> service location geofence test_geofence on_exit bootup true
(config)>
```

b. Set the number of update_intervals that must take place prior to performing the actions:

```
(config)> service location geofence test_geofence on_exit num_intervals int
(config)>
```

For example, if the update interval is **1m** (one minute) and the **num_intervals** is set to **3**, the actions will not be performed until the device has been outside the geofence for three minutes.

c. Add an action:

i. Type **...** to return to the root of the configuration:

```
(config service location geofence test_geofence coordinates 3)> ...
(config)>
```

ii. Add the action:

```
(config)> add service location geofence test_geofence on_exit action end
(config service location geofence test_geofence on_exit action 0)>
```

d. Set the type of action:

```
(config service location geofence test_geofence on_exit action 0)> type value
(config service location geofence test_geofence on_exit action 0)>
```

where *value* is either:

- **factory_erase**—Erases the device configuration when the action is triggered.
- **script**—Executes a custom script when the action is triggered.

factory_erase or **script**.

If **type** is set to **script**:

i. Type or paste the script, closed in quote marks:

```
(config service location geofence test_geofence on_exit action 0)> commands
"script"
(config service location geofence test_geofence on_exit action 0)>
```

If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

ii. To log the output of the script to the system log:

```
(config service location geofence test_geofence on_exit action 0)> syslog_stdout
true
(config service location geofence test_geofence on_exit action 0)>
```

iii. To log the errors from the script to the system log:

```
(config service location geofence test_geofence on_exit action 0)> syslog_stderr
true
(config service location geofence test_geofence on_exit action 0)>
```

iv. (Optional) Set the maximum amount of system memory that will be available for the script and it spawned processes:

```
(config service location geofence test_geofence on_exit action 0)> max_memory
value
(config service location geofence test_geofence on_exit action 0)>
```

where *value* is any integer followed by one of the following: **b|bytes|KB|k|MB|M|GB|G|TB|T**.

For example. the allocate one megabyte of memory to the script and its spawned processes:

```
(config service location geofence test_geofence on_exit action 0)> max_memory
1MB
(config service location geofence test_geofence on_exit action 0)>
```

v. A sandbox is enabled by default to prevent the script from adversely affecting the system. To disable the sandbox:

```
(config service location geofence test_geofence on_exit action 0)> sandbox false
(config service location geofence test_geofence on_exit action 0)>
```

If you disable the sandbox, the script may render the system unusable.

vi. Repeat for any additional actions.

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show location information

You can view status and statistics about location information from either the WebUI or the command line.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.
2. Under **Services**, click **Location**.

   The device's current location is displayed, along with the status of any configured geofences.

Command line

Show location information

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show location command at the system prompt:

```
> show location

Location Status
---------------
State          : enabled
Source          : 192.168.2.3
Latitude        : 44* 55' 14.809" N (44.92078)
Longitude       : 93* 24' 47.262" w (-93.413128)
Altitude        : 279 meters
Velocity        : 0 meters per second
Direction       : None
Quality         : Standard GNSS (2D/3D)
UTC Date and Time : Fri, Jan 12, 2024 12:10:00 03
No. of Satellites : 7

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show geofence information

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show location geofence command at the system prompt:

```
> show location geofence

Geofence      Status  State   Transitions  Last Transition
------------- ------ ------ ----------- ---------------
test_geofence  Up     Inside  0

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Modbus gateway

The IX10 supports the ability to function as a Modbus gateway, to provide serial-to-Ethernet connectivity to Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and other industrial devices. MODBUS provides client/server communication between devices connected on different types of buses and networks, and the Modbus gateway allows for communication between buses and networks that use the Modbus protocol.

This section contains the following topics:

Configure the Modbus gateway 571
Modbus hardening 584
Show Modbus gateway status and statistics 585

Configure the Modbus gateway

Required configuration items

- Server configuration:
  - Enable the server.
  - Connection type, either socket or serial.
    - If the connection type is socket, the IP protocol to be used.
    - If the connection type is serial, the serial port to be used.
- Client configuration:
  - Enable the client.
  - Connection type, either socket or serial.
    - If the connection type is socket:
      - The IP protocol to be used.
      - The hostname or IPv4 address of the remote host on which the Modbus server is running.
    - If the connection type is serial:
      - The serial port to be used.
  - Modbus address or addresses to determine if messages should be forwarded to a destination device.

Additional configuration items

- Server configuration:
  - The packet mode.
  - The maximum time between bytes in a packet.
  - If the connection type is set to socket:
    - The port to use.
    - The inactivity timeout.
    - Access control list.
  - If the connection type is set to serial:
    - Whether to use half duplex (two wire) mode.
- Client configuration:
  - The packet mode.
  - The maximum time between bytes in a packets.
  - Whether to send broadcast messages.
  - Response timeout
  - If connection type is set to socket:
    - The port to use.
    - The inactivity timeout.
  - If connection type is set to serial:
    - Whether to use half duplex (two wire) mode.

- Whether packets should be delivered to a fixed Modbus address.
- Whether packets should have their Modbus address adjusted downward before to delivery.

Web

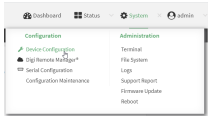
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

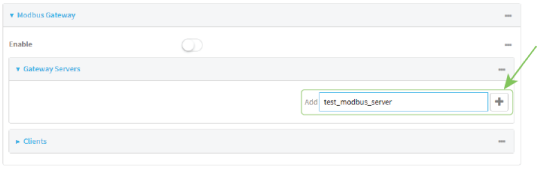
   

   The **Configuration** window is displayed.
3. Click **Services** > **Modbus Gateway**.

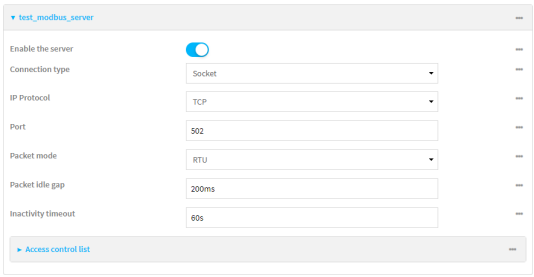
4. Click **Enable** to enable the gateway.
5. Click **Debug** to allow verbose logging in the system log.

Configure gateway servers

1. Click to expand **Gateway Servers**.
2. For **Add Modbus server**, type a name for the server and click .

   The new Modbus gateway server configuration is displayed.



3. The new Modbus gateway server is enabled by default. Toggle off **Enable the server** to disable.
4. For **Connection type**, select **Socket** or **Serial**. Available options in the gateway server configuration vary depending on this setting.
   - If **Socket** is selected for **Connection type**:
     a. For **IP Protocol**, select **TCP** or **UDP**. The default is **TCP**.
     b. For **Port**, enter or select an appropriate port. The default is port **502**.
   - If **Serial** is selected for **Connection type**:
     a. For **Serial port**, select the appropriate serial port on the IX10 device.
5. For **Packet mode**, select **RTU** or **RAW** (if **Connection type** is set to **Socket**) or **ASCII** (if **Connection type** is set to **Serial**) for the type of packet that will be used by this connection. The default is **RTU**.
6. For **Packet idle gap**, type the maximum allowable time between bytes in a packet.

   Allowed values are between 10 milliseconds and one second, and take the format ***number*** {**ms|s**}.

   For example, to set **Packet idle gap** to 20 milliseconds, enter **20ms**.
7. If **Connection type** is set to **Socket**, for **Inactivity timeout**, type the amount of time to wait before disconnecting the socket when it has become inactive.

   Allowed values are any number of minutes or seconds up to a maximum of 15 minutes, and take the format ***number***{**m|s**}.

   For example, to set **Inactivity timeout** to ten minutes, enter **10m** or **600s**.
8. (Optional) If **Connection type** is set to **Serial**, click **Half duplex** to enable half duplex (two wire) mode.
9. (Optional) If **Connection type** is set to **Socket**, click to expand **Access control list**:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the web administration service.
     d. Click again to list additional IP addresses or networks.

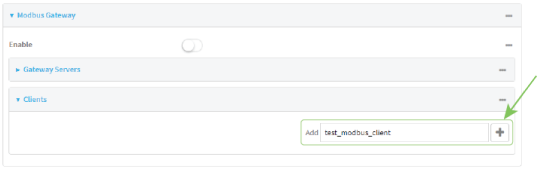
- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click ♈.
  c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the web administration service.
  d. Click ♈ again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click ♈.
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click ♈ again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click ♈.
  c. For **Zone**, select the appropriate firewall zone from the dropdown.

     See Firewall configuration for information about firewall zones.
  d. Click ♈ again to allow access through additional firewall zones.

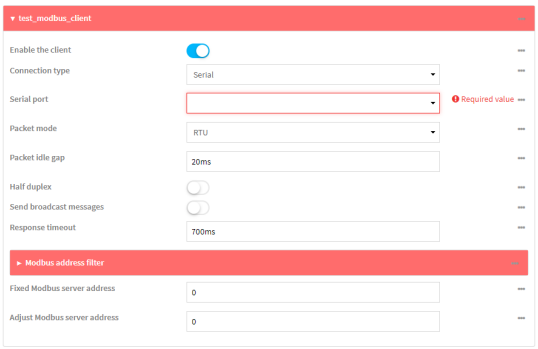
10. Repeat these steps to configure additional servers.

Configure clients

1. Click to expand **Clients**.
2. For **Add Modbus client**, type a name for the client and click ♈.



The new Modbus gateway client configuration is displayed.



3. The new Modbus gateway client is enabled by default. Toggle off **Enable the client** to disable.
4. For **Connection type**, select **Socket** or **Serial**. Available options in the gateway server configuration vary depending on this setting.
   - If **Socket** is selected for **Connection type**:
     a. For **IP Protocol**, select **TCP** or **UDP**. The default is **TCP**.
     b. For **Port**, enter or select an appropriate port. The default is port **502**.
     c. For **Remote host**, type the hostname or IP address of the remote host on which the Modbus server is running.
   - If **Serial**is selected for **Connection type**:
     a. For **Serial port**, select the appropriate serial port on the IX10 device.
5. For **Packet mode**, select **RTU** or **RAW** (if **Connection type** is set to **Socket**) or **ASCII** (if **Connection type**is set to **Serial**) for the type of packet that will be used by this connection. The default is **RTU**.
6. For **Packet idle gap**, type the maximum allowable time between bytes in a packet.

   Allowed values are between 10 milliseconds and one second, and take the format ***number*** {**ms|s**}.

   For example, to set **Packet idle gap** to 20 milliseconds, enter **20ms**.
7. If **Connection type** is set to **Socket**, for **Inactivity timeout**, type the amount of time to wait before disconnecting the socket when it has become inactive.

   Allowed values are any number of minutes or seconds up to a maximum of 15 minutes, and take the format ***number***{**m|s**}.

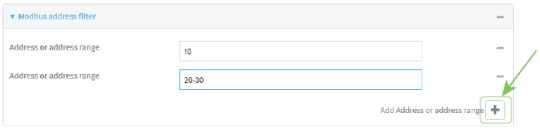
   For example, to set **Inactivity timeout** to ten minutes, enter **10m** or **600s**.
8. (Optional) If **Connection type** is set to **Serial**, click **Half duplex** to enable half duplex (two wire) mode.
9. (Optional) If **Connection type** is set to **Socket**, click to expand **Access control list**:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.

- **any**: No limit to IPv4 addresses that can access the web administration service.

d. Click to add again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click to add.
  c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the web administration service.
  d. Click to add again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click to add.
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click to add again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click to add.
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click to add again to allow access through additional firewall zones.

10. (Optional) Enable **Send broadcast messages** to configure the gateway to send broadcast messages to this client.
11. For **Response timeout**, type the maximum time to wait for a response to a message.
    Allowed values are between 1 millisecond and 700 milliseconds, and take the format ***number*ms**.
    For example, to set **Response timeout** to 100 milliseconds, enter **100ms**. The default is **700ms**.
12. Click to expand **Modbus address filter**.
    This filter is used by the gateway to determine if a message should be forwarded to a destination device. If the Modbus address in the message matches one or more of the filters, the message is forwarded. If it does not match the filters, the message is not forwarded.
13. For **Address or address range**, type a Modbus address or range of addresses. Allowed values are **1** through **255** or a hyphen-separated range.
    For example, to have this client filter for incoming messages that contain the Modbus address of 10, type **10**. To filter for all messages with addresses in the range of 20 to 30, type **20-30**.
    To add additional address filters for this client, click to add.



14. For **Fixed Modbus server address**, if request messages handled by this client should always be forwarded to a specific device, type the device's Modbus address. Leave at the default setting of **0** to allow messages that match the **Modbus address filter** to be forwarded to devices based on the Modbuss address in the message.
15. For **Adjust Modbus server address**, type a value to adjust the Modbus server address downward by the specified value prior to delivering the message. Allowed values are **0** through **255**. Leave at the default setting of **0** to not adjust the server address.

    If a packet contains a Modbus server address above the amount entered here, the address will be adjusted downward by this amount before the packet is delivered. This allows you to configure clients on the gateway that will forward messages to remote devices with the same Modbus address on different buses. For example, if there are two devices on two different buses that have the same Modbus address of 10, you can create two clients on the gateway:

    - Client one:
      - **Modbus address filter** set to **10**.

      This will configure the gateway to deliver all messages that have the Modbus server address of 10 to this device.
    - Client two:
      - **Modbus address filter** set to **20**.
      - **Adjust Modbus server address** set to **10**.

      This will configure the gateway to deliver all messages that have the Modbus server address address of 20 to the device with address 10.
16. Repeat these steps to configure additional clients.
17. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the Modbus gateway:

```
(config)> service modbus_gateway enable true
(config)>
```

4. Configure servers:
   a. Add a server:

```
(config)> add service modbus_gateway server name
(config service modbus_gateway server name)>
```

   where *name* is a name for the server, for example:

```
(config)> add service modbus_gateway server test_modbus_server
(config service modbus_gateway server test_modbus_server)>
```

   The Modbus server is enabled by default. To disable:

```
(config service modbus_gateway server test_modbus_server)> enable false
(config service modbus_gateway server test_modbus_server)>
```

   b. Set the connection type:

```
(config service modbus_gateway server test_modbus_server)> connection_type type
(config service modbus_gateway server test_modbus_server)>
```

   where *type* is either **socket** or **serial**. The default is **socket**.

   - If **connection_type** is set to **socket**:
     i. Set the IP protocol:

```
(config service modbus_gateway server test_modbus_server)> socket protocol
value
(config service modbus_gateway server test_modbus_server)>
```

     where *value* is either **tcp** or **udp**.

     ii. Set the port:

```
(config service modbus_gateway server test_modbus_server)> socket port
(config service modbus_gateway server test_modbus_server)>
```

     where *port* is an integer between **1** and **65535**. The default is **502**.

     iii. Set the packet mode:

```
(config service modbus_gateway server test_modbus_server)> socket packet_
mode value
(config service modbus_gateway server test_modbus_server)>
```

     where *value* is either **rtu** or **raw**. The default is **rtu**.

     iv. Set the maximum allowable time between bytes in a packet:

```
(config service modbus_gateway server test_modbus_server)> socket idle_gap
value
(config service modbus_gateway server test_modbus_server)>
```

     where *value* is any number between 10 milliseconds and one second, and take the format ***number*{ms|s}**.

For example, to set idle_gap to 20 milliseconds, enter **20ms**.

v. Set the amount of time to wait before disconnecting the socket when it has become inactive:

```
(config service modbus_gateway server test_modbus_server)> inactivity_timeout
value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is any number of minutes or seconds up to a maximum of 15 minutes, and takes the format ***number***{**m|s**}.

For example, to set **inactivity_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config service modbus_gateway server test_modbus_server)> inactivity_timeout
600s
(config service modbus_gateway server test_modbus_server)>
```

- If **connection_type** is set to **serial**:

  i. Set the serial port:

  i. Use the **?** to determine available serial ports:

```
(config service modbus_gateway server test_modbus_server)> ... serial port ?

Serial

  Additional Configuration
  ------------------------------------------------------------------------------
  port1              Port 1

(config service modbus_gateway server test_modbus_server)>
```

  ii. Set the port:

```
(config service modbus_gateway server test_modbus_server)> serial port
(config service modbus_gateway server test_modbus_server)>
```

  ii. Set the packet mode:

```
(config service modbus_gateway server test_modbus_server)> serial packet_mode
value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is either **rtu** or **ascii**. The default is **rtu**.

  iii. Set the maximum allowable time between bytes in a packet:

```
(config service modbus_gateway server test_modbus_server)> serial idle_gap
value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is any number between 10 milliseconds and one second, and take the format ***number*{ms|s}**.

For example, to set idle_gap to one second, enter **1000ms** or **1s**.

iv. (Optional) Enable half-duplex (two wire) mode:

```
(config service modbus_gateway server test_modbus_server)> serial half_duplex
true
(config service modbus_gateway server test_modbus_server)>
```

c. Repeat the above instructions for additional servers.

5. Configure clients:

a. Type **...** to return to the root of the configuration:

```
(config)> add service modbus_gateway server test_modbus_server)> ...
(config)>
```

b. Add a client:

```
(config)> add service modbus_gateway client name
(config service modbus_gateway client name)>
```

where *name* is a name for the client, for example:

```
(config)> add service modbus_gateway client test_modbus_client
(config service modbus_gateway client test_modbus_client)>
```

The Modbus client is enabled by default. To disable:

```
(config service modbus_gateway client test_modbus_client)> enable false
(config service modbus_gateway client test_modbus_client)>
```

c. Set the connection type:

```
(config service modbus_gateway client test_modbus_client)> connection_type type
(config service modbus_gateway client test_modbus_client)>
```

where *type* is either **socket** or **serial**. The default is **socket**.

- If **connection_type** is set to **socket**:

i. Set the IP protocol:

```
(config service modbus_gateway client test_modbus_client)> socket protocol value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is either **tcp** or **udp**.

ii. Set the port:

```
(config service modbus_gateway client test_modbus_client)> socket port
(config service modbus_gateway client test_modbus_client)>
```

where *port* is an integer between **1** and **65535**. The default is **502**.

iii. Set the packet mode:

```
(config service modbus_gateway client test_modbus_client)> socket packet_mode
value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is either **rtu** or **ascii**. The default is **rtu**.

iv. Set the maximum allowable time between bytes in a packet:

```
(config service modbus_gateway client test_modbus_client)> socket idle_gap value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is any number between 10 milliseconds and one second, and take the format ***number*{ms|s}**.

For example, to set idle_gap to 20 milliseconds, enter **20ms**.

v. Set the amount of time to wait before disconnecting the socket when it has become inactive:

```
(config service modbus_gateway client test_modbus_client)> inactivity_timeout
value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is any number of minutes or seconds up to a maximum of 15 minutes, and takes the format ***number*{m|s}**.

For example, to set **inactivity_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config service modbus_gateway client test_modbus_client)> inactivity_timeout
600s
(config service modbus_gateway client test_modbus_client)>
```

vi. Set the hostname or IP address of the remote host on which the Modbus server is running:

```
(config service modbus_gateway client test_modbus_client)> remote_host ip_
address|hostname
(config service modbus_gateway client test_modbus_client)>
```

- If **connection_type** is set to **serial**:
  i. Set the serial port:
    i. Use the **?** to determine available serial ports:

```
(config service modbus_gateway client test_modbus_client)> ... serial port ?

Serial

 Additional Configuration
 ------------------------------------------------------------------------------
port1            Port 1
```

```
(config service modbus_gateway client test_modbus_client)>
```

ii. Set the port:

```
(config service modbus_gateway client test_modbus_client)> serial port
(config service modbus_gateway client test_modbus_client)>
```

ii. Set the packet mode:

```
(config service modbus_gateway client test_modbus_client)> serial packet_mode
value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is either **rtu** or **ascii**. The default is **rtu**.

iii. Set the maximum allowable time between bytes in a packet:

```
(config service modbus_gateway client test_modbus_client)> serial idle_gap value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is any number between 10 milliseconds and one second, and take the format ***number*{ms|s}**.

For example, to set idle_gap to one second, enter **1000ms** or **1s**.

iv. (Optional) Enable half-duplex (two wire) mode:

```
(config service modbus_gateway client test_modbus_client)> serial half_duplex
true
(config service modbus_gateway client test_modbus_client)>
```

d. (Optional) Enable the gateway to send broadcast messages to this client:

```
(config service modbus_gateway client test_modbus_client)> broadcast true
(config service modbus_gateway client test_modbus_client)>
```

e. Set the maximum time to wait for a response to a message:

```
(config service modbus_gateway client test_modbus_client)> response_timeout value
(config service modbus_gateway client test_modbus_client)>
```

Allowed values are between 1 millisecond and 700 milliseconds, and take the format ***number*ms**.

For example, to set response_timeout to 100 milliseconds:

```
(config service modbus_gateway client test_modbus_client)> response_timeout 100ms
(config service modbus_gateway client test_modbus_client)>
```

The default is **700ms**.

f. Configure the address filter:

This filter is used by the gateway to determine if a message should be forwarded to a destination device. If the Modbus address in the message matches one or more of the filters, the message is forwarded. If it does not match the filters, the message is not forwarded. Allowed values are **1** through **255** or a hyphen-separated range.

For example:

- To have this client filter for incoming messages that contain the Modbus address of 10, set the index **0** entry to **10**:

```
(config service modbus_gateway client test_modbus_client)> filter 0 10
(config service modbus_gateway client test_modbus_client)>
```

- To filter for all messages with addresses in the range of 20 to 30, set the index **0** entry to **20-30**:

```
(config service modbus_gateway client test_modbus_client)> filter 0 20-30
(config service modbus_gateway client test_modbus_client)>
```

To add additional filters, increment the index number. For example, to add an additional filter for addresses in the range of 50-100:

```
(config service modbus_gateway client test_modbus_client)> filter 1 50-100
(config service modbus_gateway client test_modbus_client)>
```

g. If request messages handled by this client should always be forwarded to a specific device, , use **fixed_server_address** to set the device's Modbus address:

```
(config service modbus_gateway client test_modbus_client)> fixed_server_address value
(config service modbus_gateway client test_modbus_client)>
```

Leave at the default setting of **0** to allow messages that match the Modbus address filter to be forwarded to devices based on the Modbuss address in the message.

h. To adjust the Modbus server address downward by the specified value prior to delivering the message, use **adjust_server_address**:

```
(config service modbus_gateway client test_modbus_client)> adjust_server_address value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is an integer from **0** to **255**. Leave at the default setting of **0** to not adjust the server address.

If a packet contains a Modbus server address above the amount entered here, the address will be adjusted downward by this amount before the packet is delivered. This allows you to configure clients on the gateway that will forward messages to remote devices with the same Modbus address on different buses. For example, if there are two devices on two different buses that have the same Modbus address of 10, you can create two clients on the gateway:

- Client one:
  - **filter** set to **10**.

  This will configure the gateway to deliver all messages that have the Modbus server address of 10 to this device.
- Client two:
  - **filter** set to **20**.
  - **adjust_server_address** set to **10**.

This will configure the gateway to deliver all messages that have the Modbus server address address of 20 to the device with address 10.

i. Repeat the above instructions for additional clients.

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Modbus hardening

Modbus hardening refers to the process of enhancing the security and reliability of Modbus communications between devices over a network by implementing various protective measures. This includes configuring the Modbus systems to minimize vulnerabilities, applying access controls, using encryption, segmenting networks, upgrading firmware on the devices, as well as monitoring and logging. Modbus hardening is about making the serial communication between devices over a network more secure against cyber threats.

Hardening can involve implementing various security measures, such as:

- **Access control**

  Update the **Services** > **Modbus Gateway** > **Gateway servers** > **Access control list** settings to only allow access to the Modbus service on the specific network interfaces, firewall zones, and source IP addresses that you expect the Modbus queries to come from. See Configure the Modbus gateway for more information.

- **Encryption**

  Further lock down access to the Modbus gateway service on the IX10 by configuring it to establish a VPN tunnel, then update the access control list as mentioned above to only allow access to the Modbus service through the VPN connection.

- **Network segmentation**

  Use a separate firewall zone for the network interface(s) and/or VPN tunnels that the user will be accessing the Modbus gateway service through to ensure that the Modbus access is separate from other network traffic

- **Monitoring and logging**

  Utilize Digi Remote Manager or an external logging service to monitor the activity on your Digi router

- **Firmware upgrades**

  Keep your firmware current so your IX10 has the most recent security patches and bug fixes.

Note To see how you can implement security measures for you Modbus gateway service, see Use case | Secure your Modbus gateway service.

Use case | Secure your Modbus gateway service

Do you want to secure Modbus messaging across an internet connection to safeguard the information being communicated between Digi devices over your network?
You can by implementing security measures, such as access control, encryption, network segmentation, monitoring and logging, and firmware upgrades to ensure the integrity and confidentiality of Modbus communications between Digi devices on your network.

1. Determine the devices on your network that need to communicate with each other via the Modbus Gateway service.
2. Isolate Modbus traffic using VLANS or separate network interfaces.
3. Implement strong authentication.
4. Define access policies.

   Update the **Services** > **Modbus Gateway** > **Gateway servers** > **Access control list** settings to only allow access to the Modbus service on the specific network interfaces, firewall zones, and source IP addresses that you expect the Modbus queries to come from. See Configure the Modbus gateway for more information.
5. Create a VPN tunnel, such as IPsec or Wireguard, to protect data in transit between your devices.
6. Configure firewalls to monitor and control incoming and outgoing traffic.

By implementing these advanced security protocols and ensuring reliable data transmission, this service effectively addresses the challenges of data integrity and privacy on your network.

Show Modbus gateway status and statistics

You can view status and statistics about location information from either the WebUI or the command line.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, select **Status** > **Modbus Gateway**.

   The **Modbus Gateway** page appears.

   Statistics related to the Modbus gateway server are displayed. If the message **Server connections not available** is displayed, this indicates that there are no connected clients.

   - To view information about Modbus gateway clients, click **Clients**.
   - To view statistics that are common to both the clients and server, click **Common Statistics**.
   - To view configuration details about the gateway, click the ✷ (configuration) icon in the upper right of the gateway's status pane.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show modbus-gateway command at the system prompt:

```
> show modbus-gateway

Server Connection  IP Address   Port   Uptime
-----------------  -----------  -----  ------
modbus_socket      10.45.1.139  49570  6
modbus_socket      10.45.1.139  49568  13

Client             Uptime
-------------------  ------
modbus_socket_41     0
modbus_socket_21     0
modbus_serial_client  428

>
```

If the message **Server connections not available** is displayed, this indicates that there are no connected clients.

3. Use the show modbus-gateway verbose command at the system prompt to display more information:

```
> show modbus-gateway verbose

Client             Uptime
-------------------  ------
modbus_socket_41     0
modbus_socket_21     0
modbus_serial_client  506

Common Statistics
-----------------
Configuration Updates        : 1
Client Configuration Failure  : 0
Server Configuration Failure  : 0
Configuration Load Failure    : 0
Incoming Connections          : 4
Internal Error                : 0
Resource Shortages            : 0

Servers
-------

modbus_socket
-------------
Client Lookup Errors          : 0
Incoming Connections          : 4
Packet Errors                 : 0
RX Broadcasts                 : 0
RX Requests                   : 12
TX Exceptions                 : 0
```

```
TX Responses              : 12

Clients
-------

modbus_socket_41
----------------
Address Translation Errors    : 0
Connection Errors             : 0
Packet Errors               : 0
RX Responses                : 4
RX Timeouts                 : 0
TX Broadcasts               : 0
TX Requests                 : 4

modbus_socket_21
----------------
Address Translation Errors    : 0
Connection Errors             : 0
Packet Errors               : 0
RX Responses                : 4
RX Timeouts                 : 0
TX Broadcasts               : 0
TX Requests                 : 4

modbus_serial_client
--------------------
Address Translation Errors    : 0
Connection Errors             : 0
Packet Errors               : 0
RX Responses                : 4
RX Timeouts                 : 0
TX Broadcasts               : 0
TX Requests                 : 4

>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

System time synchronization

System time synchronization refers to the process of coordinating the system time of your IX10 device with an external, more accurate time source. By default, this synchronization occurs one time per day, but will also synchronize at startup, and in response to a change in the route. There are two configuration parameters that control system time synchronization: **ntpdate** and **system.time.resyn_interval**.

The **ntpdate** default configurations include the following:

- Time zone: **UTC**
- NTP server: the Digi NTP server, **time.digicloud.com**

The **system.time.resyn_interval** default configuration includes the following:

- Frequency of the synchronization: **1d** (one day). Set to **O** (zero) for no synchronization except at startup and route change.

No additional configuration is required for the synchronization if this default configuration is sufficient for your setup. However, you can change per-day synchronization, the default time zone, and the default NTP server, as well as adding additional NTP servers. If multiple NTP servers are added, time samples are obtained from each server. Selection algorithms are used to determine the most accurate time. See Configure the system time synchronization for details about changing the default configuration.

The IX10 device can also be configured to serve as an NTP server, providing NTP services to downstream devices. See Network Time Protocol for more information about NTP server support.

You can also set the local date and time manually, if there is no access to the configured NTP servers or modem time sources. See Manually set the system date and time for more information.

Configure the system time synchronization

To configure or change the system time synchronization:

Web

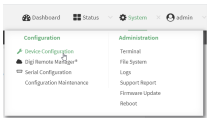
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System** > **Time**.
4. Modify the settings.

CAUTION! If you enable the NTP service, either disable the server configured in `system time` or make sure to match the server(s) configured in `service ntp server`. If you do not do one of these options, then the System time synchronization may fail, which could result in the following error message: `ntpdate[2901]: the NTP socket is in use, exiting`.

System time setting	UI Configuration
Timezone	Choose the time zone closest to where the device is located. The default time zone is **UTC**.
Resynchronization interval	Type the frequency of the daily update. The default is **1d** (one day). Set to **0** (zero) for no synchronization.
Time sources	a. Click to add a new time source. The time source is now enabled by default. b. In **Type of time source**, choose whether you want to use an **NTP** or **Modem** as the external source to which the device synchronizes. ■ If using an NTP, click to add the **Server** hostname. The default is time.devicecloud.com. Note If multiple NTP servers are added, time samples are obtained from each server. Selection algorithms are used to determine the most accurate time. ■ If using a modem, specify the **Modem** and **Modem time offset**. The default offset is **Local**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Type **system time** to enter configuration mode for system time.

```
 > config system time
(config system time)>
```

4. Add a new time source or modify the settings.

CAUTION! If you enable the NTP service, either disable the server configured in `system time` or make sure to match the server(s) configured in `service ntp server`. If you do not do one of these options, then the System time synchronization may fail, which could result in the following error message: `ntpdate[2901]: the NTP socket is in use, exiting`.

System time setting	UI Configuration

Timezone	(Optional) Set the timezone for the location of your IX10 device. The default is **UTC**.
	`(config)> system time timezone value`
	`(config)>`
	Where *value* is the timezone using the format specified with the following command:
	`(config)> system time timezone ?`
	`Timezone: The timezone for the location of this device. This is used to adjust the time for log`
	`messages. It also affects actions that occur at a specific time of day.`
	`Format:`
	`Africa/Abidjan`
	`Africa/Accra`
	`Africa/Addis_Ababa`
	`...`
	`(config)>`

Resynchronization interval	Type the frequency of the daily update. The default is **1d** (one day). Set to **0** (zero) for no synchronization.
	`(config) system time resync_interval value`
	`(config) >`

System time setting	UI Configuration

	Where *value* is {w|d|h|m|s}. For more information:
	`(config)> system time resync_interval ?`
	
	`Format: number {w|d|h|m|s}...`
	`Optional: yes`
	`Dafault value: 1 d`
	`Current value: 1 d`
	`(config)>`

Time sources	Add a new time source, either an NTP server or a modem.
	Note The default NTP server is time.devicecloud.com.
	■ If adding one or more NTP servers:
	`add service ntp server 0 time.server.com`
	Note If multiple NTP servers are added, time samples are obtained from each server. Selection algorithms are used to determine the most accurate time.
	Note This list is synchronized with the list of servers included with NTP server configuration, and changes made to one will be reflected in the other. See Configure the device as an NTP server for more information about NTP server configuration.
	■ If adding a modem, specify the mode and time offset:
	The default offset is **Local**.
	`(config system time source)> add end`
	`(config system time source 1)>`
	`(config system time source 1)> type modem`
	`(config time source 1) > modem modem`
	■ To see the modem and its settings:
	`(config system time source 1)> show`
	`enable true`
	`no label`
	`modem modem`
	`offset local`
	`type modem`

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Test the connection to the NTP servers

The following procedure tests the configured NTP servers for connectivity. This test does not affect the device's current local date and time.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Test the configured NTP servers for connectivity:

```
> system time test
Testing NTP server time.devicecloud.com on UDP port 123...
server 52.2.40.158, stratum 2, offset -0.000216, delay 0.05800
server 35.164.164.69, stratum 2, offset -0.000991, delay 0.07188
24 Aug 22:01:20 ntpdate[28496]: adjust time server 52.2.40.158 offset -0.000216 sec
NTP test sync successful

Testing NTP server time.accns.com on UDP port 123...
server 128.136.167.120, stratum 3, offset -0.001671, delay 0.08455
24 Aug 22:01:20 ntpdate[28497]: adjust time server 128.136.167.120 offset -0.001671 sec
NTP test sync successful
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Manually synchronize with the NTP server

The following procedure perform a NTP query to the configured servers and set the local time to the first server that responds.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Synchronize the device's local date and time:

```
> system time sync
24 Aug 22:03:55 ntpdate[2520]: step time server 52.2.40.158 offset -0.000487 sec
NTP sync to time.devicecloud.com successful
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Manually set the system date and time

If your network restricts access to NTP servers, use this procedure to set the local date and time.

This procedure is available at the Admin CLI only.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Set the device's local date and time:

```
> system time set value
>
```

   where *value* is the date in year-month-day hour:minute:second format. The *value* must be surrounded by double quotes. For example:

```
> system time set "2024-01-12 12:10:00"
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Network Time Protocol

Network Time Protocol (NTP) enables devices connected on local and worldwide networks to synchronize their internal software and hardware clocks to the same time source. The IX10 device can be configured as an NTP server, allowing downstream hosts that are attached to the device's Local Area Networks to synchronize with the device.

When the device is configured as an NTP server, it also functions as an NTP client. The NTP client will be consistently synchronized with one or more upstream NTP servers, which means that NTP packets are transferred every few seconds. A minimum of one upstream NTP server is required. Additional NTP servers can be configured. If multiple servers are configured, a number of time samples are obtained from each of the servers and a subset of the NTP clock filter and selection algorithms are applied to select the best of these.

See Configure the device as an NTP server for information about configuring your device as an NTP server.

Configure the device as an NTP server

Required Configuration Items

- Enable the NTP service.
- At least one upstream NTP server for synchronization. The default setting is the Digi NTP server, time.devicecloud.com.

Additional Configuration Options

- Additional upstream NTP servers.
- Access control list to limit downstream access to the IX10 device's NTP service.
- The time zone setting, if the default setting of UTC is not appropriate.

To configure the IX10 device's NTP service:

Web

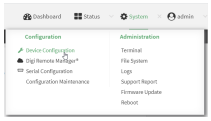
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **NTP**.
4. Enable the IX10 device's NTP service by clicking **Enable**.
5. (Optional) Configure the access control list to limit downstream access to the IX10 device's NTP service.
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's NTP service. Allowed values are:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the NTP service.

d. Click to add again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click to add.
  c. For **Address**, enter the IPv6 address or network that can access the device's NTP service. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the NTP service.
  d. Click to add again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click to add.
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click to add again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click to add.
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click to add again to allow access through additional firewall zones.

Note By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the IX10 device can use the NTP service.

---

6. Enable **Fall back to local clock** to allow the device's local system clock to be used as backup time source.
7. (Optional) Add upstream NTP servers that the device will use to synchronize its time. The default setting is **time.devicecloud.com**.
   - To change the default value of the NTP server:
     a. Click **NTP servers**.
     b. For **Server**, type a new server name.
   - To add an NTP server:
     a. Click **NTP servers**.
     b. For **Add Server**, click to add.
     c. For **Server**, enter the hostname of the upstream NTP server that the device will use to synchronize its time.

d. Click to add additional NTP servers. If multiple servers are included, servers are tried in the order listed until one succeeds.

Note This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See Configure the system time synchronization for more information about NTP client configuration.

8. (Optional) Configure the system time zone. The default is **UTC**.
   a. Click **System** > **Time**
   b. Select the **Timezone** for the location of your IX10 device.
9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the ntp service:

```
(config)> service ntp enable true
(config)>
```

4. (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.
   - To delete the default NTP server, **time.devicecloud.com**:

```
(config)> del service ntp server 0
(config)>
```

   - To add the NTP server to the beginning of the list, use the index value of **0** to indicate that it should be added as the first server:

```
(config)> add service ntp server 0 time.server.com
(config)>
```

   - To add the NTP server to the end of the list, use the index keyword **end**:

```
(config)> add service ntp server end time.server.com
(config)>
```

   - To add the NTP server in another location in the list, use an index value to indicate the appropriate position. For example:

```
(config)> add service ntp server 1 time.server.com
(config)>
```

Note This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See Configure the system time synchronization for more information about NTP client configuration.

5. Allow the device's local system clock to be used as backup time source:

```
(config)> service ntp local true
(config)>
```

6. (Optional) Configure the access control list to limit downstream access to the IX10 device's NTP service.
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config)> add service ntp acl address end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the NTP server agent.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

     ```
     (config)> add service ntp acl address6 end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the NTP server agent.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

     ```
     (config)> add service ntp acl interface end value
     (config)>
     ```

     Where *value* is an interface defined on your device.

     Display a list of available interfaces:

     Use **... network interface ?** to display interface information:

     ```
     (config)> ... network interface ?

     Interfaces

     Additional Configuration
     ------------------------------------------
     setupip         Setup IP
     ```

```
setuplinklocalip     Setup Link-local IP
eth                  ETH
loopback             Loopback
modem                Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service ntp acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

Note By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the IX10 device can use the NTP service.

7. (Optional) Set the timezone for the location of your IX10 device. The default is **UTC**.

```
(config)> system time timezone value
(config)>
```

Where *value* is the timezone using the format specified with the following command:

```
(config)> system time timezone ?

Timezone: The timezone for the location of this device. This is used to adjust the time for log
```

```
messages. It also affects actions that occur at a specific time of day.
Format:
 Africa/Abidjan
 Africa/Accra
 Africa/Addis_Ababa
 ...

(config)>
```

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show status and statistics of the NTP server

You can display status and statistics for active NTP servers

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.
2. Under **Services**, click **NTP**.

   The NTP server status page is displayed.

Command line

Show NTP information

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show ntp command at the system prompt:

```
> show ntp

 NTP Status Status
 -----------------
 Status     : Up
 Sync Status : Up

 Remote          Refid       ST  T  When  Poll  Reach  Delay   Offset  Jitter
 ---------------- ------------- -- - ---- ---- ----- ------ ------ ------
```

```
*ec2-52-2-40-158  129.6.15.32   2  u 191   1024 377   33.570 +1.561  0.991
128.136.167.120   128.227.205.3 3  u 153   1024 1     43.583 -1.895  0.382

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure a multicast route

Multicast routing allows a device to transmit data to a single multicast address, which is then distributed to a group of devices that are configured to be members of that group.

To configure a multicast route:

Web

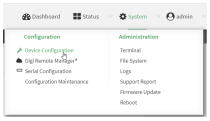
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Multicast**.
4. For **Add Multicast route**, type a name for the route and click .
5. The new route is enabled by default. To disable, toggle off **Enable**.
6. Type the **Source address** for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.
7. Select a **Source interface** where multicast packets will arrive.
8. To add one or more destination interface that the IX10 device will send mutlicast packets to:
   a. Click to expand **Destination interfaces**.
   b. Click .

c. For **Destination interface**, select the interface.

d. Repeat for additional destination interfaces.

9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the multicast route. For example, to add a route named **test**:

```
(config)> add service multicast test
(config service multicast test)>
```

4. The multicast route is enabled by default. If it has been disabled, enable the route:

```
(config service multicast test)> enable true
(config service multicast test)>
```

5. Set the source address for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.

```
(config service multicast test)> dst ip-address
(config service multicast test)>
```

6. Set the source interface for the route where multicast packets will arrive:

   a. Use the **?** to determine available interfaces:

   b. Set the interface. For example:

```
(config service multicast test)> src_interface /network/interface/eth1
(config service multicast test)>
```

7. Set a destination interface that the IX10 device will send mutlicast packets to:

   a. Use the **?** to determine available interfaces:

   b. Set the interface. For example:

```
(config service multicast test)> add interface end /network/interface/eth1
(config service multicast test)>
```

   c. Repeat for each additional destination interface.

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable service discovery (mDNS)

Multicast DNS mDNS is a protocol that resolves host names in small networks that do not have a DNS server. You can enable the IX10 device to use mDNS.

Web

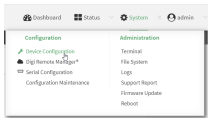
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **Service Discovery (mDNS)**.
4. **Enable** the mDNS service.
5. Click **Access control list** to configure access control:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click ♈.
     c. For **Address**, enter the IPv4 address or network that can access the device's mDNS service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the mDNS service.
     d. Click ♈ again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
  a. Click **IPv6 Addresses**.
  b. For **Add Address**, click ⅄.
  c. For **Address**, enter the IPv6 address or network that can access the device's mDNS service. Allowed values are:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the mDNS service.
  d. Click ⅄ again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click ⅄.
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click ⅄ again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click ⅄.
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click ⅄ again to allow access through additional firewall zones.

6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the mDNS service:

```
(config)> service mdns enable true
(config)>
```

4. Configure access control:
   - To limit access to specified IPv4 addresses and networks:

```
(config)> add service mdns acl address end value
(config)>
```

     Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service mdns acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service mdns acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service mdns acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Use the MQTT broker service

MQTT is a lightweight publish/subscribe messaging protocol for the Internet of Things (IoT) applications, designed to connect devices using a small footprint and minimum network bandwidth.

Your IX10 device includes an MQTT broker service that serves as an intermediary between MQTT clients. The broker receives and distributes client messages.

Required configuration items

- Enable the MQTT broker.
- MQTT client usernames and passwords.
  - Topic access control for each client.
- Encryption type.
- How to control client access to topics on the MQTT broker.

Additional configuration Items

- The port used by the MQTT broker.
- Access control list to limit downstream access to the IX10 device's MQTT broker.

- Include debug messages in the system log.
- Whether to allow anonymous clients.
- Whether to allow clients that have no client ID to connect.
- Whether replace the client's ID with its username.

Web

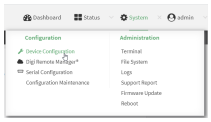
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

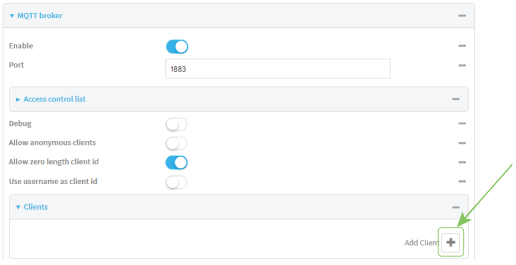
   The **Configuration** window is displayed.
3. Click **Services** > **MQTT broker**.
4. Click **Enable**.
5. (Optional) For **Port**, type the port number for the MQTT broker to listen for incoming connections. The default is **1883**.
6. (Optional) Click to expand **Access control list** to restrict access to the MQTT broker:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click ⋎.
     c. For **Address**, enter the IPv4 address or network that can access the device's iperf service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the iperf service.
     d. Click ⋎ again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click ⋎.

c. For **Address**, enter the IPv6 address or network that can access the device's iperf service. Allowed values are:
   - A single IP address or host name.
   - A network designation in CIDR notation, for example, 2001:db8::/48.
   - **any**: No limit to IPv6 addresses that can access the iperf service.

d. Click to add again to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the device:
  a. Click **Interfaces**.
  b. For **Add Interface**, click to add.
  c. For **Interface**, select the appropriate interface from the dropdown.
  d. Click to add again to allow access through additional interfaces.
- To limit access based on firewall zones:
  a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
  b. For **Add Zone**, click to add.
  c. For **Zone**, select the appropriate firewall zone from the dropdown.
     See Firewall configuration for information about firewall zones.
  d. Click to add again to allow access through additional firewall zones.

7. Click to toggle on **Debug** to write MQTT debug messages to the system log.
8. Click to toggle on **Allow anonymous clients** to allow connections from clients that do not provide a username.
9. By default, the MQTT broker will allow clients without client IDs to connect, and will generate a client ID for them. To disable, click to toggle off **Allow zero length client id**.
10. Click to toggle on **Use username as client id**. When enabled, the broker will replace the client ID with the username, which will prevent one client from disconnecting another by using the same client ID.
11. Add a client:
    a. Click to expand **Clients**.
    b. Click to add a client.



    c. Type the **Username** and **Password** for the client.
    d. Add a topic to control this client's access to:
       i. Click to expand **Topic access control list**.
       ii. Click to add a topic.

iii. For **Topic**, type the topic. The signal level wildcard, **+**, and multi-level wildcard, #, are supported.

iv. For **Access**, select the level of access that the client will have:

- **Read**
- **Write**
- **Read/write**
- **Deny**

v. Click to add additional topics.

e. Click to add additional clients.

12. Click to expand **Encryption**.
13. For **Type**, select either **None** or **PSK**.
    - If **PSK** is selected:
      a. Click to enable **Use PSK identity as username** to use the PSK identity sent by the client as its username.
      b. (Optional) For **Identifier**, type a string that identifies the listener and is sent to the clients.
      c. Click to expand **Pre-shared keys**.
      d. Click to add a pre-shared key.
      e. For **Identity**, type the identity sent to the client.
      f. For **Key**, type or paste the pre-shared key in hexadecimal format that is associated with the client identity.
      g. Click to add additional pre-shared keys.
14. Click to expand **Topic access control list**.

    The topic access control lists controls what topics clients can access. If no topics are included, then clients have access to all topics. If any topics are listed, access is restricted to only the listed topics.

    - To restrict access for anonymous clients to particular topics:
      a. Click to expand **Anonymous**.
      b. Click to add a topic.
      c. For **Topic**, type the topic. The signal level wildcard, **+**, and multi-level wildcard, #, are supported.
      d. For **Access**, select the level of access that the client will have:
         - **Read**
         - **Write**
         - **Read/write**
         - **Deny**
      e. Click to add additional topics.
    - To restrict access to topics based on pattern substitution:
      a. Click to expand **Pattern**.
      b. Click to add a topic.

c. For **Topic**, type the topic. The variables **%c** and **%u** can be used as substitutes for the client ID or username. If a variable is used, it can be the only text for that level of the hierarchy..

d. For **Access**, select the level of access that the client will have:

- **Read**
- **Write**
- **Read/write**
- **Deny**

e. Click Yo again to add additional topics.

15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the MQTT broker:

```
(config)> service mqtt enable true
(config)>
```

4. (Optional) Set the port number for the MQTT broker to listen for incoming connections:

```
(config)> service mqtt port int
(config)>
```

   The default is **1883**.

5. (Optional) Set the access control list to restrict access to the MQTT broker:

   - To limit access to specified IPv4 addresses and networks:

```
(config)> add service mqtt acl address end value
(config)>
```

     Where *value* can be:

     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the iperf service.

     Repeat this step to list additional IP addresses or networks.

   - To limit access to specified IPv6 addresses and networks:

```
(config)> add service mqtt acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the iperf service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX10 device:

```
(config)> add service mqtt acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-------------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service mqtt acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

Additional Configuration
-------------------------------------------------------------------------------
any
dynamic_routes
```

```
edge
external
internal
ipsec
loopback
setup

(config)>
```

Repeat this step to include additional firewall zones.

6. Enable the system to write MQTT debug messages to the system log:

```
(config)> service mqtt debug true
(config)>
```

7. Enable connections from clients that do not provide a username:

```
(config)> service mqtt allow_anonymous true
(config)>
```

8. By default, the MQTT broker will allow clients without client IDs to connect, and will generate a client ID for them. To disable:

```
(config)> service mqtt allow_zero_length_client_id false
(config)>
```

9. Enable the broker to replace the client ID with the username, which will prevent one client from disconnecting another by using the same client ID:

```
(config)> service mqtt use_username_as_client_id true
(config)>
```

10. Add and configure clients that are allowed to connect to the broker:
    a. Add a client:

```
(config)> add service mqtt client end
(config service mqtt client 0)>
```

    b. Set the username and password for the client:

```
(config service mqtt client 0)> username value
(config service mqtt client 0)> password value
(config service mqtt client 0)>
```

    c. Add a topic to control this client's access to:
        i. Add a topic:

```
(config service mqtt client 0)> add topic_acl end
(config service mqtt client 0 topic_acl 0)>
```

ii. Set the topic:

```
(config service mqtt client 0 topic_acl 0)> topic value
(config service mqtt client 0 topic_acl 0)>
```

where *value* is one of:

- The topic.
- The signal level wildcard, **+**.
- The multi-level wildcard, #.

iii. Set the access type to apply to the topic:

```
(config service mqtt client 0 topic_acl 0)> access value
(config service mqtt client 0 topic_acl 0)>
```

where *value* is one of:

- **deny**
- **read**
- **readwrite**
- **write**

The default is **readwrite**.

iv. Add additional topics:

```
(config service mqtt client 0 topic_acl 0)> add .. .. topic_acl end
(config service mqtt client 0 topic_acl 1)>
```

v. Repeat the above steps to set the topic and access type.

11. Set the encryption:

a. Return to the root of the configuration:

```
(config service mqtt client 0 topic_acl 1)> ...
(config)>
```

b. Set the encryption type:

```
(config)> service mqtt encryption type value
(config)>
```

where *value* is either:

- **none**
- **psk**

  If **psk** is used:

  a. (Optional) Set a string that identifies the listener and is sent to the clients:

  ```
  (config)> service mqtt encryption identifier string
  (config)>
  ```

b. Enable the PSK identity sent by the client to be used as its username:

```
(config)> service mqtt encryption use_identity_as_username true
(config)>
```

c. Set the pre-shared keys:

i. Add a pre-shared key:

```
(config)> add service mqtt encryption psk end
(config service mqtt encryption psk 0)>
```

ii. Set the identity sent to the client:

```
(config service mqtt encryption psk 0)> indentity value
(config service mqtt encryption psk 0)>
```

iii. Set the pre-shared key:

```
(config service mqtt encryption psk 0)> key value
(config service mqtt encryption psk 0)>
```

where *value* is the pre-shared key in hexadecimal format that is associated with the client identity.

iv. Add additional keys:

```
(config service mqtt encryption psk 0)> add .. end
(config service mqtt encryption psk 1)>
```

Repeat the above steps to set the identity and the pre-shared key.

12. The topic access control lists controls what topics clients can access. If no topics are included, then clients have access to all topics. If any topics are listed, access is restricted to only the listed topics.

- To restrict access for anonymous clients to particular topics:

a. Return to the service mqtt node of the schema:

```
(config service mqtt encryption psk 1)> ... service mqtt
(config service mqtt)>
```

b. Add a topic:

```
(config service mqtt)> add topic_acl anonymous end
(config service mqtt topic_acl anonymous 0)>
```

c. Set the topic:

```
(config service mqtt topic_acl anonymous 0)> topic value
(config service mqtt topic_acl anonymous 0)>
```

where *value* is one of:

- The topic.
- The signal level wildcard, **+**.
- The multi-level wildcard, #.

d. Set the access type to apply to the topic:

```
(config service mqtt topic_acl anonymous 0)> access value
(config service mqtt topic_acl anonymous 0)>
```

where *value* is one of:

- **deny**
- **read**
- **readwrite**
- **write**

The default is **readwrite**.

e. Add additional topics:

```
(config service mqtt topic_acl anonymous 0)> add .. .. anonymous end
(config service mqtt topic_acl anonymous 1)>
```

f. Repeat the above steps to set the topic and access type.

- To restrict access to topics based on pattern substitution:

a. Return to the service mqtt node of the schema:

```
(config service mqtt encryption psk 1)> ... service mqtt
(config service mqtt)>
```

b. Add a topic:

```
(config service mqtt)> add topic_acl pattern end
(config service mqtt topic_acl pattern 0)>
```

c. Set the topic:

```
(config service mqtt topic_acl pattern 0)> topic value
(config service mqtt topic_acl pattern 0)>
```

where *value* is one of:

- The topic.
- The variable **%c** as a substitute for the client ID.
- The variable **%u** as a substitute for the username.

If a variable is used, it can be the only text for that level of the hierarchy.

d. Set the access type to apply to the topic:

```
(config service mqtt topic_acl pattern 0)> access value
(config service mqtt topic_acl pattern 0)>
```

where *value* is one of:

- **deny**
- **read**
- **readwrite**
- **write**

The default is **readwrite**.

e. Add additional topics:

```
(config service mqtt topic_acl pattern 0)> add .. .. pattern end
(config service mqtt topic_acl pattern 1)>
```

f. Repeat the above steps to set the topic and access type.

13. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

14. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show MQTT broker information

You can view status and statistics about the MQTT broker from either the WebUI or the command line.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.
2. Under **Services**, click **MQTT Broker**.

Command line

Show MQTT broker information

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show mqtt command at the system prompt:

```
> show location

MQTT Broker Status
------------------
Enabled        : true
Status         : up
```

```
Version         : mosquitto version 2.0.14
Uptime          :  (202s)

Totals
------
Bytes sent      : 158400
Bytes received  : 4500
Messages sent   : 0
Messages received : 0

Clients
-------
Total           : 1
Maximum         : 5
Connected       : 1
Disconnected    : 0
Expired         : 0

Subscriptions
-------------
Total           : 1
Shared          : 1

Message Store
-------------
Bytes           : 151
Messages        : 35
Retained messages : 40

PUBLISH Messages
----------------
Bytes sent      : 0
Bytes received  : 0
Messages sent   : 0
Messages received : 0
Messages dropped  : 0


>
```

3. Use the show mqtt command to return additional information, including averages over one, five, and fifteen minutes.
4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Use the iPerf service

Your IX10 device includes an iPerf3 server that you can use to test the performance of your network.

iPerf3 is a command-line tool that measures the maximum network throughput an interface can handle. This is useful when diagnosing network speed issues, to determine, for example, whether a cellular connection is providing expected throughput.

The IX10 implementation of iPerf3 supports testing with both TCP and UDP.

Note Using iPerf clients that are at a version earlier than iPerf3 to connect to the IX10 device's iPerf3 server may result in unpredictable results. As a result, Digi recommends using an iPerf client at version 3 or newer to connect to the IX10 device's iPerf3 server.

Required configuration items

- Enable the iPerf server on the IX10 device.
- An iPerf3 client installed on a remote host. iPerf3 software can be downloaded at https://iperf.fr/iperf-download.php.

Additional configuration Items

- The port that the IX10 device's iPerf server will use to listen for incoming connections.
- The access control list for the iPerf server.

  When the iPerf server is enabled, the IX10 device will automatically configure its firewall rules to allow incoming connections on the configured listening port. You can restrict access by configuring the access control list for the iPerf server.

To enable the iPerf3 server:

Web

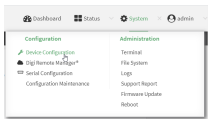
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Services** > **iPerf**.

4. Click **Enable**.
5. (Optional) For **IPerf Server Port**, type the appropriate port number for the iPerf server listening port.
6. (Optional) Click to expand **Access control list** to restrict access to the iPerf server:
   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's iperf service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the iperf service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's iperf service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the iperf service.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.
        See Firewall configuration for information about firewall zones.
     d. Click again to allow access through additional firewall zones.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the iPerf server:

```
(config)> service iperf enable true
(config)>
```

4. (Optional) Set the port number for the iPerf server listening port. The default is 5201.

```
(config)> service iperf port port_number
(config)>
```

5. (Optional) Set the access control list to restrict access to the iPerf server:
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config)> add service iperf acl address end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

     ```
     (config)> add service iperf acl address6 end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

     ```
     (config)> add service iperf acl interface end value
     (config)>
     ```

     Where *value* is an interface defined on your device.

     Display a list of available interfaces:

     Use **... network interface ?** to display interface information:

     ```
     (config)> ... network interface ?

     Interfaces
     ```

```
Additional Configuration
-----------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service iperf acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example performance test using iPerf3

On a remote host with iPerf3 installed, enter the following command:

```
$ iperf3 -c device_ip
```

where *device_ip* is the IP address of the IX10 device. For example:

```
$ iperf3 -c 192.168.2.1
Connecting to host 192.168.2.1, port 5201
[ 4] local 192.168.3.100 port 54934 connected to 192.168.1.1 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[ 4]   0.00-1.00   sec  26.7 MBytes   224 Mbits/sec    8   2.68 MBytes
[ 4]   1.00-2.00   sec  28.4 MBytes   238 Mbits/sec   29   1.39 MBytes
[ 4]   2.00-3.00   sec  29.8 MBytes   250 Mbits/sec    0   1.46 MBytes
[ 4]   3.00-4.00   sec  31.2 MBytes   262 Mbits/sec    0   1.52 MBytes
[ 4]   4.00-5.00   sec  32.1 MBytes   269 Mbits/sec    0   1.56 MBytes
[ 4]   5.00-6.00   sec  32.5 MBytes   273 Mbits/sec    0   1.58 MBytes
[ 4]   6.00-7.00   sec  33.9 MBytes   284 Mbits/sec    0   1.60 MBytes
[ 4]   7.00-8.00   sec  33.7 MBytes   282 Mbits/sec    0   1.60 MBytes
[ 4]   8.00-9.00   sec  33.5 MBytes   281 Mbits/sec    0   1.60 MBytes
[ 4]   9.00-10.00  sec  33.2 MBytes   279 Mbits/sec    0   1.60 MBytes
- - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[ 4]   0.00-10.00  sec   315 MBytes   264 Mbits/sec   37             sender
[ 4]   0.00-10.00  sec   313 MBytes   262 Mbits/sec                  receiver

iperf Done.
$
```

Configure the ping responder service

Your IX10 device's ping responder service replies to ICMP and ICMPv6 echo requests. The service is enabled by default. You can disable the service, or you can configure the service to use an access control list to limit the service to specified IP address, interfaces, and/or zones.

To enable the iPerf3 server:

Web

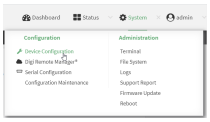
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services** > **Ping responder**.

   The ping responder service is enabled by default. Click **Enable** to disable all ping responses.

4. Click to expand **Access control list** to restrict ping responses to specified IP address, interfaces, and/or zones:

   - To limit access to specified IPv4 addresses and networks:
     a. Click **IPv4 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv4 address or network that can access the device's ping responder. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 192.168.1.0/24.
        - **any**: No limit to IPv4 addresses that can access the ping responder.
     d. Click again to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:
     a. Click **IPv6 Addresses**.
     b. For **Add Address**, click .
     c. For **Address**, enter the IPv6 address or network that can access the device's ping responder. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the ping responder.
     d. Click again to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the device:
     a. Click **Interfaces**.
     b. For **Add Interface**, click .
     c. For **Interface**, select the appropriate interface from the dropdown.
     d. Click again to allow access through additional interfaces.
   - To limit access based on firewall zones:
     a. Click **Zones**. By default, there are three firewall zones already configured: Internal, Edge, and IPsec.
     b. For **Add Zone**, click .
     c. For **Zone**, select the appropriate firewall zone from the dropdown.

        See Firewall configuration for information about firewall zones.
     d. Click again to allow access through additional firewall zones.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the iPerf server:

```
(config)> service iperf enable true
(config)>
```

4. (Optional) Set the port number for the iPerf server listening port. The default is 5201.

```
(config)> service iperf port port_number
(config)>
```

5. (Optional) Set the access control list to restrict access to the iPerf server:
   - To limit access to specified IPv4 addresses and networks:

     ```
     (config)> add service iperf acl address end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 192.168.1.0/24.
     - **any**: No limit to IPv4 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to specified IPv6 addresses and networks:

     ```
     (config)> add service iperf acl address6 end value
     (config)>
     ```

     Where *value* can be:
     - A single IP address or host name.
     - A network designation in CIDR notation, for example, 2001:db8::/48.
     - **any**: No limit to IPv6 addresses that can access the service-type.

     Repeat this step to list additional IP addresses or networks.
   - To limit access to hosts connected through a specified interface on the IX10 device:

     ```
     (config)> add service iperf acl interface end value
     (config)>
     ```

     Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **... network interface ?** to display interface information:

```
(config)> ... network interface ?

Interfaces

Additional Configuration
-----------------------------------------------
setupip          Setup IP
setuplinklocalip     Setup Link-local IP
eth              ETH
loopback         Loopback
modem            Modem

config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service iperf acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type **... firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be referred to by packet
filtering rules and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config)>
```

Repeat this step to include additional firewall zones.

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example performance test using iPerf3

On a remote host with Iperf3 installed, enter the following command:

```
$ iperf3 -c device_ip
```

where *device_ip* is the IP address of the IX10 device. For example:

```
$ iperf3 -c 192.168.2.1
Connecting to host 192.168.2.1, port 5201
[ 4] local 192.168.3.100 port 54934 connected to 192.168.1.1 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[ 4]   0.00-1.00   sec  26.7 MBytes   224 Mbits/sec    8   2.68 MBytes
[ 4]   1.00-2.00   sec  28.4 MBytes   238 Mbits/sec   29   1.39 MBytes
[ 4]   2.00-3.00   sec  29.8 MBytes   250 Mbits/sec    0   1.46 MBytes
[ 4]   3.00-4.00   sec  31.2 MBytes   262 Mbits/sec    0   1.52 MBytes
[ 4]   4.00-5.00   sec  32.1 MBytes   269 Mbits/sec    0   1.56 MBytes
[ 4]   5.00-6.00   sec  32.5 MBytes   273 Mbits/sec    0   1.58 MBytes
[ 4]   6.00-7.00   sec  33.9 MBytes   284 Mbits/sec    0   1.60 MBytes
[ 4]   7.00-8.00   sec  33.7 MBytes   282 Mbits/sec    0   1.60 MBytes
[ 4]   8.00-9.00   sec  33.5 MBytes   281 Mbits/sec    0   1.60 MBytes
[ 4]   9.00-10.00  sec  33.2 MBytes   279 Mbits/sec    0   1.60 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[ 4]   0.00-10.00  sec   315 MBytes   264 Mbits/sec   37             sender
[ 4]   0.00-10.00  sec   313 MBytes   262 Mbits/sec                  receiver

iperf Done.
$
```

Applications

The IX10 supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. You can also specify Python applications and other scripts to be run each time the device system restarts, at specific intervals, or at a specified time.

This chapter contains the following topics:

Develop Python applications 627
The use(led) function 656
Releasing the LEDs to system control 656
Use Python to control the color of multi-colored LEDs 657
Set up the IX10 to automatically run your applications 666
Start an interactive Python session 676
Run a Python application at the shell prompt 677
Configure scripts to run manually 678
Start a manual script 684
Python versions and corresponding DAL OS firmware versions 685

Develop Python applications

The IX10 features a standard Python 3.6 distribution. Python is a dynamic, object-oriented language for developing software applications, from simple programs to complex embedded applications. Digi offers the Digi IoT PyCharm Plugin to help you while writing, building, and testing your application. See Create and test a Python application.

In addition to the standard Python library, the IX10 includes a set of extensions to access its configuration and interfaces. See Python modules.

The IX10 provides you with the ability to:

- Run Python applications on the device interactively or from a file.
- Specify Python applications and other scripts to be run each time the device system restarts, at specific intervals, or at a specified time. See Configure scripts to run automatically.
- Use pip to install Python packages.

> **Note** Although pip is provided to help facilitate the installation of Python packages, there are limitations in Python package support due to package dependencies, storage limitations, and other issues.

This section contains the following topics:

Set up the IX10 for Python development 628
Create and test a Python application 628
Python modules 632

Set up the IX10 for Python development

1. Access the IX10 local web interface
   a. Use an Ethernet cable to connect the IX10 to your local laptop or PC.
   The factory Setup IP address is **192.168.2.1**
   b. Log into the IX10 WebUI as a user with full admin access rights.
   The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
2. Go to the Configuration window
   a. On the menu, click **System**.
   b. Under **Configuration**, click **Device Configuration**. The Configuration window displays.
3. (Optional) If you want to connect to a local network (LAN) that has a DHCP server
   a. Click **Network** > **Interfaces** > **LAN** > **IPv4**.
   b. Select **DHCP address**.

   For LAN configuration, see the following topics:
   - Change the default LAN subnet
   - Change the LAN address type
   - Allow remote access for web administration and SSH
4. Enable service discovery (mDNS)
   a. Click **Services** > **Service Discovery (mDNS)**.
   b. **Enable** the mDNS service.

Note For more information, see Enable service discovery (mDNS).

5. Configure SSH access
   a. Click **Services** > **SSH**.
   b. Click **Enable**.

Note For more information, see the following topics: Configure SSH access, Use SSH with key authentication, and Allow remote access for web administration and SSH.

6. Enable shell access
   a. Click **Authentication** > **Groups** > **admin**.
   b. Click the **Interactive shell access** option.
   c. If this option is not displayed, see Disable shell access.
7. Click **Apply** to save the configuration and apply the changes.
   The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Create and test a Python application

To develop a Python application for the IX10:

1. Set up the IX10 for Python development.
2. Create and test your application with:

- PyCharm. You can create, build, and remotely launch your application in the IX10.
- Your preferred editor and manually transfer the application, install dependencies, and launch in the IX10.

Develop an application in PyCharm

The Digi IoT PyCharm Plugin allows you to write, build and run Python applications for Digi devices in a quick and easy way. See the Digi XBee PyCharm IDE Plugin User Guide for details.

This is what you can do with it:

- Create Python projects from scratch or import one of the available examples.
- Get help while you write your code thanks to the syntax highlight, quick documentation, and code completion features.
- Build and upload Python applications to your Digi device with just one click.
- Add libraries that facilitate the usage of external peripherals or non-standard APIs.
- Communicate with your Digi device through the integrated SSH console to see the application output or execute quick tests.

Manually install and launch an application

To create, build, and launch your application:

1. Write your Python application code. Code can include:
   - Any Python 3.6 standard feature.
   - Access to the IX10 configuration and hardware with the Python modules.
   - Third-party modules included in the IX10, for example:
     - pySerial 3.4
     - Eclipse Paho MQTT Python Client
   - Any other third-party module implemented in Python.
2. Install the application in **/etc/config/scripts** directory.
3. Launch your application:
   - Run your application at the shell prompt.
   - Configure your application to run automatically.

PyCharm FAQ: My IX10 is not listed in Digi Device Selector

If an IX10 does not appear on the list of the Digi Device Selector:

- Ensure that your device has the mDNS service enabled and is on the same network as the computer. See Set up the IX10 for Python development.
- Or click the link **Click here to add it manually** to specify the IP address, port, username, and password.

Example: Configure a custom port to listen for incoming socket connections

The following example Python script configures a custom port, port 9999, to accept incoming socket connections.

You will also need to add a custom firewall rule to accept the incoming traffic on this port.

Example script

```
import socket
import socketserver

class MyTCPHandler(socketserver.BaseRequestHandler):
    """
    The request handler class for our server.

    It is instantiated once per connection to the server, and must
    override the handle() method to implement communication to the
    client.
    """

    def handle(self):
        # self.request is the TCP socket connected to the client
        self.data = self.request.recv(1024).strip()
        print("{} wrote:".format(self.client_address[0]))
        print(self.data)
        # just send back the same data, but upper-cased
        self.request.sendall(self.data.upper())
```

```
if __name__ == "__main__":
    HOST, PORT ='', 9999

    # Create the server, binding to localhost on port 9999
    with socketserver.TCPServer((HOST, PORT), MyTCPHandler) as server:
        # Activate the server; this will keep running until you
        # interrupt the program with Ctrl-C
        print("Waiting for data...")
        server.serve_forever()
```

Create a custom firewall rule

Web

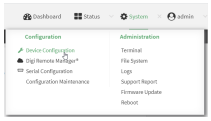
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

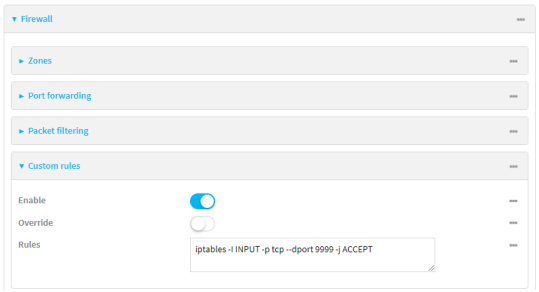
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Firewall** > **Custom rules**.
4. **Enable** the custom rules.
5. For **Rules**, type the following:

   ```
   iptables -I INPUT -p tcp --dport 9999 -j ACCEPT
   ```

6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable custom firewall rules:

```
(config)> firewall custom enable true(config)>
```

4. Set the shell command that will execute the custom firewall rules script:

```
(config)> firewall custom rules "iptables -I INPUT -p tcp --dport 9999 -j ACCEPT"
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Python modules

The IX10 supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. It also offers extensions to manage your IX10:

- The **digidevice** module provides platform-specific extensions that allow you to interact with the device's configuration and interfaces.
  The following submodules are included with the **digidevice** module:
  - LEDs: **digidevice.led**
  - SMS: **digidevice.sms**
  - GPS: **digidevice.location**
  - Digi Remote Manager:
    - **digidevice.datapoint**
    - **digidevice.device_request**
    - **digidevice.name**
  - Device configuration: **digidevice.config**
  - Command line interface: **digidevice.cli**

  - Access runtime database: **digidevice.runt**
  - Set the maintenance window: **digidevice.maintenance**
- Use the Python **serial** module—pySerial—to access the serial ports.
- Eclipse Paho MQTT Python client enables applications to connect to an MQTT broker to publish messages, and to subscribe to topics and receive published messages.

Note Module-related documentation is in the Digidevice module section.

Digidevice module

The Python **digidevice** module provides platform-specific extensions that allow you to interact with the device's configuration and interfaces. The following submodules are included with the **digidevice** module:

This section contains the following topics:

Use digidevice.cli to execute CLI commands

Use the **digidevice.cli** Python module to issue CLI commands from Python to retrieve status and statistical information about the device.

For example, to display the system status and statistics by using an interactive Python session, use the show system command with the **cli** module:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **cli** submodule:

```
>>> from digidevice import cli
>>>
```

4. Execute a CLI command using the **cli.execute(*command*)** function. For example, to print the system status and statistics to stdout using the **show system** command:

```
>>> response = cli.execute("show system")
>>>
>>> print (response)

  Model              : Digi IX10
  Serial Number          : IX10xxxxxxxxyyyyxx
  SKU                : IX10
  Hostname             : IX10
  MAC Address            : DF:DD:E2:AE:21:18

  Hardware Version       : 50001947-01 1P
  Firmware Version       : 25.2
  Alt. Firmware Version    : 25.2
  Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
  Bootloader Version     : 19.7.23.0-15f936e0ed

  Current Time           : Thu, Jan 11, 2024 12:10:00 +0000
  CPU                : 1.4%
  Uptime               : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature            : 40C
  Location             :
  Contact              :

>>>
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Help for using Python to execute IX10 CLI commands

Get help executing a CLI command from Python by accessing help for **cli.execute**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

   ```
   # python
   Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```
3. Import the **cli** submodule:

   ```
   >>> from digidevice import cli
   >>>
   ```
4. Use the help command with **cli.execute**:

   ```
   >>> help(cli.execute)
   Help on function execute in module digidevice.cli:

   execute(command, timeout=5)
   Execute a CLI command with the timeout specified returning the results.
   ...
   ```
5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use digidevice.datapoint to upload custom datapoints to Digi Remote Manager

Use the **datapoint** Python module to upload custom datapoints to Digi Remote Manager.

The following characteristics can be defined for a datapoint:

- Stream ID
- Value
- (Optional) Data type
  - integer
  - long
  - float
  - double
  - string
  - binary
- Units (optional)
- Timestamp (optional)
- Location (optional)

    - Tuple of latitude, longitude and altitude
- Description (optional)
- Quality (optional)
    - An integer describing the quality of the data point

For example, to use an interactive Python session to upload datapoints related to velocity, temperature, and the state of the emergency door:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

   ```
   # python
   Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```
3. Import the **datapoint** submodule and other necessary modules:

   ```
   >>> from digidevice import datapoint
   >>> import time
   >>>
   ```
4. Upload the datapoints to Remote Manager:

   ```
   >>> datapoint.upload("Velocity", 69, units="mph")
   >>> datapoint.upload("Temperature", 24, geo_location=(54.409469, -1.718836, 129))
   >>> datapoint.upload("Emergency_Door", "closed", timestamp=time.time())
   ```
5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

You can also upload multiple datapoints:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

   ```
   # python
   Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```

3. Import the **datapoint** submodule and other necessary modules:

```
>>> from digidevice import datapoint
>>> import time
>>>
```

4. Create datapoint objects:

```
>>> p1 = datapoint.DataPoint("Velocity", 69, units="mph")
>>> p2 = datapoint.DataPoint("Temperature", 24, geo_location=(54.409469, -1.718836, 129))
>>> p3 = datapoint.DataPoint("Emergency_Door", "closed", timestamp=time.time())
>>>
```

5. Upload the datapoints to Remote Manager:

```
>>> datapoint.upload_multiple([p1, p2, p3])
>>>
```

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Once the datapoints have been uploaded to Remote Manager, they can be viewed via Remote Manager or accessed using Web Services calls. See the *Digi Remote Manager Programmers Guide* for more information on web services and datapoints.

Help for using Python to upload custom datapoints to Remote Manager

Get help for uploading datapoints to your Digi Remote Manager account by accessing help for **datapoint.upload** and **datapoint.upload_multiple**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **datapoint** submodule and other necessary modules:

```
>>> from digidevice import datapoint
>>>
```

4. Use the help command with **datapoint.upload**:

```
>>> help(datapoint.upload)
Help on function upload in module digidevice.datapoint:

upload(stream_id:str, data, *, description:str=None, timestamp:float=None, units:str=None,
geo_location:Tuple[float, float, float]=None, quality:int=None,
```

```
data_type:digidevice.datapoint.DataType=None, timeout:float=None)
...
```

5. Use the help command with **datapoint.upload_multiple**:

```
>>> help(datapoint.upload_multiple)
Help on function upload_multiple in module digidevice.datapoint:

upload_multiple(datapoints:List[digidevice.datapoint.DataPoint], timeout:float=None)
...
```

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use digidevice.config for device configuration

Use the **config** Python module to access and modify the device configuration.

Read the device configuration

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **config** submodule:

```
>>> from digidevice import config
>>>
```

4. Use **config.load()** and the **get()** method to return the device's configuration:
   a. Return the entire configuration:

```
>>> from pprint import pprint # use pprint vs. print to make the output easier to read
>>> cfg = config.load()
>>> pprint(cfg.dump().splitlines())
```

   This returns the device configuration:

```
...
network.interface.lan1.device=/network/bridge/lan1
network.interface.lan1.enable=true
network.interface.lan1.ipv4.address=192.168.2.1/24
network.interface.lan1.ipv4.connection_monitor.attempts=3
...
```

   b. Print a list of available interfaces:

```
>>> cfg = config.load()
>>> interfaces = cfg.get("network.interface")
>>> print(interfaces.keys())
```

This returns the following:

```
['setupip', 'setuplinklocal', 'lan1', 'loopback', 'wan1', 'wwan1', 'wwan2']
```

c. Print the IPv4 address of the LAN interface:

```
>>> cfg = config.load()
>>> interfaces = cfg.get(“network.interfaces”)
>>> print(interfaces.get("lan.ipv4.address"))
```

Which returns:

```
192.168.2.1/24
```

Modify the device configuration

Use the **set()** and **commit()** methods to modify the device configuration:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

   ```
   # python
   Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```

3. Import the **config** submodule:

   ```
   >>> from digidevice import config
   >>>
   ```

4. Use **config.load(writable=True)** to enable write mode for the configuration:

   ```
   >>> cfg = config.load(writable=True)
   >>>
   ```

5. Use the **set()** method to make changes to the configuration:

   ```
   >>> cfg.set("system.name", "New-Name")
   >>>
   ```

6. Use the **commit()** method to save the changes:

```
>>> cfg.commit()
True
>>>
```

7. Use the **get()** method to verify the change:

```
>>> print(cfg.get("system.name"))
New-Name
>>>
```

Help for using Python to read and modify device configuration

Get help for reading and modifying the device configuration by accessing help for **digidevice.config**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **config** submodule:

```
>>> from digidevice import config
>>>
```

4. Use the help command with **config**:

```
>>> help(config)
Help on module acl.config in acl:

NAME
acl.config - Python interface to ACL configuration (libconfig).
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use Python to respond to Digi Remote Manager SCI requests

The **device_request** Python module allows you to interact with Digi Remote Manager by using Remote Manager's Server Command Interface (SCI), a web service that allows users to access information and perform commands that relate to their devices.

Use Remote Manager's SCI interface to create SCI requests that are sent to your IX10 device, and use the **device_request** module to send responses to those requests to Remote Manager.

See the *Digi Remote Manager Programmers Guide* for more information on SCI.

Task one: Use the device_request module on your IX10 device to create a response

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **device_request** module:

```
>>> from digidevice import device_request
>>>
```

4. Create a function to handle the request from Remote Manager:

```
>>> def handler(target, request):
    print ("received request %s for target %s" % (request, target))
    return "OK"
>>>
```

5. Register a callbackup function that will be called when the device receives a SCI request from Remote Manager:

```
>>> device_request.register("myTarget", handler)
>>>
```

Note Leave the interactive Python session active while completing task two, below. Once you have completed task two, exit the interactive session by using **Ctrl-D**. You can also exit the session using **exit()** or **quit()**.

Task two: Create and send an SCI request from Digi Remote Manager

The second step in using the **device_request** module is to create an SCI request that Remote Manager will forward to the device. For example, you can create in SCI request a the Remote Manager API explorer:

1. In Remote Manager, click **Documentation** > **API Explorer**.
2. Select the device to use as the SCI target:
   a. Click **SCI Targets**.
   b. Click **Add Targets**.
   c. Enter or select the device ID of the device.
   d. Click **Add**.
   e. Click **OK**.

3. Click **Examples** > **SCI** > **Data Service** > **Send Request**.

   Code similar to the following will be displayed in the HTTP message body text box:

```
<sci_request version="1.0">
  <data_service>
  <targets>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
  </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

   Note The value of the **target_name** parameter in the **device_request** element must correspond to the **target** parameter of the **device_request.register** function in the Python script. In this example, the two are the same.

4. Click **Send**.

   Once that the request has been sent to the device, the handler on the device is executed.

   - On the device, you will receive the following output:

```
>>> received request
      my payload string
     for target myTarget
>>>
```

   - In Remote Manager, you will receive a response similar to the following:

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
      <requests>
        <device_request target_name="myTarget" status="0">OK</device_request>
      </requests>
    </device>
  </data_service>
</sci_request>
```

Example: Use digidevice.cli with digidevice.device_request

In this example, we will use the **digidevice.cli** module in conjunction with the **digidevice.device_request** module to return information about multiple devices to Remote Manager.

1. Create a Python application, called showsystem.py, that uses the **digidevice.cli** module to create a response containing information about device and the **device_request** module to respond with this information to a request from Remote Manager:

```
from digidevice import device_request
from digidevice import cli
```

```
import time

def handler(target, request):
  return cli.execute("show system verbose")

def status_cb(error_code, error_description):
  if error_code != 0:
    print("error handling showSystem device request: %s" % error_description)

device_request.register("showSystem", handler, status_callback = status_cb)

# Do not let the process finish so that it handles device requests
while True:
  time.sleep(10)
```

2. Upload the showsystem.py application to the /etc/config/scripts directory on two or more Digi devices. In this example, we will upload it to two devices, and use the same request in Remote Manager to query both devices.

   See Configure scripts to run automatically for information about uploading Python applications to your device. You can also create the script on the device by using the **vi** command when logged in with shell access.

3. For both devices:
   a. Configure the device to automatically run the showsystem.py application on reboot, and to restart the application if it crashes. This can be done from either the WebUI or the command line:

      Web

      i. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

      ii. Access the device configuration:

      Remote Manager:

      i. Locate your device as described in Use Digi Remote Manager to view and manage your device.

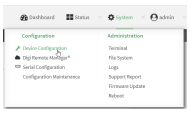
      ii. Click the **Device ID**.

      iii. Click **Settings**.

      iv. Click to expand **Config**.

      Local Web UI:

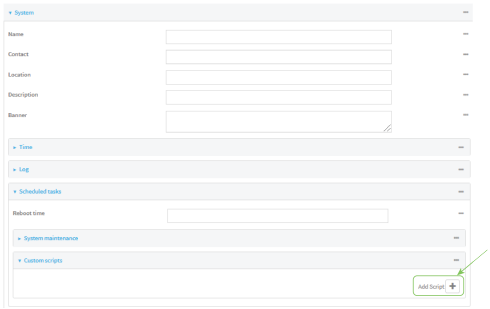
      i. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

      The **Configuration** window is displayed.

      iii. Click **System** > **Scheduled tasks** > **Custom scripts**.

iv. Click to add a custom script.

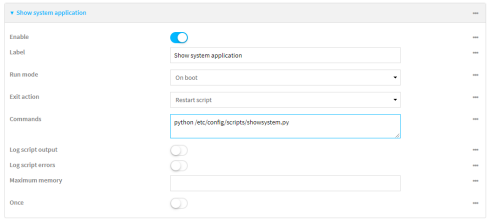


v. For **Label**, type **Show system application**.

vi. For **Run mode**, select **On boot**.

vii. For **Exit action**, select **Restart script**.

viii. For **Commands**, type **python /etc/config/scripts/showsystem.py**.



ix. Click **Apply** to save the configuration and apply the change.

Command line

i. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

ii. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

iii. Add an application entry:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

Scheduled scripts are enabled by default. To disable:

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

iv. Provide a label for the script:

```
(config system schedule script 0)> label "Show system application"
```

v. Configure the application to run automatically when the device reboots:

```
(config system schedule script 0)> when boot
(config system schedule script 0)>
```

vi. Configure the application to restart if it crashes:

```
(config system schedule script 0)> exit_action restart
(config system schedule script 0)>
```

vii. Set the command that will execute the application:

```
(config system schedule script 0)> commands "python /etc/config/scripts/showsystem.py"
(config system schedule script 0)>
```

viii. Save the configuration and apply the change:

```
(config)> save
Configuration saved.
>
```

b. Run the showsystem.py application. You can run the application by either rebooting the device, or by running it from the shell prompt.

- To reboot the device:
  i. From the WebUI:
     i. From the main menu, click **System**.
     ii. Click **Reboot**.
  i. From the command line, at the Admin CLI prompt, type:

```
> reboot
```

- To run the application from the shell prompt:
  i. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
  ii. Type the following at the shell prompt:

```
# python /etc/config/scripts/showsystem.py &
#
```

  iii. Exit the shell:

```
# exit
```

4. In Remote Manager, click **Documentation** > **API Explorer**.
5. Select the devices to use as the SCI targest:
   a. Click **SCI Targets**.
   b. Click **Add Targets**.
   c. Enter or select the device ID of one of the devices.
   d. Click **Add**.
   e. Enter or select the device ID of the second device and click **Add**.
   f. Click **OK**.
6. Click **Examples** > **SCI** > **Data Service** > **Send Request**.

   Code similar to the following will be displayed in the HTTP message body text box:

```
<sci_request version="1.0">
  <data_service>
  <targets>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    <device id="00000000-00000000-0000FFFF-485740BC"/>
  </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

7. For the **device_request** element, replace the value of **target_name** with **showSystem**. This matches the **target** parameter of the **device_request.register** function in the showsystem.py application.

```
      <device_request target_name="showSystem">
```

8. Click **Send**.

   You should receive a response similar to the following:

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
      <requests>
        <device_request target_name="showSystem" status="0">Model              : Digi IX10
          Serial Number        : IX10-000068
          Hostname             : IX10
          MAC                  : 00:40:D0:13:35:36

          Hardware Version     : 50001959-01 A
          Firmware Version     : 25.2
          Bootloader Version   : 1
          Firmware Build Date  : Fri, Jan 12, 2024 12:10:00
          Schema Version       : 461

          Timezone             : UTC
          Current Time         : Thu, Jan 11, 2024 12:10:00
```

```
      CPU                : 1.1
      Uptime             : 1 day, 21 hours, 49 minutes, 47 seconds (164987s)
      Temperature        : 39C

      Contact            : Jane Smith

      Disk
      ----
      Load Average       : 0.10, 0.05, 0.00
      RAM Usage          : 85.176MB/250.484MB(34%)
      Disk /etc/config Usage  : 0.068MB/13.416MB(1%)
      Disk /opt Usage    : 47.724MB/5309.752MB(1%)
      Disk /overlay Usage     : MB/MB(%)
      Disk /tmp Usage    : 0.004MB/40.96MB(0%)
      Disk /var Usage    : 0.820MB/32.768MB(3%)</device_request>
    </requests>
  </device>
  <device id="00000000-00000000-0000FFFF-485740BC"/>
    <requests>
      <device_request target_name="showSystem" status="0">Model              : Digi IX10
      Serial Number      : IX10-000023
      Hostname           : IX10
      MAC                : 00:40:D0:26:79:1C

      Hardware Version   : 50001959-01 A
      Firmware Version   : 25.2
      Bootloader Version : 1
      Firmware Build Date     : Fri, Jan 12, 2024 12:10:00
      Schema Version     : 461

      Timezone           : UTC
      Current Time       : Thu, Jan 11, 2024 12:10:00
      CPU                : 1.1
      Uptime             : 4 day, 13 hours, 43 minutes, 22 seconds (395002s)
      Temperature        : 37C

      Contact            : Omar Ahmad
      Disk
      ----
      Load Average       : 0.10, 0.05, 0.00
      RAM Usage          : 85.176MB/250.484MB(34%)
      Disk /etc/config Usage  : 0.068MB/13.416MB(1%)
      Disk /opt Usage    : 47.724MB/5309.752MB(1%)
      Disk /overlay Usage     : MB/MB(%)
      Disk /tmp Usage    : 0.004MB/40.96MB(0%)
      Disk /var Usage    : 0.820MB/32.768MB(3%)</device_request>
    </requests>
  </device>
 </data_service>
</sci_request>
```

Help for using Python to respond to Digi Remote Manager SCI requests

Get help for respond to Digi Remote Manager Server Command Interface (SCI) requests by accessing help for **digidevice.device_request**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **device_request** submodule:

```
>>> from digidevice import device_request
>>>
```

4. Use the help command with **device_request**:

```
>>> help(device_request)
Help on module digidevice.device_request in digidevice:

NAME
digidevice.device_request - APIs for registering device request handlers
...
```

You can also use the help command with available **device_request** functions:

- Use the help command with **device_request.register**:

```
>>> help(device_request.register)
Help on function register in module digidevice.device_request:

register(target:str, response_callback:Callable[[str, str], str], status_callback:Callable[[int, str], NoneType]=None, xml_encoding:str='UTF-8')
...
```

- Use the help command with **device_request.unregister**:

```
>>> help(device_request.unregister)
Help on function unregister in module digidevice.device_request:

unregister(target:str) -> bool
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use digidevice runtime to access the runtime database

Use the **runt** submodule to access and modify the device runtime database.

Read from the runtime database

Use the **keys()** and **get()** methods to read the device configuration:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **runt** submodule:

```
>>> from digidevice import runt
>>>
```

4. Use the **start()** method to open the runtime database:

```
>>> runt.start()
>>>
```

5. Use the **keys()** method to display available keys in the runtime database, and use the **get()** method to print information from the runtime database:
   a. Print available keys:

   ```
   >>> print(runt.keys(""))
   ```

   This returns available keys:

   ```
   ['advanced', 'drm', 'firmware', 'location', 'manufacture', 'metrics', 'mm', 'network', 'pam', 'serial', 'system']
   ```

   b. Print available keys for the system key:

   ```
   >>> print(runt.keys("system"))
   ```

   This will return the following:

   ```
   ['boot_count', 'chassis', 'cpu_temp', 'cpu_usage', 'disk', 'load_avg', 'local_time', 'mac', 'mcu', 'model', 'ram', 'serial', 'uptime']
   ```

   c. Use the **get()** method to print the device's MAC address:

   ```
   >>> print(runt.get("system.mac"))
   ```

   This will return the MAC address of the device.
6. Use the **stop()** method to close the runtime database:
7. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Modify the runtime database

Use the **set()** method to modify the runtime database:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a

user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **runt** submodule:

```
>>> from digidevice import runt
>>>
```

4. Use **start()** method to open the runtime database:

```
>>> runt.start()
>>>
```

5. Use the **set()** method to make changes to the runtime database:

```
>>> runt.set("my-variable", "my-value")
>>>
```

6. Use the **get()** method to verify the change:

```
>>> print(runt.get("my-variable"))
my-variable
>>>
```

7. Close the runtime database:

```
>>> runt.stop()
>>>
```

8. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Help for using Python to access the runtime database

Get help for reading and modifying the device runtime database by accessing help for **digidevice.runt**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **runt** submodule:

```
>>> from digidevice import runt
>>>
```

4. Use the help command with **runt**:

```
>>> help(runt)

Help on module acl.runt in digidevice:

NAME
acl.runt - Python interface to ACL runtime database (runtd).
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use Python to upload the device name to Digi Remote Manager

The **name** submodule can be used to upload a custom name for your device to Digi Remote Manager.

When you use the **name** submodule to upload a custom device name to Remote Manager, the following issues apply:

- If the name is being used by to another device in your Remote Manager account, the name will be removed from the previous device and added to the new device.
- If Remote Manager is configured to apply a profile to a device based on the device name, changing the name of the device may cause Remote Manager to automatically push a profile onto the device.

Together, these two features allow you to swap one device for another by using the **name** submodule to change the device name, while guaranteeing that the new device will have the same configuration as the previous one.

Note Because causing a profile to be automatically pushed from Remote Manager may change the behavior of the device, including overwriting existing usernames and passwords, the **name** submodule should be used with caution. As a result, support for this functionality is disabled by default on Remote Manager.

Enable support on Digi Remote Manager for uploading custom device names

1. In Remote Manager, click **API Explorer**.
2. For the HTTP method, select **PUT**.
3. For **Enter and API or select an example**, type **/ws/v1/settings/inventory/AllowDeviceToSetOwnNameEnabled**.

4. In the HTTP message body text box, type the following:

```
{
  "name" : "AllowDeviceToSetOwnNameEnabled",
  "value" : "true"
}
```

5. Click **Send**.

Upload a custom name

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **name** submodule:

```
>>> from digidevice import name
```

4. Upload the name to Remote Manager:

```
>>> name.upload("my_name")
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Help for uploading the device name to Digi Remote Manager

Get help for uploading the device name to Digi Remote Managerby accessing help for **digidevice.name**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **name** submodule:

```
>>> from digidevice import name
>>>
```

4. Use the help command with **name**:

```
>>> help(name)

Help on module digidevice.name in digidevice:

NAME
digidevice.name - API for uploading name from the device
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use Python to set the maintenance window

The **maintenance** Python module allows you to set the service state of a device. When the module sets the device to out of service, this can be used as trigger to begin maintenance activity. See Schedule system maintenance tasks for more details.

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **maintenance** module:

```
>>> from digidevice import maintenance
>>>
```

4. To determine the current service state of the device:

```
>>> maintenance.state()
'IN_SERVICE'
>>>
```

5. To set the device to out of service:

```
>>> maintenance.out_of_service()
>>> maintenance.state()
'OUT_OF_SERVICE'
>>>
```

6. To set the device to in service:

```
>>> maintenance.in_service()
>>> maintenance.state()
'IN_SERVICE'
>>>
```

Note Leave the interactive Python session active while completing task two, below. Once you have completed task two, exit the interactive session by using **Ctrl-D**. You can also exit the session using **exit()** or **quit()**.

Help for the digidevice maintenance module

Get help for the **digidevice** maintenance module:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **maintenance** submodule:

```
>>> from digidevice import maintenance
>>>
```

4. Use the help command with **maintenance** :

```
>>> help(maintenance )
Help on module digidevice.maintenance in digidevice:

NAME
  digidevice.maintenance

DESCRIPTION
  API for setting the device's service state. The service state is stored
  in runt.
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

The digidevice led submodule

Use the **led** submodule to redefine the purpose of any front-panel LED on the IX10 device. With this submodule, you can:

- Gain control of the LED with the led.acquire() function.
- Define the state of the LED with the led.set() function.
- Use the use() function to create a function that acquires, sets, and releases an LED.
- Optionally release control of the LED with the led.release() function.

See The use(led) function for instructions on using these methods.

Available LEDs

LED		Attribute name	Color
All available LEDs		Led.ALL	
Online indicator		Led.LAN3_RX	Blue
SIM indicator		Led.SIM_FAIL	Red
		Led.SIM1	Green
		Led.SIM2	Blue
LTE connection indicator		Led.COM	Red
		Led.ETH	Green
		Led.ONLINE	Blue
Signal strength indicators	1	Led.RSS1	Green
	2	Led.RSS2	
	3	Led.RSS3	
	4	Led.RSS4	
	5	Led.RSS5	

Available LED states

State	Attribute name
Solid on	State.ON
Off	State.OFF
Flash	State.FLASH

Use Python to set the state of LEDs

The following example uses an interactive Python session to set the state of all LEDs to flashing:

1. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

2. Import the **led** submodule:

```
>>> from digidevice import led
```

3. Import the **Led** and **State** objects from the **led** submodule:

```
>>> from digidevice.led import Led, State
```

4. Use led.acquire() to gain control of the all LEDs:

```
>>> led.acquire(Led.ALL)
```

5. Use led.set() to set the state of the LEDs:

```
>>> led.set(Led.ALL, State.FLASH)
```

6. (Optional) Use led.release() to release the LEDs to system control:

```
>>> led.release(Led.ALL)
```

7. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

The use(led) function

The use(led) function can be used to acquire control of LEDs and then release them back to system control.

To create a function that acquires control of the power LED, sets it to a state of fast flashing, and then releases control when the function has completed, use the following code in a python application:

```
with use(Led.POWER) as pwr:
  pwr(State.FLASH)
```

Releasing the LEDs to system control

During a Python interactive session, or from within a Python script, you can release control of the LED from Python to system control using the led.release() method.

If the Python script or session terminates prior to releasing control to the system, the LEDs will continue to have the state that Python set to them, until the device is rebooted. See Configure scripts to run automatically for information about configuring the device so that the LED state is controlled by the Python script even after reboot.

If any system processes attempt to take control of the LED while Python is in control of it, the state information from the system process is recorded but the LED state is not updated until Python releases control of the LED. When the LED is returned to system control, the state of the LED will reflect the correct, recorded state information.

Setting the state of multi-colored LEDs.

Use Python to control the color of multi-colored LEDs

One or more LEDs in the IX10 are RGB (red, green, and blue) LEDs, capable of producing a wide range of colors. You can use the digidevice.led Python module to control the color as well as the state of these LEDs.

For example, the LTE connection indicator can be set to various colors:

LED attribute name	Color	State
Led.COM	Red	ON
Led.ETH		OFF
Led.ONLINE		OFF
Led.COM	Red flashing	FLASH
Led.ETH		OFF
Led.ONLINE		OFF
Led.COM	Green	OFF
Led.ETH		ON
Led.ONLINE		OFF
Led.COM	Green flashing	OFF
Led.ETH		FLASH
Led.ONLINE		OFF
Led.COM	Blue	OFF
Led.ETH		OFF
Led.ONLINE		ON
Led.COM	Blue flashing	OFF
Led.ETH		OFF
Led.ONLINE		FLASH
Led.COM	White	ON
Led.ETH		ON
Led.ONLINE		ON
Led.COM	White flashing	FLASH
Led.ETH		FLASH
Led.ONLINE		FLASH

LED attribute name	Color	State
Led.COM	Yellow	ON
Led.ETH		ON
Led.ONLINE		OFF
Led.COM	Yellow flashing	FLASH
Led.ETH		FLASH
Led.ONLINE		OFF
Led.COM	Purple	ON
Led.ETH		OFF
Led.ONLINE		ON
Led.COM	Purple flashing	FLASH
Led.ETH		OFF
Led.ONLINE		FLASH
Led.COM	Cyan	OFF
Led.ETH		ON
Led.ONLINE		ON
Led.COM	Cyan flashing	OFF
Led.ETH		FLASH
Led.ONLINE		FLASH

See The digidevice led submodule for a definition of the IX10's LEDs, including RGB leds, and the names of the attributes for each LED that will be used by the digidevice.led module.

Example: Set the LTE connection indicator to flashing purple

1. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

2. Import the **led** submodule:

```
>>> from digidevice import led
```

3. Import the **Led** and **State** objects from the **led** submodule:

```
>>> from digidevice.led import Led, State
```

4. Use led.acquire() to gain control of the all LEDs:

```
>>> led.acquire(Led.ALL)
```

5. Use led.set() to set the state of the Led.COM and Led.ONLINE to FLASH:

```
>>> led.set(Led.COM, State.FLASH)
>>> led.set(Led.ONLINE, State.FLASH)
```

6. Set the state of the Led.ETH to OFF:

```
>>> led.set(Led.ETH, State.OFF)
```

7. (Optional) Use led.release() to release the LEDs to system control:

```
>>> led.release(Led.ALL)
```

8. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use Python to send and receive SMS messages

You can create Python scripts that send and receive SMS message in tandem with the Digi Remote Manager by using the digidevice.sms module. To use a script to send or receive SMS messages, you must also enable the ability to schedule SMS scripting.

Enable the ability to schedule SMS scripting

Web

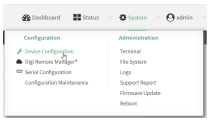
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

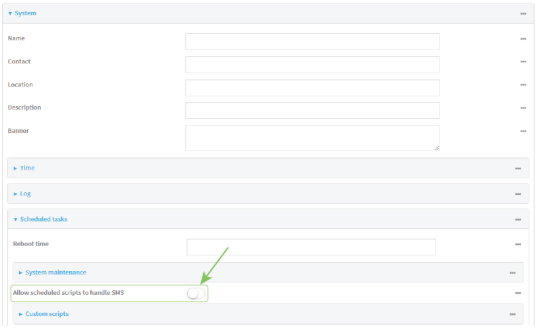
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System** > **Scheduled tasks**.
4. Click to enable **Allow scheduled scripts to handle SMS**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> system schedule sms_script_handling true
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See Configure scripts to run automatically for more information about scheduling scripts.

Example digidevice.sms script

The following example script receives an SMS message and sends a response:

```
#!/usr/bin/python3.10.1


import os
import threading
```

```
import sys
from digidevice.sms import Callback, send
COND = threading.Condition()

def sms_test_callback(sms, info):
    print(f"SMS message from {info['content.number']} received")
    print(sms)
    print(info)
    COND.acquire()
    COND.notify()
    COND.release()

def send_sms(destination, msg):
    print("sending SMS message", msg)
    if len(destination) == 10:
        destination = "+1" + destination
    send(destination, msg)

if __name__ == '__main__':
    if len(sys.argv) > 1:
        dest = sys.argv[1]
    else:
        dest = '+15005550006'
    my_callback = Callback(sms_test_callback, metadata=True)
    send_sms(dest, 'Hello World!')
    print("Please send an SMS message now.")
    print("Execution halted until a message is received or 60 seconds have passed.")
    # acquire the semaphore and wait until a callback occurs
    COND.acquire()
    try:
        COND.wait(60.0)
    except Exception as err:
        print("exception occured while waiting")
        print(err)
    COND.release()
    my_callback.unregister_callback()
```

Example script using digidevice.sms to send CLI commands

The following example script listens for an incoming SMS message from a specific phone number (2223334444) and then executes the SMS message as a CLI command. If the CLI command being run has output, it will send that output as a response SMS message. If the CLI command being run has no output but ran successfully, the script will instead send an OK response SMS message. Errors in running the CLI will have those error messages sent as a SMS response.

```
#!/usr/bin/python

# Take an incoming SMS message from a specified phone number and run it as
# a CLI command. Send a reponse SMS to the sender before running the command

import os
import threading
import sys
from digidevice import cli
from digidevice.sms import Callback, send
COND = threading.Condition()
allowed_incoming_phone_number = '2223334444'

def sms_test_callback(sms, info):
```

```
    if info['content.number'] == allowed_incoming_phone_number:
        print(f"SMS message from {info['content.number']} received")
        print(sms)
        print(info)
        #if sms == "Reboot":
        #  send_sms(dest, 'Reboot message received, rebooting device...')
        #  response = cli.execute("reboot")
        #  print (response)
        send_sms(dest, 'Message received (' + sms + ').  Performing as CLI command...')
        response = cli.execute(sms)
        if not response:
            response = 'OK'
        send_sms(dest, 'CLI results: ' + response)
        print (response)
    COND.acquire()
    COND.notify()
    COND.release()

def send_sms(destination, msg):
    print("sending SMS message", msg)
    if len(destination) == 10:
    destination = "+1" + destination
    send(destination, msg)

if __name__ == '__main__':
    if len(sys.argv) > 1:
        dest = sys.argv[1]
    else:
        dest = allowed_incoming_phone_number
    my_callback = Callback(sms_test_callback, metadata=True)
    #send_sms(dest, 'Ready to receive incoming SMS message')
    print("Waiting up to 60 seconds for incoming SMS message")
    # acquire the semaphore and wait until a callback occurs
    COND.acquire()
    try:
        COND.wait(60.0)
    except Exception as err:
        print("exception occured while waiting")
        print(err)
    COND.release()
    my_callback.unregister_callback()
    os.system('rm -f /var/run/sms/scripts/*') # remove all stored SMS messages, since we've processed them
    print("SMS script finished.  Please re-run if you want to check for more incoming SMS messages")
    os._exit(0)
```

Use Python to access serial ports

You can use the Python **serial** module to access serial ports on your IX10 device that are configured to be in Application mode. See Configure Application mode for a serial port for information about configuring a serial port in Application mode.

To use Python to access serial ports:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. Determine the path to the serial port:

```
# ls /dev/serial/
by-id  by-path  port1
#
```

3. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

4. Import the **serial** module:

```
>>> import serial
>>>
```

5. You can now perform operations on the serial port. For example, to write a message to the serial port:

```
>>> s = serial.Serial("/dev/serial/port1", 115200)
>>> s.write(b"Hello from serial port")
26
>>>
```

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use the Paho MQTT python library

Your IX10 device includes support for the Paho MQTT python library. MQTT is a lightweight messaging protocol used to communicate with various applications including cloud-based applications such as Amazon Web Services and Microsoft Azure. The following is example code that reads CPU and RAM usage on the device, updates the device firmware, then publishes information about DHCP clients and system information to the MQTT server at 192.168.1.100. The MQTT server IP is configurable.

```
"""
MQTT client example:
- Reporting some device metrics from runt
- Reporting DHCP clients
- Firmware update feature (simple implementation, read TODO in cmd_fwupdate)
"""

import sys
import time
import paho.mqtt.client as mqtt
import json
from acl import runt, config
from http import HTTPStatus
import urllib.request
import tempfile
import os
from digidevice import cli
```

```
POLL_TIME = 60

def cmd_reboot(params):
   print("Rebooting unit...")
   try:
      cli.execute("reboot", 10)
   except:
      print("Failed to run 'reboot' command")
      return HTTPStatus.INTERNAL_SERVER_ERROR

return HTTPStatus.OK

def cmd_fwupdate(params):
   try:
      fw_uri = params["uri"]
   except:
      print("Firmware file URI not passed")
      return HTTPStatus.BAD_REQUEST

   print("Request to update firmware with URI: {}".format(fw_uri))

     try:
      fd, fname = tempfile.mkstemp()
      os.close(fd)
      try:
         urllib.request.urlretrieve(fw_uri, fname)
      except:
         print("Failed to download FW file from URI {}".format(fw_uri))
         return HTTPStatus.NOT_FOUND

      try:
         ret = cli.execute("system firmware update file " + fname, 60)
      except:
         print("Failed to run firmware update command")
         return HTTPStatus.INTERNAL_SERVER_ERROR

      if not "Firmware update completed" in ret:
         print("Failed to update firmware")
         return HTTPStatus.INTERNAL_SERVER_ERROR
   finally:
      os.remove(fname)

   print("Firmware update finished")

   return HTTPStatus.OK

CMD_HANDLERS = {
   "reboot": cmd_reboot,
   "fw-update": cmd_fwupdate
}


def send_cmd_reply(client, cmd_path, cid, cmd, status):
   if not status or not cid:
      return

   if cmd_path.startswith(PREFIX_CMD):
      path = cmd_path[len(PREFIX_CMD):]
   else:
      print("Invalid command path ({}), cannot send reply".format(cmd_path))
```

```
        return

    reply = {
        "cmd": cmd,
        "status": status
    }

    client.publish(PREFIX_RSP + path + "/" + cid, json.dumps(reply, separators=(',',':')))

def on_connect(client, userdata, flags, rc):
    print("Connected to MQTT server")
    client.subscribe(PREFIX_CMD + "/system")

def on_message(client, userdata, msg):
    """ Supporting only a single topic for now, no need for filters
    Expects the following message format:
    {
        "cid": "<client-id>",
        "cmd": "<command>",
        "params": {
            <optional_parameters>
        }
    }

    Supported commands:
    - "fw-update"
        params:
            - "uri": "<firmware_file_URL>"
    - "reboot"
        params:
    """

    try:
        m = json.loads(msg.payload)
        cid = m["cid"]
        cmd = m["cmd"]
        try:
            payload = m["params"]
        except:
            payload = None
    except:
        print("Invalid command format: {}".format(msg.payload))
        if not cid:
            # Return if client-ID not passed
            return None
        send_cmd_reply(client, msg.topic, cid, cmd, HTTPStatus.BAD_REQUEST)

    try:
        status = CMD_HANDLERS[cmd](payload)
    except:
        print("Invalid command: {}".format(cmd))
        status = HTTPStatus.NOT_IMPLEMENTED

    send_cmd_reply(client, msg.topic, cid, cmd, status)


def publish_dhcp_leases():
    leases = []
    try:
        with open('/etc/config/dhcp.leases', 'r') as f:
```

```
            for line in f:
                elems = line.split()
                if len(elems) != 5:
                    continue
                leases.append({"mac": elems[1], "ip": elems[2], "host": elems[3]})
        if leases:
            client.publish(PREFIX_EVENT + "/leases", json.dumps(leases, separators=(',',':')))
    except:
        print("Failed to open DHCP leases file")

def publish_system():
    avg1, avg5, avg15 = runt.get("system.load_avg").split(', ')
    ram_used = runt.get("system.ram.per")
    disk_opt = runt.get("system.disk./opt.per")
    disk_config = runt.get("system.disk./etc/config.per")

    msg = json.dumps({
        "load_avg": {
            "1min": avg1,
            "5min": avg5,
            "15min": avg15
        },
        "disk_usage": {
            "/opt": disk_opt,
            "/etc/config:": disk_config,
            "ram": ram_used
        }
    })

    client.publish(PREFIX_EVENT + "/system", json.dumps(msg))

runt.start()
serial = runt.get("system.serial")

PREFIX = "router/" + serial
PREFIX_EVENT = "event/" + PREFIX
PREFIX_CMD = "cmd/" + PREFIX
PREFIX_RSP = "rsp/" + PREFIX

client = mqtt.Client()
client.on_connect = on_connect
client.on_message = on_message

try:
    client.connect("192.168.1.100", 1883, 60)
    client.loop_start()
except:
    print("Failed to connect to MQTT server")
    sys.exit(1)

while True:
    publish_dhcp_leases()
    publish_system()
    time.sleep(POLL_TIME)
```

Set up the IX10 to automatically run your applications

This section contains the following topics:

- Configure scripts to run automatically
- Show script information
- Stop a script that is currently running

Configure scripts to run automatically

You can configure a script or a python application to run automatically when the system restarts, at specific intervals, or at a specified time. By default, scripts execute in a "sandbox," which restricts access to the file system and available commands that can be used by the script.

Required configuration items

- Upload or create the script. The script must be uploaded to /etc/config/scripts or a subdirectory.
- Enable the script.
- Select whether the script should run:
  - When the device boots.
  - At a specified time.
  - At a specified interval.
  - During system maintenance.

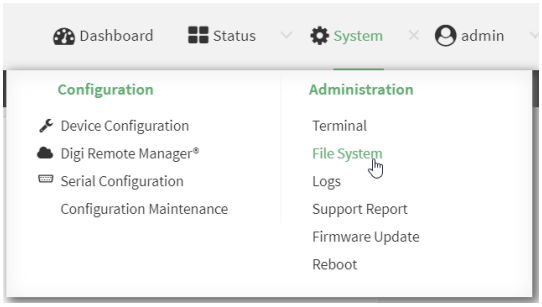
Additional configuration items

- If the script is a Python application, include the full path to the script.
- A label used to identify the script.
- The action to take if the script finishes. The actions that can be taken are:
  - None.
  - Restart the script.
  - Reboot the device.
- Whether to write the script output and errors to the system log.
- If the script is set to run at a specified interval, whether another instance of the script should be run at the specified interval if the previous instance is still running.
- The memory available to be used by the script .
- Whether the script should run one time only.

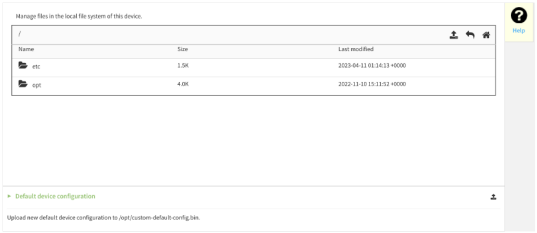
Task one: Upload the application

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight the **scripts** directory and click ⏏ to open the directory.
3. Click ❽ (upload).
4. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, use the scp command to upload the Python application script to the IX10 device:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

   where:

   - *hostname-or-ip* is the hostname or IP address of the remote host.
   - *username* is the name of the user on the remote host.
   - *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
   - *local-path* is the location on the IX10 device where the copied file will be placed.

   For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the /etc/config/scripts directory on the IX10 device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local /etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                 100%   36MB   11.1MB/s      00:03
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Note You can also create scripts by using the **vi** command when logged in with shell access.

Task two: Configure the application to run automatically

Note This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

Web

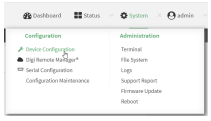
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

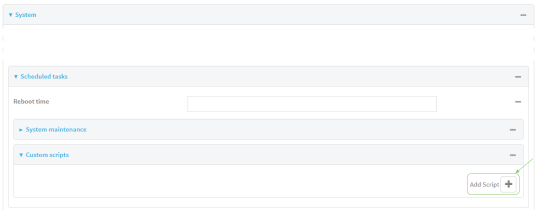
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

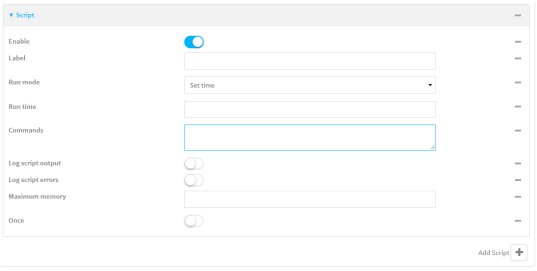
   

   The **Configuration** window is displayed.
3. Click **System** > **Scheduled tasks** > **Custom scripts**.

4. For **Add Script**, click .



The script configuration window is displayed.



Custom scripts are enabled by default. To disable, toggle off **Enable** to toggle off.

5. (Optional) For **Label**, provide a label for the script.
6. For **Run mode**, select the mode that will be used to run the script. Available options are:
   - **On boot**: The script will run once each time the device boots.
     - If **On boot** is selected, select the action that will be taken when the script completes in **Exit action**. Available options are:
       - **None**: Action taken when the script exits.
       - **Restart script**: Runs the script repeatedly.
       - **Reboot**: The device will reboot when the script completes.
   - **Interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved.
     - If **Interval** is selected, in **Interval**, type the interval.

       Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

       For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
     - Click to enable **Run single** to run only a single instance of the script at a time.

       If **Run single** is not enabled, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.
   - **Set time**: Runs the script at a specified time of the day.
     - If **Set Time** is selected, specify the time that the script should run in **Run time**, using the format *HH*:*MM*.
   - **During system maintenance**: The script will run during the system maintenance time window.
7. For **Commands**, type the commands that will execute the script.

- If a Python script is being used, include the full path to the Python script. For example:

```
python /etc/config/scripts/test.py
```

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

8. Script logging options:
   a. Click to enable **Log script output** to log the script's output to the system log.
   b. Click to enable **Log script errors** to log script errors to the system log.

   If neither option is selected, only the script's exit code is written to the system log.
9. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{**b**|**bytes**|**KB**|**k**|**MB**|**MB**|**M**|**GB**|**G**|**TB**|**T**}.
10. **Sandbox** is enabled by default, which restricts access to the file system and available commands that can be used by the script. This option protects the script from accidentally destroying the system it is running on.
11. Click to enable **Once** to configure the script to run only once at the specified time.

    If **Once** is enabled, rebooting the device will cause the script to not run again. The only way to re-run the script is to:
    - Remove the script from the device and add it again.
    - Make a change to the script.
    - Uncheck **Once**.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a script:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

   Scheduled scripts are enabled by default. To disable:

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

4. (Optional) Provide a label for the script.

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

where *value* is any string. if spaces are used, enclose *value* within double quotes.

5. Set the mode that will be used to run the script:

```
(config system schedule script 0)> when mode
(config system schedule script 0)>
```

where *mode* is one of the following:

- **boot**: The script will run once each time the device boots.
  - If **boot** is selected, set the action that will be taken when the script completes:

    ```
    (config system schedule script 0)> exit_action action
    (config system schedule script 0)>
    ```

    where *action* is one of the following:
    - **none**: Action taken when the script exits.
    - **restart**: Runs the script repeatedly.
    - **reboot**: The device will reboot when the script completes.
- **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected:
  - Set the interval:

    ```
    (config system schedule script 0)> on_interval value
    (config system schedule script 0)>
    ```

    where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

    For example, to set **on_interval** to ten minutes, enter either **10m** or **600s**:

    ```
    (config system schedule script 0)> on_interval 600s
    (config system schedule script 0)>
    ```

  - (Optional) Configure the script to run only a single instance at a time:

    ```
    (config system schedule script 0)> once true
    (config system schedule script 0)>
    ```

    If **once** is set to **false**, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.
- **set_time**: Runs the script at a specified time of the day.
  - If **set_time** is set, set the time that the script should run, using the format *HH:MM*:

    ```
    (config system schedule script 0)> run_time HH:MM
    (config system schedule script 0)>
    ```

- **maintenance_time**: The script will run during the system maintenance time window.

6. Set the commands that will execute the script:

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

where *filename* is the path and filename of the script, and any related command line information.

- If a Python script is being used, include the full path to the Python script and enclose in quotation marks. For example:

```
(config system schedule script 0)> commands python "/etc/config/scripts/test.py"
(config system schedule script 0)>
```

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

7. Script logging options:
   - To log the script's output to the system log:

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

   - To log script errors to the system log:

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

   If **syslog_stdout** and **syslog_stderr** are not enabled, only the script's exit code is written to the system log.

8. Set the maximum amount of memory available to be used by the script and its subprocesses:

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

where *value* uses the syntax ***number***{**b|bytes|KB|k|MB|MB|M|GB|G|TB|T**}.

9. To run the script only once at the specified time:

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:

- Remove the script from the device and add it again.
- Make a change to the script.
- Disable **once**.

10. **Sandbox** is enabled by default. This option protects the script from accidentally destroying the system it is running on.

```
(config system schedule script 0)> sandbox true
(config system schedule script 0)>
```

11. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show script information

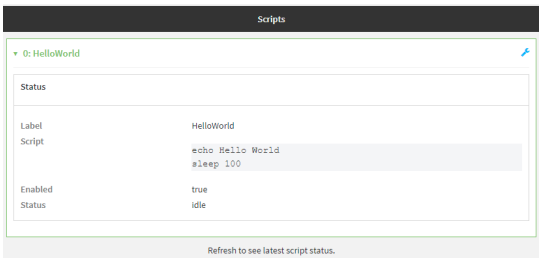
You can view status and statistics about location information from either the WebUI or the command line.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show scripts command at the system prompt:

```
> show scripts

 Index  Label      Enabled  Status  Run time
 -----  ---------- -------  ------  --------
 0      script1    true     active
 1      script2    true     idle    01:00
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Stop a script that is currently running

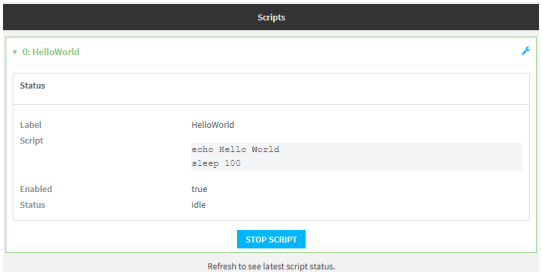
You can stop a script that is currently running.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



2. For scripts that are currently running, click **Stop Script** to stop the script.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Determine the name of scripts that are currently running:

```
> show scripts

 Index  Label      Enabled  Status  Run time
 -----  ---------- -------  ------  --------
 0      script1    true     active
 1      script2    true     idle    01:00
>
```

   Scripts that are currently running have the status of **active**.

3. Stop the appropriate script:

```
)> system script stop script1
>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Start an interactive Python session

Use the **python** command without specifying any parameters to start an interactive Python session. The Python session operates interactively using REPL (Read Evaluate Print Loop) to allow you to write Python code on the command line.

Note The Python interactive session is not available from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See Authentication groups for information about configuring authentication groups that include shell access.

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Type Python commands at the Python prompt. For example, to view help for the digidevice module, type:

```
>>> help("digidevice")
Help on package digidevice:

NAME
    digidevice - Digi device python extensions

DESCRIPTION
    This module includes various extensions that allow Python
    to interact with additional features offered by the device.
...
```

4. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Run a Python application at the shell prompt

Python applications can be run from a file at the shell prompt. The Python application will run until it completes, displaying output and prompting for additional user input if needed. To interrupt the application, enter **CTRL-C**.

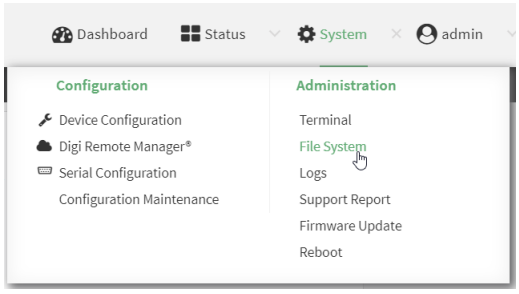
Note Python applications cannot be run from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See Authentication groups for information about configuring authentication groups that include shell access.

1. Upload the Python application to the IX10 device:

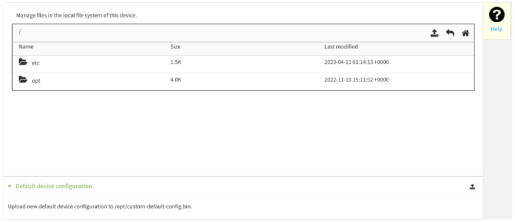
Web

Log into the IX10 WebUI as a user with full Admin access rights.

a. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



b. Highlight the **scripts** directory and click to open the directory.

c. Click ❸ (upload).

d. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

Command line

a. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

b. At the command line, use the scp command to upload the Python application script to the IX10 device:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
- *local-path* is the location on the IX10 device where the copied file will be placed.

For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the /etc/config/scripts directory on the IX10 device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local /etc/config/scripts/ to
local
admin@192.168.4.1's password: adminpwd
test.py                  100%   36MB   11.1MB/s      00:03
>
```

c. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Note You can also create scripts by using the **vi** command when logged in with shell access.

2. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

3. Use the **python** command to run the Python application. In the following example, the Python application, **test.py**, takes 3 parameters: **120**, **ports** and **storage**:

```
# python /etc/config/scripts/test.py 120 ports storage
```

Configure scripts to run manually

You can configure an scripts to be manually run.

Required configuration items

- Upload or create the script.
- Enable the script.
- Set the script to run manually.

Additional configuration items

- A label used to identify the script.
- The arguments for the script.

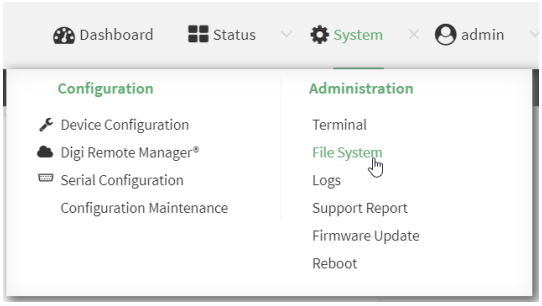
- Whether to write the script output and errors to the system log.
- The memory available to be used by the script.
- Whether the script should run one time only.

Task one: Upload the application

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.

2. Highlight the **scripts** directory and click to open the directory.
3. Click (upload).
4. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, use the scp command to upload the Python application script to the IX10 device:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
- *local-path* is the location on the IX10 device where the copied file will be placed.

For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the /etc/config/scripts directory on the IX10 device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local /etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                100%   36MB   11.1MB/s      00:03
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Note You can also create scripts by using the **vi** command when logged in with shell access.

Task two: Configure the application to run automatically

Note This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

Web

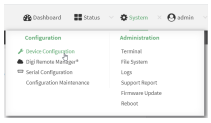
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

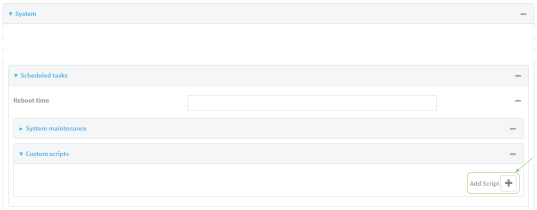
   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

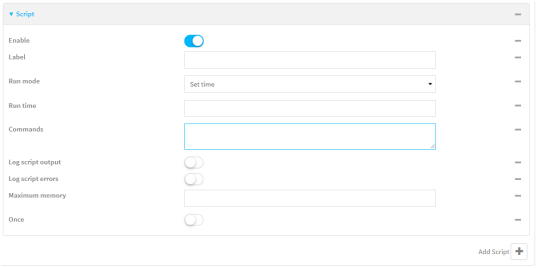


The **Configuration** window is displayed.

3. Click **System** > **Scheduled tasks** > **Custom scripts**.
4. For **Add Script**, click



The script configuration window is displayed.



Custom scripts are enabled by default. To disable, toggle off **Enable** to toggle off.

5. (Optional) For **Label**, provide a label for the script.
6. For **Run mode**, select **Manual**.
7. For **Commands**, type the commands that will execute the script.
   - If a Python script is being used, include the full path to the Python script. For example:

     ```
     python /etc/config/scripts/test.py
     ```

   - If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).
8. Script logging options:
   a. Click to enable **Log script output** to log the script's output to the system log.
   b. Click to enable **Log script errors** to log script errors to the system log.

   If neither option is selected, only the script's exit code is written to the system log.
9. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{**b**|**bytes**|**KB**|**k**|**MB**|**MB**|**M**|**GB**|**G**|**TB**|**T**}.
10. **Sandbox** is enabled by default, which restricts access to the file system and available commands that can be used by the script. This option protects the script from accidentally destroying the system it is running on.

11. Click to enable **Once** to configure the script to run only once at the specified time.

    If **Once** is enabled, rebooting the device will cause the script to not run again. The only way to re-run the script is to:

    - Remove the script from the device and add it again.
    - Make a change to the script.
    - Uncheck **Once**.

12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a script:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

   Scheduled scripts are enabled by default. To disable:

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

4. (Optional) Provide a label for the script.

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

   where *value* is any string. if spaces are used, enclose *value* within double quotes.

5. Set the run mode to manual:

```
(config system schedule script 0)> when manual
(config system schedule script 0)>
```

6. Set the commands that will execute the script:

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

   where *filename* is the path and filename of the script, and any related command line information.

   - If a Python script is being used, include the full path to the Python script and enclose in quotation marks. For example:

```
(config system schedule script 0)> commands python "/etc/config/scripts/test.py"
(config system schedule script 0)>
```

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

7. Script logging options:
   - To log the script's output to the system log:

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

   - To log script errors to the system log:

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

   If **syslog_stdout** and **syslog_stderr** are not enabled, only the script's exit code is written to the system log.
8. Set the maximum amount of memory available to be used by the script and its subprocesses:

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

   where *value* uses the syntax ***number***{**b**|**bytes**|**KB**|**k**|**MB**|**MB**|**M**|**GB**|**G**|**TB**|**T**}.
9. To run the script only once at the specified time:

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

   If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:
   - Remove the script from the device and add it again.
   - Make a change to the script.
   - Disable **once**.
10. **Sandbox** is enabled by default. This option protects the script from accidentally destroying the system it is running on.

```
(config system schedule script 0)> sandbox true
(config system schedule script 0)>
```

11. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Start a manual script

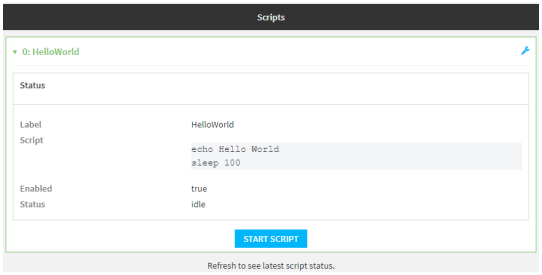
You can start a script that is enabled and configured to have a run mode of **Manual**.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



2. For scripts that are enabled and configured to have a run mode of **Manual**, click **Start Script** to start the script.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Determine the name of scripts that are currently running:

```
> show scripts

 Index  Label      Enabled  Status  Run time
 -----  ---------- -------  ------  --------
 0      script1    true     active
 1      script2    true     idle    01:00
>
```

3. Start the script:

```
)> system script start script1
>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Python versions and corresponding DAL OS firmware versions

The table lists the Python versions where changes were made the to programming language and the corresponding DAL OS version to which those changes align.

Python version history	DAL OS version history
Python 3.13	DAL OS 24.12.153.120
Python 3.10.13	DAL OS 24.3.28.88
Python 3.6.15	DAL OS 21.11.60.63

To see the Python change log, go to https://docs.python.org/3/whatsnew/changelog.html#.

User authentication

This chapter contains the following topics:

IX10 user authentication 687
User authentication methods 687
Authentication groups 694
Local users 704
Terminal Access Controller Access-Control System Plus (TACACS+) 717
Remote Authentication Dial-In User Service (RADIUS) 724
LDAP 729
Configure serial authentication 737
Disable shell access 739
Set the idle timeout for IX10 users 741
Example user configuration 743

IX10 user authentication

User authentication on the IX10 has the following features and default configuration:

Feature	Description	Default configuration
Idle timeout	Determines how long a user session can be idle before the system automatically disconnects.	■ 10 minutes
Allow shell	If disabled, prevents all authentication prohibits access to the shell prompt for all authentication groups. This does not prevent access to the Admin CLI. Note If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.	■ Enabled
Methods	Determines how users are authenticated for access: **local users**, **TACACS+**, or **RADIUS**.	■ **local users**
Groups	Associates access permissions for a group. . You can modify the released groups and create additional groups as needed for your site. A user can be assigned to more than one group.	■ **admin**: Provides the logged-in user with administrative and shell access. ■ **serial**: Provides the logged-in user with access to serial ports.
Users	Defines local users for the IX10.	■ **admin**: Belongs to both the **admin** and **serial** groups.
TACACS+	Configures support for TACACS+ (Terminal Access Controller Access-Control System Plus) servers and users.	■ Not configured
RADIUS	Configures support for RADIUS (Remote Authentication Dial-In User Service) servers and users.	■ Not configured
LDAP	Configures support for LDAP (Lightweight Directory Access Protocol) servers and users.	■ Not configured
Serial	Configures authentication for serial TCP and autoconnect services.	■ Not configured

User authentication methods

Authentication methods determine how users of the IX10 device are authenticated. Available authentication methods are:

- **Local users**: User are authenticated on the local device.
- **RADIUS**: Users authenticated by using a remote RADIUS server for authentication.

  See Remote Authentication Dial-In User Service (RADIUS) for information about configuring RADIUS authentication.
- **TACACS+**: Users authenticated by using a remote TACACS+ server for authentication.

  See Terminal Access Controller Access-Control System Plus (TACACS+) for information about configuring TACACS+ authentication.
- **LDAP**: Users authenticated by using a remote LDAP server for authentication.

  See LDAP for information about configuring LDAP authentication.

Add a new authentication method

Required configuration items

- The types of authentication method to be used:

To add an authentication method:

Web

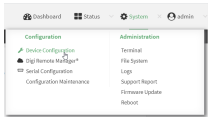
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

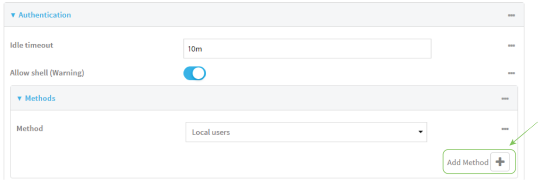
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

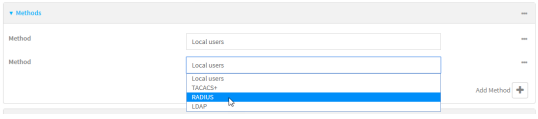
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Methods**.
4. For **Add Method**, click .

5. Select the appropriate authentication type for the new method from the **Method** drop-down.

Note Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. See Rearrange the position of authentication methods for information about how to reorder the authentication methods.

6. Repeat these steps to add additional methods.
7. Click **Apply** to save the configuration and apply the change.

Command line

Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This procedure describes how to add methods to various places in the list.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the new authentication method to the appropriate location in the list:
   - To determine the current list of authentication methods:
     a. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

        Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
     b. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

     c. Use the **show auth method** command to display the current authentication methods configuration:

```
(config)> show auth method
0 local
(config)>
```

   - To add the new authentication method to the beginning of the list, use the index value of **0** to indicate that it should be added as the first method:

```
(config)> add auth method 0 auth_type
(config)>
```

     where *auth_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.
   - To add the new authentication method to the end of the list, use the index keyword **end**:

```
(config)> add auth method end auth_type
(config)>
```

where *auth_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.

- To add the new authentication in another location in the list, use an index value to indicate the appropriate position. For example:

```
(config)> add auth method 1 auth_type
(config)>
```

where *auth_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.

- You can also use the **move** command to rearrange existing methods. See Rearrange the position of authentication methods for information about how to reorder the authentication methods.

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete an authentication method

Web

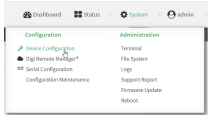
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

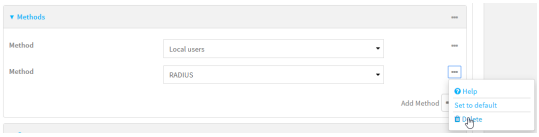
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication** > **Methods**.
4. Click the menu icon (**...**) next to the method and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **show auth method** command to determine the index number of the authentication method to be deleted:

```
(config)> show auth method
0 local
1 radius
2 tacacs+
(config)>
```

4. Delete the appropriate authentication method:

```
(config)> del auth method n
```

   Where *n* is index number of the authentication method to be deleted. For example, to delete the TACACS+ authentication method as displayed by the example **show** command, above:

```
(config)> del auth method 2
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

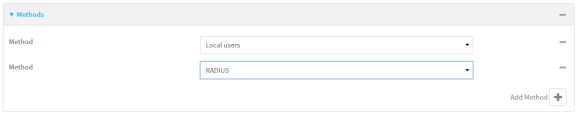
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Rearrange the position of authentication methods

Web

Authentication methods are reordered by changing the method type in the **Method** drop-down for each authentication method to match the appropriate order.

For example, the following configuration has **Local users** as the first method, and **RADIUS** as the second.



To reorder these so that **RADIUS** is first and **Local users** is second:

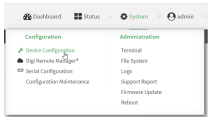
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

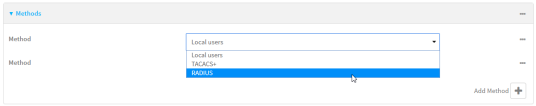
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

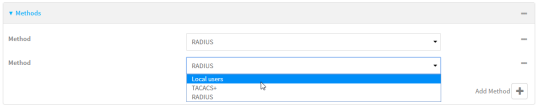
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click to expand the first **Method**.
4. In the **Method** drop-down, select **RADIUS**.

5. Click to expand the second **Method**.
6. In the **Method** drop-down, select **Local users**.

7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **show** command to display current configuration:

```
(config)> show auth method
0 local
1 radius
(config)>
```

4. Use the **move** command to rearrange the methods:

```
(config)> move auth method 1 0
(config)>
```

5. Use the **show** command again to verify the change:

```
(config)> show auth method
0 radius
1 local
(config)>
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Authentication groups

Authentication groups are used to assign access rights to IX10 users. Three types of access rights can be assigned:

- **Admin access**: Users with Admin access can be configured to have either:
  - The ability to manage the IX10 device by using the WebUI or the Admin CLI.
  - Read-only access to the WebUI and Admin CLI.
- **Shell access**: Users with Shell access have the ability to access the shell when logging into the IX10 via ssh, telnet, or the serial console.

  Shell access is not available if the **Allow shell** parameter has been disabled. See Disable shell access for more information about the **Allow shell** parameter.

Note When Primary Responder mode is enabled, Telnet is not available. For more information about Primary Responder mode, see Differences between standard firmware operation and Primary Responder mode.

- **Serial access**: Users with Serial access have the ability to log into the IX10 device by using the serial console.

Preconfigured authentication groups

The IX10 device has two preconfigured authentication groups:

- The **admin** group is configured by default to have full **Admin access**.
- The **serial** group is configured by default to have **Serial access**.

The preconfigured authentication groups cannot be deleted, but the access rights defined for the group are configurable.

This section contains the following topics:

Change the access rights for a predefined group 696
Add an authentication group 698
Delete an authentication group 702

Change the access rights for a predefined group

By default, two authentication groups are predefined: **admin** and **serial**. To change the access rights of the predefined groups:

Web

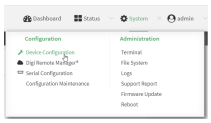
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

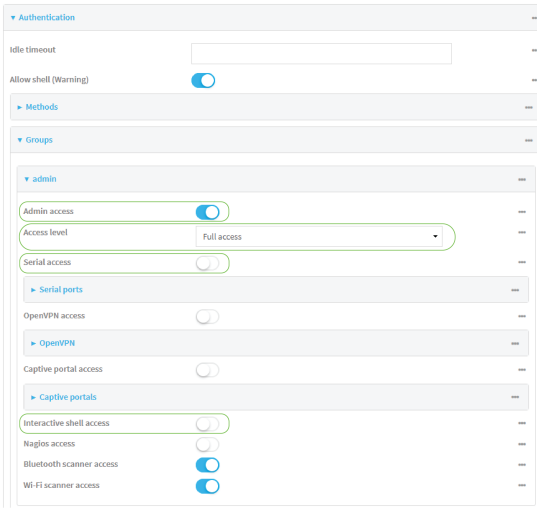
   

   The **Configuration** window is displayed.
3. Click **Authentication** > **Groups**.
4. Click the authentication group to be changed, either **admin** or **serial**, to expand its configuration node.
5. Click the box next to the following options, as appropriate, to enable or disable access rights for each:
   - **Admin access**

     For groups assigned Admin access, you can also determine whether the **Access level** should be **Full access** or **Read-only access**.
     - **Full access** provides users of this group with the ability to manage the IX10 device by using the WebUI or the Admin CLI.
     - **Read-only access** provides users of this group with read-only access to the WebUI and Admin CLI.

     The default is **Full access**.
   - **Serial access**
   - **Interactive shell access**

     Shell access is not available if the **Allow shell** parameter has been disabled. See Disable shell access for more information about the **Allow shell** parameter.



6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable or disable access rights for the group. For example:
   - Admin access:
     - To set the access level for Admin access of the **admin** group:

```
(config)> auth group admin acl admin level value
(config)>
```

       where *value* is either:
       - **full**: provides users of this group with the ability to manage the IX10 device by using the WebUI or the Admin CLI.
       - **read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

       The default is **full**.
     - To disable Admin access for the **admin** group:

```
(config)> auth group admin acl admin enable false
(config)>
```

   - Shell access:

- To enable Shell access for the **serial** group:

```
(config)> auth group serial acl shell enable true
(config)>
```

Shell access is not available if the **Allow shell** parameter has been disabled. See Disable shell access for more information about the **Allow shell** parameter.

- Serial access:
  - To enable Serial access for the **admin** group:

```
(config)> auth group admin acl serial enable true
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Add an authentication group

Required configuration items

- The access rights to be assigned to users that are assigned to this group.

Additional configuration items

- Access rights to OpenVPN tunnels, and the tunnels to which they have access.
- Access rights to captive portals, and the portals to which they have access.
- Access rights to query the device for Nagios monitoring.

To add an authentication group:

Web

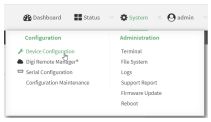
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

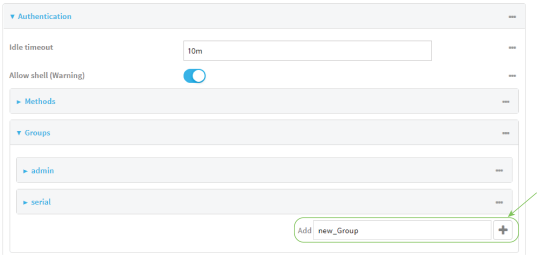
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

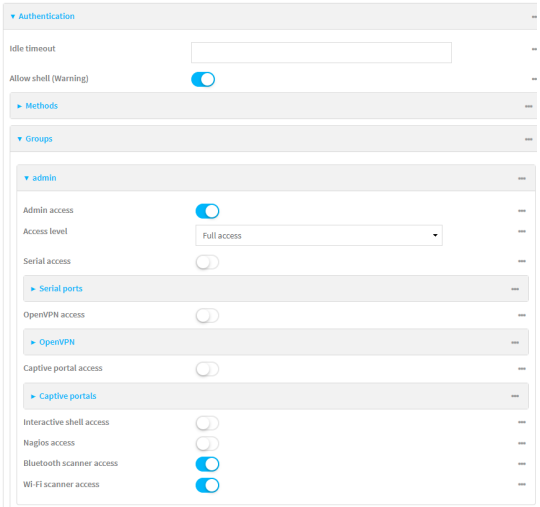


The **Configuration** window is displayed.

3. Click **Authentication** > **Groups**.
4. For **Add**, type a name for the group and click ✓.



The group configuration window is displayed.



5. Click the following options, as appropriate, to enable or disable access rights for each:
   - **Admin access**

     For groups assigned Admin access, you can also determine whether the **Access level** should be **Full access** or **Read-only access**.

     where *value* is either:

     - **Full access full**: provides users of this group with the ability to manage the IX10 device by using the WebUI or the Admin CLI.
     - **Read-only access read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

     The default is **Full access full**.

- **Serial access**

6. (Optional) Configure the serial ports to which users of this group have access:
   a. Click **Serial ports** to expand the **Serial ports** node.
   b. For **Add Port**, click .
   c. In the **Port** dropdown, select a port.
   d. Click again to add additional serial ports.
7. (Optional) Configure OpenVPN access. See for further information.
8. (Optional) Configure captive portal access:
   a. Enable captive portal access rights for users of this group by checking the box next to **Captive portal access**.
   b. Click **Captive portals** to expand the **Captive portal** node.
   c. For **Add Captive portal**, click .
   d. In the **Captive portal** dropdown, select a captive portal to which users of this group will have access.
   e. Click again to add additional captive portals.
9. **Interactive shell access**

   Shell access is not available if the **Allow shell** parameter has been disabled. See Disable shell access for more information about the **Allow shell** parameter.
10. (Optional) Enable users that belong to this group to query the device for Nagios monitoring by checking the box next to **Nagios access**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **add auth group** command to add a new authentication. For example, to add a group named **test**:

```
(config)> add auth group test
(config auth group test)>
```

4. Enable access rights for the group:
   - Admin access:

```
(config auth group test)> acl admin enable true
(config)>
```

- Set the access level for Admin access:

```
(config)> auth group admin acl admin level value
(config)>
```

where *value* is either:

- **full**: provides users of this group with the ability to manage the IX10 device by using the WebUI or the Admin CLI.
- **read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

The default is **full**.

- Shell access:

```
(config auth group test)> acl shell enable true
(config)>
```

Shell access is not available if the **Allow shell** parameter has been disabled. See Disable shell access for more information about the **Allow shell** parameter.

- Serial access:

```
(config auth group test)> acl serial enable true
(config)>
```

5. (Optional) Configure captive portal access:
   a. Return to the config prompt by typing three periods (**...**):

```
(config auth group test)> ...
(config)>
```

   b. Enable captive portal access rights for users of this group:

```
(config)> auth group test acl portal enable true
(config)>
```

   c. Add a captive portal to which users of this group will have access:
      i. Determine available portals:

```
(config)> show firewall portal
portal1
    auth none
    enable true
    http redirect
    no interface
    no message
    no redirect_url
    no terms
    timeout 24h
    no title
(config)>
```

ii. Add a captive portal:

```
(config)> add auth group test acl portal portals end portal1
(config)>
```

6. (Optional) Configure Nagios monitoring:

```
(config)> auth group test acl nagios enable true
(config)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete an authentication group

By default, the IX10 device has two preconfigured authentication groups: **admin** and **serial**. These groups cannot be deleted.

To delete an authentication group that you have created:

Web

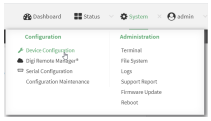
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

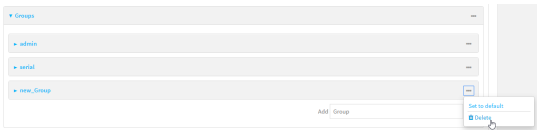
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Groups**.

4. Click the menu icon **(...)** next to the group to be deleted and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> del auth group groupname
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Local users

Local users are authenticated on the device without using an external authentication mechanism such as TACACS+ or RADIUS. Local user authentication is enabled by default, with one preconfiged default user.

Default user

At manufacturing time, each IX10 device comes with a default user configured as follows:

- Username: **admin**.
- Password: The default password is displayed on the label on the bottom of the device.

> **Note** The default password is a unique password for the device, and is the most critical security feature for the device. If you reset the device to factory defaults, you must log in using the default user and password, and you should immediately change the password to a custom password. Before deploying or mounting the IX10 device, record the default password, so you have the information available when you need it even if you cannot physically access the label on the bottom of the device.

The default **admin** user is preconfigured with both Admin and Serial access. You can configure the **admin** user account to fit with the needs of your environment.

This section contains the following topics:

Change a local user's password 705
Configure a local user 707
Delete a local user 714

Change a local user's password

Note When updating the password for the local user, you will be prompted to enter the current password before applying the configuration update.

To change a user's password:

Web

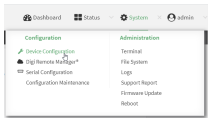
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

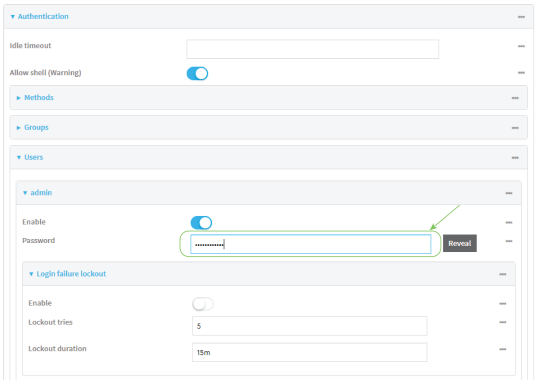
   

   The **Configuration** window is displayed.
3. Click **Authentication** > **Users**.
4. Click the username to expand the user's configuration node.
5. For **Password**, enter the new password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

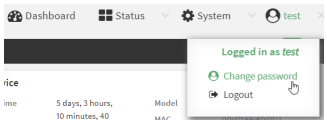
   Note If the Primary Responder feature is enabled, the password must be at least 10 characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

   For the **admin** user, the password field can be left blank:

   - If the password field for the **admin** user is left blank, the **admin** user's password will be the default password printed on the device's label.
   - If the **admin** user's password has been changed from the default and the configuration saved, if you then clear the password field for the **admin** user, this will result in the device device's configuration being erased and reset to the default configuration.



You can also change the password for the active user by clicking the user name in the menu bar:



The active user must have full Admin access rights to be able to change the password.

6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> auth user username password pwd
```

Where:

- *username* is the name of the user.
- *pwd* is the new password for the user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure a local user

Required configuration items

- A username.
- A password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character. For security reasons, passwords are stored in hash form. There is no way to get or display passwords in clear-text form, although prior to saving the configuration, the password can be shown by clicking **Reveal**.

  Note If the Primary Responder feature is enabled, the password must be at least 10 characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

- The authentication group or groups from which the user will inherit access rights. See Authentication groups for information about configuring groups.

Additional configuration items

- An alias for the user. Because the username cannot contain any special characters, such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters.
- The number of unsuccessful login attempts before the user is locked out of the system.
- The amount of time that the user is locked out of the system after the specified number of unsuccessful login attempts.
- An optional public ssh key, to authenticate the user when using passwordless SSH login.
- Two-factor authentication information for user login over SSH, telnet, and the serial console:
  - The verification type for two-factor authentication: Either time-based or counter-based.
  - The security key.
  - Whether to allow passcode reuse (time based verification only).
  - The passcode refresh interval (time based verification only).
  - The valid code window size.
  - The login limit.
  - The login limit period.
  - One-time use eight-digit emergency scratch codes.

To configure a local user:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

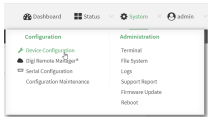
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

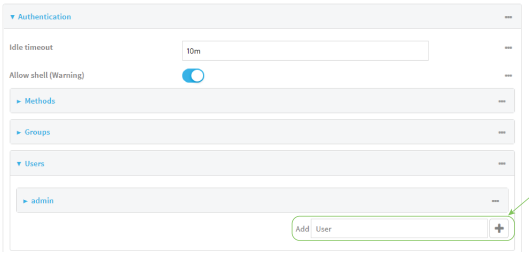
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

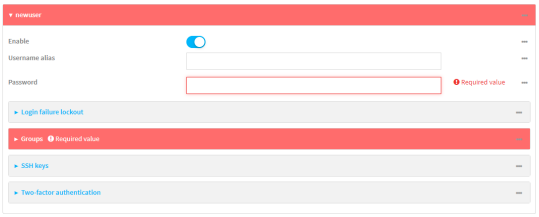
   

   The **Configuration** window is displayed.

3. Click **Authentication** > **Users**.
4. In **Add User**, type a name for the user and click .

   The user configuration window is displayed.

   The user is enabled by default. To disable, toggle off **Enable**.

5. (Optional) For **Username alias**, type an alias for the user.

   Because the name used to create the user and cannot contain special characters such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters. For security purposes, if two users have the same alias, the alias will be disabled.

6. Enter a password for the user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

7. Click to expand **Login failure lockout**.

   The login failure lockout feature is enabled by default. To disable, toggle off **Enable**.

   a. For **Lockout tries**, type the number of unsuccessful login attempts before the user is locked out of the device. The default is **5**.

   b. For **Lockout duration**, type the amount of time that the user is locked out after the number of unsuccessful login attempts defined in **Lockout tries**.

      Allowed values are any number of minutes, or seconds, and take the format ***number*{m|s}**.

      For example, to set **Lockout duration** to ten minutes, enter **10m** or **600s**.

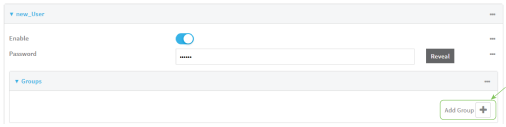
      The minimum value is 1 second, and the maximum is 15 minutes. The default is 15 minutes.

8. Add groups for the user.

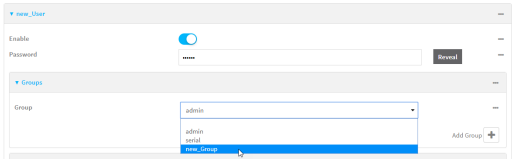
   Groups define user access rights. See Authentication groups for information about configuring groups.

   a. Click to expand **Groups**.

   b. For **Add Group**, click .



   c. For **Group**, select an appropriate group.



Note Every user must be configured with at least one group. You can add multiple groups to a user by clicking **Add** again and selecting the next group.

9. (Optional) Add SSH keys for the user to use passwordless SSH login:

   a. Click **SSH keys**.

   b. In **Add SSH key**, paste or type a public encryption key that this user can use for passwordless SSH login and click .

10. (Optional) Configure two-factor authentication for SSH, telnet, and serial console login:

    a. Click **Two-factor authentication**.

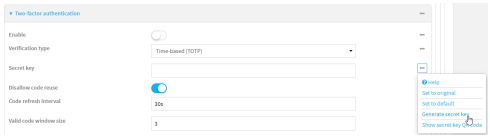
    b. Check **Enable** to enable two-factor authentication for this user.

    c. Select the **Verification type**:

       - **Time-based (TOTP)**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
       - **Counter-based (HOTP)**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.

d. Generate a **Secret key**:

   i. Click **...** next to the field label and select **Generate secret key**.



   ii. Copy the secret key for use with an application or mobile device to generate passcodes.

e. For time-based verification only, select **Disallow code reuse** to prevent a code from being used more than once during the time that it is valid.

f. For time-based verification only, in **Code refresh interval**, type the amount of time that a code will remain valid.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}. For example, to set **Code refresh interval** to ten minutes, enter **10m** or **600s**.

g. In **Valid code window size**, type the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the **Valid code window size** may be necessary when the clocks used by the server and client are not synchronized.

h. For **Login limit**, type the number of times that the user is allowed to attempt to log in during the **Login limit period**. Set **Login limit** to **0** to allow an unlimited number of login attempts during the **Login limit period**.

i. For **Login limit period**, type the amount of time that the user is allowed to attempt to log in.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}. For example, to set **Login limit period** to ten minutes, enter **10m** or **600s**.

j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:

   i. Click **Scratch codes**.

   ii. For **Add Code**, click .

   iii. For **Code**, enter the scratch code. The code must be eight digits, with a minimum of 10000000.

   iv. Click again to add additional scratch codes.

11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a user. For example, to create a user named **new_user**:

```
(config)> add auth user new_user
(config auth user new_user)>
```

The user is enabled by default. To disable the user, type:

```
(config auth user new_user)> enable false
(config auth user new_user)>
```

4. (Optional) Create a username alias for the user.

Because the name to create the user cannot contain special characters such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters. For security purposes, if two users have the same alias, the alias will be disabled.

```
(config auth user new_user> username username_alias
(config auth user new_user)>
```

5. Set the user's password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

```
(config auth user new_user> password pwd
(config auth user new_user)>
```

6. Configure login failure lockout settings:

The login failure lockout feature is enabled by default. To disable:

```
(config auth user new_user> lockout enable false
(config auth user new_user)>
```

a. Set the number of unsuccessful login attempts before the user is locked out of the device.

where *value* is any integer. The minimum value is **1**, and the default value is **5**.

b. Set the amount of time that the user is locked out after the number of unsuccessful login attempts defined in **lockout tries**:

```
(config auth user new_user> lockout duration value
(config auth user new_user)>
```

where *value* is any number of minutes, or seconds, and takes the format ***number***{**m|s**}.

For example, to set **duration** to ten minutes, enter either **10m** or **600s**:

```
(config auth user new_user)> lockout duration 600s
(config auth user new_user)>
```

The minimum value is 1 second, and the maximum is 15 minutes. The default is 15 minutes.

7. Add groups for the user.

   Groups define user access rights. See Authentication groups for information about configuring groups.

   a. Add a group to the user. For example, to add the admin group to the user:

   ```
   (config auth user new_user> add group end admin
   (config auth user new_user)>
   ```

   Note Every user must be configured with at least one group.

   b. (Optional) Add additional groups by repeating the add group command:

   ```
   (config auth user new_user> add group end serial
   (config auth user new_user)>
   ```

   To remove a group from a user:

   a. Use the **show** command to determine the index number of the group to be deleted:

   ```
   (config auth user new_user> show group
   0 admin
   1 serial
   (config auth user new_user>
   ```

   b. Type the following:

   ```
   (config auth user new_user)> del group n
   (config auth user new_user)>
   ```

   Where *n* is index number of the authentication method to be deleted. For example, to delete the serial group as displayed by the example **show** command, above:

   ```
   (config auth user new_user)> del group 1
   (config auth user new_user)>
   ```

8. (Optional) Add SSH keys for the user to use passwordless SSH login:

   a. Change to the user's ssh_key node:

   ```
   (config auth user new_user)> ssh_key
   (config auth user new_user ssh_key)>
   ```

   b. Add the key by using the ssh_key command and pasting or typing a public encryption key that this user can use for passwordless SSH login:

   ```
   (config auth user new_user ssh_key)> ssh_key key
   (config auth user new_user ssh_key)>
   ```

9. (Optional) Configure two-factor authentication for SSH, telnet, and serial console login:

a. Change to the user's two-factor authentication node:

```
(config auth user new_user)> 2fa
(config auth user new_user 2fa)>
```

b. Enable two-factor authentication for this user:

```
(config auth user new_user 2fa)> enable true
(config auth user new_user 2fa)>
```

c. Configure the verification type. Allowed values are:
   - **totp**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
   - **hotp**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.

   The default value is **totp**.

```
(config auth user new_user 2fa)> type totp
(config auth user new_user 2fa)>
```

d. Add a secret key:

```
(config auth user new_user 2fa)> secret key
(config auth user new_user 2fa)>
```

   This key should be used by an application or mobile device to generate passcodes.

e. For time-based verification only, enable **disallow_reuse** to prevent a code from being used more than once during the time that it is valid.

```
(config auth user new_user 2fa)> disallow_reuse true
(config auth user new_user 2fa)>
```

f. For time-based verification only, configure the code refresh interval. This is the amount of time that a code will remain valid.

```
(config auth user new_user 2fa)> refresh_interval value
(config auth user new_user 2fa)>
```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **refresh_interval** to ten minutes, enter either **10m** or **600s**:

```
(config auth user name 2fa)> refresh_interval 600s
(config auth user name 2fa)>
```

   The default is **30s**.

g. Configure the valid code window size. This represents the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the valid code window size may be necessary when the clocks used by the server and client are not synchronized.

```
(config auth user new_user 2fa)> window_size 3
(config auth user new_user 2fa)>
```

h. Configure the login limit. This represents the number of times that the user is allowed to attempt to log in during the Login limit period. Set to 0 to allow an unlimited number of login attempts during the Login limit period

```
(config auth user new_user 2fa)> login_limit 3
(config auth user new_user 2fa)>
```

i. Configure the login limit period. This is the amount of time that the user is allowed to attempt to log in.

```
(config auth user new_user 2fa)> login_limit_period value
(config auth user new_user 2fa)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **login_limit_period** to ten minutes, enter either **10m** or **600s**:

```
(config auth user name 2fa)> login_limit_period 600s
(config auth user name 2fa)>
```

The default is **30s**.

j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:

i. Change to the user's scratch code node:

```
(config auth user new_user 2fa)> scratch_code
(config auth user new_user 2fa scratch_code)>
```

ii. Add a scratch code:

```
(config auth user new_user 2fa scratch_code)> add end code
(config auth user new_user 2fa scratch_code)>
```

Where code is an digit number, with a minimum of 10000000.

iii. To add additional scratch codes, use the **add end *code*** command again.

10. Save the configuration and apply the change.

```
(config auth user new 2fa scratch_code)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a local user

To delete a user from your IX10:

Web

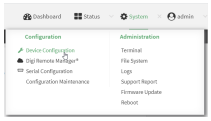
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

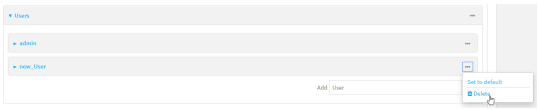
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Users**.
4. Click the menu icon (**...**) next to the name of the user to be deleted and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> del auth user username
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Terminal Access Controller Access-Control System Plus (TACACS+)

Your IX10 device supports Terminal Access Controller Access-Control System Plus (TACACS+), a networking protocol that provides centralized authentication and authorization management for users who connect to the device. With TACACS+ support, the IX10 device acts as a TACACS+ client, which sends user credentials and connection parameters to a TACACS+ server over TCP. The TACACS+ server then authenticates the TACACS+ client requests and sends back a response message to the device.

When you are using TACACS+ authentication, you can have both local users and TACACS+ users able to log in to the device. To use TACACS+ authentication, you must set up a TACACS+ server that is accessible by the IX10 device prior to configuration. The process of setting up a TACACS+ server varies by the server environment.

This section contains the following topics:

TACACS+ user configuration 718
TACACS+ server failover and fallback to local authentication 719
Configure your IX10 device to use a TACACS+ server 719

TACACS+ user configuration

When configured to use TACACS+ support, the IX10 device uses a remote TACACS+ server for user authentication (password verification) and authorization (assigning the access level of the user). Additional TACACS+ servers can be configured as backup servers for user authentication.

This section outlines how to configure a TACACS+ server to be used for user authentication on your IX10 device.

Example TACACS+ configuration

With TACACS+, users are defined in the server configuration file. On Ubuntu, the default location and filename for the server configuration file is **/etc/tacacs+/tac_plus.conf**.

Note TACACS+ configuration, including filenames and locations, may vary depending on your platform and installation. This example assumes a Ubuntu installation.

To define users:

1. Open the TACACS+ server configuration file in a text editor. For example:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

2. Add users to the file using the following format. This example will create two users, one with admin and serial access, and one with only serial access.

```
user = user1 {
      name ="User1 for IX10"
      pap = cleartext password1
      service = system {
        groupname = admin,serial
      }
}
user = user2 {
      name ="User2 for IX10"
      pap = cleartext password2
      service = system {
        groupname = serial
      }
}
```

   The **groupname** attribute is optional. If used, the value must correspond to authentication groups configured on your IX10. Alternatively, if the user is also configured as a local user on the IX10 device and the LDAP server authenticates the user but does not return any groups, the local configuration determines the list of groups. See Authentication groups for more information about authentication groups. The **groupname** attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

```
$ sudo tac_plus -C /etc/tacacs+/tac_plus.conf -P
```

   If successful, this command will echo the configuration file to standard out. If the command encounters any syntax errors, a message similar to this will display:

```
Error: Unrecognised token on line 1
```

5. Restart the TACACS+ server:

```
$ sudo /etc/init.d/tacacs_plus restart
```

TACACS+ server failover and fallback to local authentication

In addition to the primary TACACS+ server, you can also configure your IX10 device to use backup TACACS+ servers. Backup TACACS+ servers are used for authentication requests when the primary TACACS+ server is unavailable.

Falling back to local authentication

With user authentication methods, you can configure your IX10 device to use multiple types of authentication. For example, you can configure both TACACS+ authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup TACACS+ servers are unavailable. Additionally, users who are configured locally but are not configured on the TACACS+ server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the TACACS+ server, and only authenticated locally if the TACACS+ server is unavailable or if the user is not defined on the TACACS+ server, then you should list the TACACS+ authentication method prior to the Local users authentication method.

See User authentication methods for more information about authentication methods.

If the TACACS+ servers are unavailable and the IX10 device falls back to local authentication, only users defined locally on the device are able to log in. TACACS+ users cannot log in until the TACACS+ servers are brought back online.

Configure your IX10 device to use a TACACS+ server

This section describes how to configure a IX10 device to use a TACACS+ server for authentication and authorization.

Required configuration items

- Define the TACACS+ server IP address or domain name.
- Define the TACACS+ server shared secret.
- The group attribute configured in the TACACS+ server configuration.
- The service field configured in the TACACS+ server configuration.
- Add TACACS+ as an authentication method for your IX10 device.

Additional configuration items

- Whether other user authentication methods should be used in addition to the TACACS+ server, or if the TACACS+ server should be considered the authoritative login method.
- Enable command authorization, so that the device will communicate with the TACACS+ server to determine if the user is authorized to execute a specific command.
- Enable command accounting, so that the device will communicate with the TACACS+ server to log commands that the user executes.

- The TACACS+ server port. It is configured to 49 by default.
- Add additional TACACS+ servers in case the first TACACS+ server is unavailable.

Web

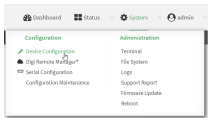
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

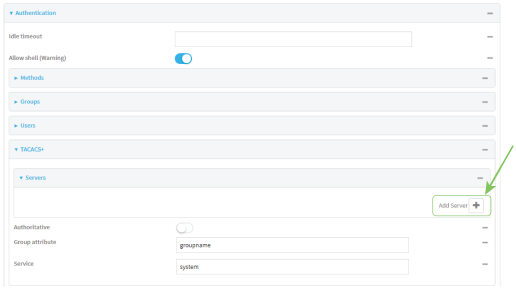
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **TACACS+** > **Servers**.
4. Add TACACS+ servers:

   a. For **Add server**, click .

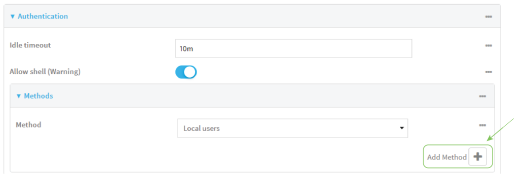
   b. For **Hostname**, type the hostname or IP address of the TACACS+ server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 49.
   d. For **Secret**, type the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's tac_plus.conf file, for example:

```
key = testing123
```

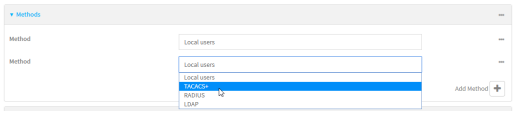
> **Note** DAL authentication does not support the use of the # character in the key (e.g., DAL#123;&). If included, the server will be unable to decipher the request.

e. (Optional) Click again to add additional TACACS+ servers.

5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if TACACS+ login fails.
6. (Optional) For **Group attribute**, type the name of the attribute used in the TACACS+ server's configuration to identify the IX10 authentication group or groups that the user is a member of. For example, in TACACS+ user configuration, the group attribute in the sample tac_plus.conf file is **groupname**, which is also the default setting in the IX10 configuration.
7. (Optional) For **Service**, type the value of the **service** attribute in the the TACACS+ server's configuration. For example, in TACACS+ user configuration, the value of the **service** attribute in the sample tac_plus.conf file is **system**, which is also the default setting in the IX10 configuration.
8. (Optional) Enable **Command authorization**, which instructs the device to communicate with the TACACS+ server to determine if the user is authorized to execute a specific command. Only the first configured TACACS+ server will be used for command authorization.
9. (Optional) Enable **Command accounting**, which instructs the device to communicate with the TACACS+ server to log commands that the user executes. Only the first configured TACACS+ server will be used for command accounting.
10. Add TACACS+ to the authentication methods:
    a. Click **Authentication** > **Methods**.
    b. For **Add method**, click



    c. Select **TACACS+** for the new method from the **Method** drop-down.



Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.

11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Prevent other authentication methods from being used if TACACS+ authentication fails. Other authentication methods will only be used if the TACACS+ server is unavailable.

```
(config)> auth tacacs+ authoritative true
(config)>
```

4. (Optional) Configure the group_attribute. This is the name of the attribute used in the TACACS+ server's configuration to identify the IX10 authentication group or groups that the user is a member of. For example, in TACACS+ user configuration, the group attribute in the sample tac_plus.conf file is **groupname**, which is also the default setting for the group_ attribute in the IX10 configuration.

```
(config)> auth tacacs+ group_attribute attribute-name
(config)>
```

5. (Optional) Configure the type of service. This is the value of the **service** attribute in the the TACACS+ server's configuration. For example, in TACACS+ user configuration, the value of the **service** attribute in the sample tac_plus.conf file is **system**, which is also the default setting in the IX10 configuration.

```
(config)> auth tacacs+ service service-name
(config)>
```

6. (Optional) Enable command authorization, which instructs the device to communicate with the TACACS+ server to determine if the user is authorized to execute a specific command. Only the first configured TACACS+ server will be used for command authorization.

```
(config)> auth tacacs+ command_authorization true
(config)>
```

7. (Optional) Enable command accounting, which instructs the device to communicate with the TACACS+ server to log commands that the user executes. Only the first configured TACACS+ server will be used for command accounting.

```
(config)> auth tacacs+ command_accounting true
(config)>
```

8. Add a TACACS+ server:
   a. Add the server:

```
(config)> add auth tacacs+ server end
(config auth tacacs+ server 0)>
```

   b. Enter the TACACS+ server's IP address or hostname:

```
(config auth tacacs+ server 0)> hostname hostname|ip-address
(config auth tacacs+ server 0)>
```

c. (Optional) Change the default port setting to the appropriate port:

```
(config auth tacacs+ server 0)> port port
(config auth tacacs+ server 0)>
```

d. (Optional) Repeat the above steps to add additional TACACS+ servers.

9. Add TACACS+ to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add TACACS+ to the end of the list. See User authentication methods for information about adding methods to the beginning or middle of the list.

```
(config)> add auth method end tacacs+
(config)>
```

10. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Remote Authentication Dial-In User Service (RADIUS)

Your IX10 device supports Remote Authentication Dial-In User Service (RADIUS), a networking protocol that provides centralized authentication and authorization management for users who connect to the device. With RADIUS support, the IX10 device acts as a RADIUS client, which sends user credentials and connection parameters to a RADIUS server over UDP. The RADIUS server then authenticates the RADIUS client requests and sends back a response message to the device.

When you are using RADIUS authentication, you can have both local users and RADIUS users able to log in to the device. To use RADIUS authentication, you must set up a RADIUS server that is accessible by the IX10 device prior to configuration. The process of setting up a RADIUS server varies by the server environment. An example of a RADIUS server is FreeRADIUS.

This section contains the following topics:

RADIUS user configuration 725
RADIUS server failover and fallback to local configuration 725
Configure your IX10 device to use a RADIUS server 726

RADIUS user configuration

When configured to use RADIUS support, the IX10 device uses a remote RADIUS server for user authentication (password verification) and authorization (assigning the access level of the user). Additional RADIUS servers can be configured as backup servers for user authentication.

This section outlines how to configure a RADIUS server to be used for user authentication on your IX10 device.

Example FreeRADIUS configuration

With FreeRADIUS, users are defined in the **users** file in your FreeRADIUS installation. To define users:

1. Open the FreeRadius user file in a text editor. For example:

```
$ sudo gedit /etc/freeradius/3.0/users
```

2. Add users to the file using the following format:

```
user1 Cleartext-Password := "user1"
      Unix-FTP-Group-Names := "admin"

user2 Cleartext-Password := "user2"
      Unix-FTP-Group-Names := "serial"
```

   The **Unix-FTP-Group-Names** attribute is optional. If used, the value must correspond to authentication groups configured on your IX10. Alternatively, if the user is also configured as a local user on the IX10 device and the RADIUS server authenticates the user but does not return any groups, the local configuration determines the list of groups. See Authentication groups for more information about authentication groups. The **Unix-FTP-Group-Names** attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

```
$ sudo freeradius -CX
```

   This should return a message that completes similar to:

```
...
Configuration appears to be OK
```

5. Restart the FreeRADIUS server:

```
$ sudo /etc/init.d/freeradius restart
```

RADIUS server failover and fallback to local configuration

In addition to the primary RADIUS server, you can also configure your IX10 device to use backup RADIUS servers. Backup RADIUS servers are used for authentication requests when the primary RADIUS server is unavailable.

Falling back to local authentication

With user authentication methods, you can configure your IX10 device to use multiple types of authentication. For example, you can configure both RADIUS authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and

backup RADIUS servers are unavailable. Additionally, users who are configured locally but are not configured on the RADIUS server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the RADIUS server, and only authenticated locally if the RADIUS server is unavailable or if the user is not defined on the RADIUS server, then you should list the RADIUS authentication method prior to the Local users authentication method.

See User authentication methods for more information about authentication methods.

If the RADIUS servers are unavailable and the IX10 device falls back to local authentication, only users defined locally on the device are able to log in. RADIUS users cannot log in until the RADIUS servers are brought back online.

Configure your IX10 device to use a RADIUS server

This section describes how to configure a IX10 device to use a RADIUS server for authentication and authorization.

Required configuration items

- Define the RADIUS server IP address or domain name.
- Define the RADIUS server shared secret.
- Add RADIUS as an authentication method for your IX10 device.

Additional configuration items

- Whether other user authentication methods should be used in addition to the RADIUS server, or if the RADIUS server should be considered the authoritative login method.
- The RADIUS server port. It is configured to 1812 by default.
- Add additional RADIUS servers in case the first RADIUS server is unavailable.
- The server NAS ID. If left blank, the default value is used:
  - If you are access the IX10 device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are access the IX10 device by using ssh, the default value is **sshd**.
- Time in seconds before the request to the server times out. The default is 3 seconds and the maximum possible value is 60 seconds.
- Enable additional debug messages from the RADIUS client.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

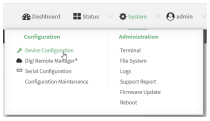
   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.

d. Click to expand **Config**.

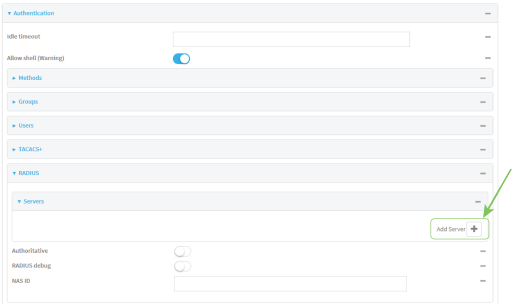
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication** > **RADIUS** > **Servers**.
4. Add RADIUS servers:
   a. For **Add server**, click .

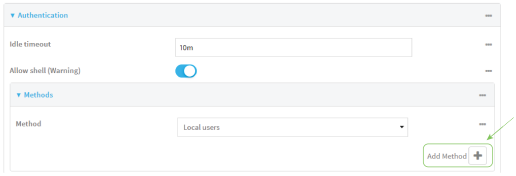


   b. For **Hostname**, type the hostname or IP address of the RADIUS server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 1812.
   d. For **Secret**, type the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file, for example:

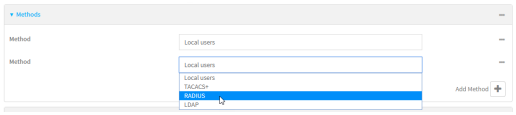
```
secret=testing123
```

   e. For **Timeout**, type or select the amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.
   f. (Optional) Click again to add additional RADIUS servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if RADIUS login fails.
6. (Optional) Click **RADIUS debug** to enable additional debug messages from the RADIUS client.
7. (Optional) For **NAS ID**, type the unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:
   - If you are accessing the IX10 device by using the WebUI, the default value is for NAS ID is **httpd**.
   - If you are accessing the IX10 device by using ssh, the default value is **sshd**.

8. Add RADIUS to the authentication methods:
   a. Click **Authentication** > **Methods**.
   b. For **Add method**, click ♑



   c. Select **RADIUS** for the new method from the **Method** drop-down.



   Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.
9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Prevent other authentication methods from being used if RADIUS authentication fails. Other authentication methods will only be used if the RADIUS server is unavailable.

```
(config)> auth radius authoritative true
(config)>
```

4. (Optional) Enable debug messages from the RADIUS client:

```
(config)> auth radius debug true
(config)>
```

5. (Optional) Configure the NAS ID. This is a unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:
   - If you are accessing the IX10 device by using the WebUI, the default value is for NAS ID is **httpd**.
   - If you are accessing the IX10 device by using ssh, the default value is **sshd**.

```
(config)> auth radius nas_id id
(config)>
```

6. Add a RADIUS server:
   a. Add the server:

   ```
   (config)> add auth radius server end
   (config auth radius server 0)>
   ```

   b. Enter the RADIUS server's IP address or hostname:

   ```
   (config auth radius server 0)> hostname hostname|ip-address
   (config auth radius server 0)>
   ```

   c. (Optional) Change the default port setting to the appropriate port:

   ```
   (config auth radius server 0)> port port
   (config auth radius server 0)>
   ```

   d. Configure the amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.

   ```
   (config auth radius server 0)> timeout value
   (config auth radius server 0)>
   ```

   e. (Optional) Repeat the above steps to add additional RADIUS servers.
7. Add RADIUS to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add RADIUS to the end of the list. See User authentication methods for information about adding methods to the beginning or middle of the list.

   ```
   (config)> add auth method end radius
   (config)>
   ```

8. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

LDAP

Your IX10 device supports LDAP (Lightweight Directory Access Protocol), a protocol used for directory information services over an IP network. LDAP can be used with your IX10 device for centralized authentication and authorization management for users who connect to the device. With LDAP support, the IX10 device acts as an LDAP client, which sends user credentials and connection parameters to an LDAP server. The LDAP server then authenticates the LDAP client requests and sends back a response message to the device.

When you are using LDAP authentication, you can have both local users and LDAP users able to log in to the device. To use LDAP authentication, you must set up a LDAP server that is accessible by the IX10 device prior to configuration. The process of setting up a LDAP server varies by the server environment.

This section contains the following topics:

LDAP user configuration 731
LDAP server failover and fallback to local configuration 732
Configure your IX10 device to use an LDAP server 732

LDAP user configuration

When configured to use LDAP support, the IX10 device uses a remote LDAP server for user authentication (password verification) and authorization (assigning the access level of the user). Additional LDAP servers can be configured as backup servers for user authentication.

This section outlines how to configure a LDAP server to be used for user authentication on your IX10 device.

There are several different implementations of LDAP, including Microsoft Active Directory. This section uses OpenLDAP as an example configuration. Other implementations of LDAP will have different configuration methods.

Example OpenLDAP configuration

With OpenLDAP, users can be configured in a text file using the LDAP Data Interchange Format (LDIF). In this case, we will be using a file called **add_user.ldif**.

1. Create the **add_user.ldif** file in a text editor. For example:

```
$ gedit ./add_user.ldif
```

2. Add users to the file using the following format:

```
dn: uid=john,dc=example,dc=com
objectClass: inetOrgPerson
cn: John Smith
sn: Smith
uid: john
userPassword: password
ou: admin serial
```

   - The value of **uid** and **userPassword** must correspond to the username and password used to log into the IX10 device.
   - The **ou** attribute is optional. If used, the value must correspond to authentication groups configured on your IX10. Alternatively, if the user is also configured as a local user on the IX10 device and the LDAP server authenticates the user but does not return any groups, the local configuration determines the list of groups. See Authentication groups for more information about authentication groups.

   Other attributes may be required by the user's objectClass. Any objectClass may be used as long it allows the **uid**, **userPassword**, and **ou** attributes.
3. Save and close the file.
4. Add the user to the OpenLDAP server:

```
$ ldapadd -x -H 'ldap:///' -D 'cn=admin,dc=example,dc=com' -W -f add_user.ldif
adding new entry "uid=john,dc=example,dc=com"
```

5. Verify that the user has been added by performing an LDAP search:

```
$ ldapsearch -x -LLL -H 'ldap:///' -b 'dc=example,dc=com'
uid=john
dn: uid=john,dc=example,dc=com
objectClass: inetOrgPerson
cn: John Smith
```

```
sn: Smith
uid: john
ou: admin serial
```

LDAP server failover and fallback to local configuration

In addition to the primary LDAP server, you can also configure your IX10 device to use backup LDAP servers. Backup LDAP servers are used for authentication requests when the primary LDAP server is unavailable.

Falling back to local authentication

With user authentication methods, you can configure your IX10 device to use multiple types of authentication. For example, you can configure both LDAP authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup LDAP servers are unavailable. Additionally, users who are configured locally but are not configured on the LDAP server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the LDAP server, and only authenticated locally if the LDAP server is unavailable or if the user is not defined on the LDAP server, then you should list the LDAP authentication method prior to the Local users authentication method.

See User authentication methods for more information about authentication methods.

If the LDAP servers are unavailable and the IX10 device falls back to local authentication, only users defined locally on the device are able to log in. LDAP users cannot log in until the LDAP servers are brought back online.

Configure your IX10 device to use an LDAP server

This section describes how to configure a IX10 device to use an LDAP server for authentication and authorization.

Required configuration items

- Define the LDAP server IP address or domain name.
- Add LDAP as an authentication method for your IX10 device.

Additional configuration items

- Whether other user authentication methods should be used in addition to the LDAP server, or if the LDAP server should be considered the authoritative login method.
- The LDAP server port. It is configured to 389 by default.
- Whether to use Transport Layer Security (TLS) when communicating with the LDAP server.
- The distinguished name (DN) and password used to communicate with the server.
- The distinguished name used to search to user base.
- The group attribute.
- The number of seconds to wait to receive a message from the server.
- Add additional LDAP servers in case the first LDAP server is unavailable.

Web

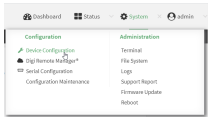
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

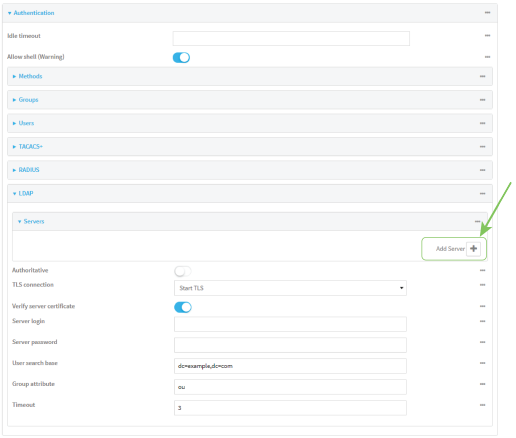
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

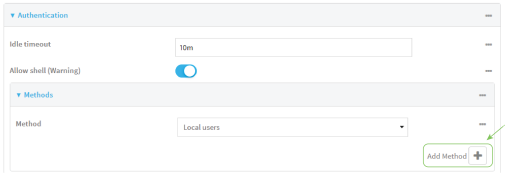
   The **Configuration** window is displayed.
3. Click **Authentication** > **LDAP** > **Servers**.
4. Add LDAP servers:
   a. For **Add server**, click .

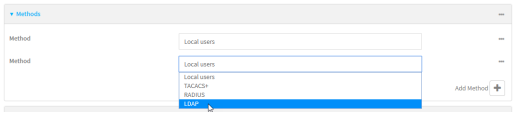
   b. For **Hostname**, type the hostname or IP address of the LDAP server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 389 for non-TLS and 636 for TLS.
   d. (Optional) Click again to add additional LDAP servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if LDAP login fails.
6. For **TLS connection**, select the type of TLS connection used by the server:
   - **Disable TLS**: Uses a non-secure TCP connection on the LDAP standard port, 389.
   - **Enable TLS**: Uses an SSL/TLS encrypted connection on port 636.

- **Start TLS**: Makes a non-secure TCP connection to the LDAP server on port 389, then sends a request to upgrade the connection to a secure TLS connection. This is the preferred method for LDAP.

7. If **Enable TLS** or **Start TLS** are selected for **TLS connection**:
   - Leave **Verify server certificate** at the default setting of enabled to verify the server certificate with a known Certificate Authority.
   - Disable **Verify server certificate** if the server is using a self-signed certificate.
8. (Optional) For **Server login**, type a distinguished name (DN) that is used to bind to the LDAP server and search for users, for example **cn=user,dc=example,dc=com**. Leave this field blank if the server allows anonymous connections.
9. (Optional) For **Server password**, type the password used to log into the LDAP server. Leave this field blank if the server allows anonymous connections.
10. For **User search base**, type the distinguished name (DN) on the server to search for users. This can be the root of the directory tree (for example, **dc=example,dc=com**) or a sub-tree (for example. **ou=People,dc=example,dc=com**).
11. For **Login attribute**, enter the user attribute containing the login of the authenticated user. For example, in the LDAP user configuration, the login attribute is **uid**. If this attribute is not set, the user will be denied access.
12. (Optional) For **Group attribute**, type the name of the user attribute that contains the list of IX10 authentication groups that the authenticated user has access to. See LDAP user configuration for further information about the group attribute.
13. For **Timeout**, type or select the amount of time in seconds to wait for the LDAP server to respond. Allowed value is between **3** and **60** seconds.
14. Add LDAP to the authentication methods:
    a. Click **Authentication** > **Methods**.
    b. For **Add method**, click ♈.



    c. Select **LDAP** for the new method from the **Method** drop-down.



    Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.
15. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Prevent other authentication methods from being used if LDAP authentication fails. Other authentication methods will only be used if the LDAP server is unavailable.

```
(config)> auth ldap authoritative true
(config)>
```

4. Set the type of TLS connection used by the LDAP server:

```
(config)> auth ldap tls value
(config)>
```

   where *value* is one of:

   - **off**: Uses a non-secure TCP connection on the LDAP standard port, 389.
   - **on**: Uses an SSL/TLS encrypted connection on port 636.
   - **start_tls**: Makes a non-secure TCP connection to the LDAP server on port 389, then sends a request to upgrade the connection to a secure TLS connection. This is the preferred method for LDAP.

   The default is **off**.

5. If **tls** is set to **on** or **start_tls**, configure whether to verify the server certificate:

```
(config)> auth ldap verify_server_cert value
(config)>
```

   where *value* is either:

   - **true**: Verifies the server certificate with a known Certificate Authority.
   - **false**: Does not verify the certificate. Use this option if the server is using a self-signed certificate.

   The default is **true**.

6. Set the distinguished name (DN) that is used to bind to the LDAP server and search for users. Leave this option unset if the server allows anonymous connections.

```
(config)> auth ldap bind_dn dn_value
(config)>
```

   For example:

```
(config)> auth ldap bind_dn cn=user,dc=example,dc=com
(config)>
```

7. Set the password used to log into the LDAP server. Leave this option unset if the server allows anonymous connections.

```
(config)> auth ldap bind_password password
(config)>
```

8. Set the distinguished name (DN) on the server to search for users. This can be the root of the directory tree (for example, **dc=example,dc=com**) or a sub-tree (for example. **ou=People,dc=example,dc=com**).

```
(config)> auth ldap base_dn value
(config)>
```

9. Set the login attribute:

```
(config)> auth ldap login_attribute value
(config)>
```

where value is the user attribute containing the login of the authenticated user. For example, in the LDAP user configuration, the login attribute is **uid**. . If this attribute is not set, the user will be denied access.

10. (Optional) Set the name of the user attribute that contains the list of IX10 authentication groups that the authenticated user has access to. See LDAP user configuration for further information about the group attribute.

```
(config)> auth ldap group_attribute value
(config)>
```

For example:

```
(config)> auth ldap group_attribute ou
(config)>
```

11. Configure the amount of time in seconds to wait for the LDAP server to respond.

```
(config)> auth ldap timeout value
(config)>
```

where *value* is any integer from **3** to **60**. The default value is **3**.

12. Add an LDAP server:
    a. Add the server:

```
(config)> add auth ldap server end
(config auth ldap server 0)>
```

    b. Enter the LDAP server's IP address or hostname:

```
(config auth ldap server 0)> hostname hostname|ip-address
(config auth ldap server 0)>
```

c. (Optional) Change the default port setting to the appropriate port:

```
(config auth ldap server 0)> port port
(config auth ldap server 0)>
```

d. (Optional) Repeat the above steps to add additional LDAP servers.

13. Add LDAP to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add LDAP to the end of the list. See User authentication methods for information about adding methods to the beginning or middle of the list.

```
(config)> add auth method end ldap
(config)>
```

14. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

15. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure serial authentication

This section describes how to configure authentication for serial access.

Web

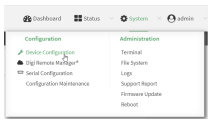
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Serial**.

4. (Optional) For **TLS identity certificate**, paste a TLS certificate and private key in PEM format. If empty, the certificate for the web administration service is used. See Configure the web administration service for more information.
5. For **Peer authentication**, select the method used to verify the certificate of a remote peer.
6. **Include standard CAs** is enabled by default. This allows peers with certificates that have been signed by standard Certificate Authorities (CAs) to authenticate.
7. Click to expand **Custom certificate authorities** to add the public certificates of custom CAs.
   a. For **Add CA certificate**, type the name of a custom CA and click ♑
   b. Paste the public certificate for the custom CA in PEM format.
   c. Repeat for additional custom CA certificates.
8. Click to expand **Peer certificates** to add the public certificates of trusted peers.
   a. For **Add Peer certificate**, type the name of a trusted peer and click ♑
   b. Paste the public certificate for the trusted peer in PEM format.
   c. Repeat for additional trusted peer certificates.
9. Enable **TelNet Login**, which requires a user to login via the TelNet connection before accessing a port.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Paste a TLS certificate and private key in PEM format:

```
(config)> auth serial identiy "cert-and-private-key"
(config)>
```

4. Set the method used to verify the certificate of a remote peer:

```
(config)> auth serial verify value
(config)>
```

   where *value* is either:
   - **ca**: Uses certificate authorities (CAs) to verify.
   - **peer**: Uses the remote peer's public certificate to verify.
5. By default, peers with certificates that have been signed by standard Certificate Authorities (CAs) are allowed to authenticate. To disable:

```
(config)> auth serial ca_standard false
(config)>
```

6. Add the public certificate for a custom certificate authority:

```
(config)> add auth serial ca_certs CA-cert-name "cert-and-private-key"
(config)>
```

where:

- *CA-cert-name* is the name of the certificate for the custom certificate authority.
- *cert-and-private-key* is the certificate and private key for the custom certificate authority.

Repeat for additional custom certificate authorities.

7. Require a user to login via the TelNet connection before accessing a port.

```
(config)> auth serial telnet_login?
(config)>
```

1. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

2. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable shell access

To prohibit access to the shell prompt for all authentication groups, disable the **Allow shell** parameter.. This does not prevent access to the Admin CLI.

Note If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

Web

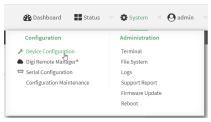
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

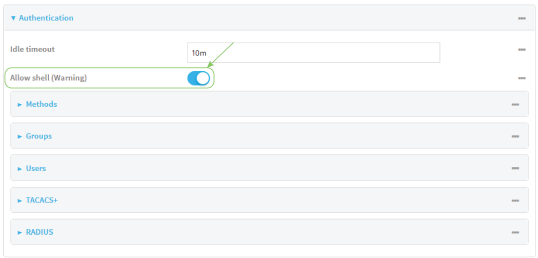
   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication**.
4. Click to disable **Allow shell**.



Note If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set the **allow_shell** parameter to **false**:

```
(config)> auth allow_shell false
```

Note If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Set the idle timeout for IX10 users

To configure the amount of time that the user's active session can be inactive before it is automatically disconnected, set the **Idle timeout** parameter.

By default, the Idle timeout is set to 10 minutes.

Web

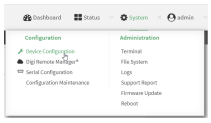
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

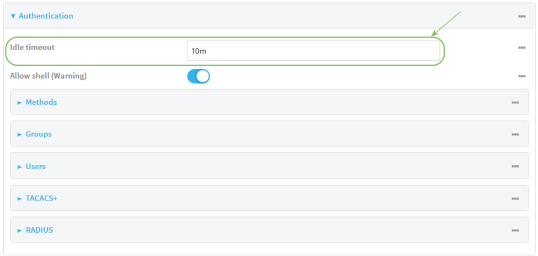
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication**.
4. For **Idle timeout**, enter the amount of time that the active session can be idle before the user is automatically logged out.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```

3. At the config prompt, type:

   ```
   (config)> auth idle_timeout value
   ```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **idle_timeout** to ten minutes, enter either **10m** or **600s**:

   ```
   (config)> auth idle_timeout  600s
   (config)>
   ```

4. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example user configuration

Example 1: Administrator user with local authentication

Goal: To create a user with administrator rights who is authenticated locally on the device.

Web

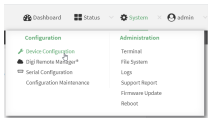
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

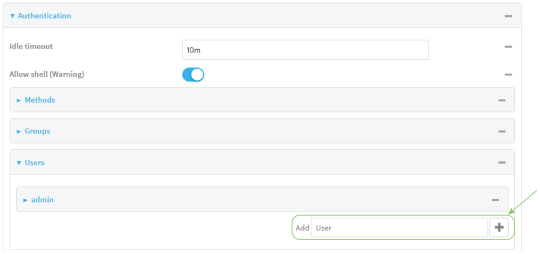
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

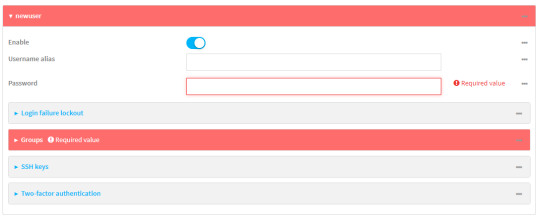
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Authentication** > **Users**.
4. In **Add User:** enter a name for the user and click ♑.

   The user configuration window is displayed.



5. Enter a **Password** for the user.
6. Assign the user to the **admin** group:
   a. Click **Groups**.
   b. For **Add Group**, click .
   c. For **Group**, select the **admin** group.
   d. Verify that the **admin** group has full administrator rights:
      i. Click **Authentication** > **Groups**.
      ii. Click **admin**.
      iii. Verify that the admin group has **Admin access** enabled. If not, click **Admin access** to enable.
      iv. Verify that **Access level** is set to **Full access**. If not, select **Full access**.
   e. Verify that **Local users** is one of the configured authentication methods:
      i. Click **Authentication** > **Methods**.
      ii. Verify that **Local users** is one of the methods listed in the list. If not:
         i. For **Add Method**, click .
         ii. For **Method**, select **Local users**.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Verify that the **admin** group has full administrator rights:

```
(config)> show auth group admin acl
admin
    enable true
    level full
...
(config)>
```

If **admin** > **enable** is set to false:

```
(config)> auth group admin acl admin enable true
(config)>
```

If **admin** > **level** is set to read-only:

```
(config)> auth group admin acl admin level full
(config)>
```

4. Verify that **local** is one of the configured authentication methods:

```
(config)> show auth method
0 local
(config)>
```

If **local** is not listed:

```
(config)> add auth method end local
(config)>
```

5. Create the user. In this example, the user is being created with the username **adminuser**:

```
(config)> add auth user adminuser
(config auth user adminuser)>
```

6. Assign a password to the user:

```
(config auth user adminuser)> password pwd
(config auth user adminuser)>
```

7. Assign the user to the **admin** group:

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

8. Save the configuration and apply the change.

```
(config auth user adminuser)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example 2: RADIUS, TACACS+, and local authentication for one user

Goal: To create a user with administrator rights who is authenticated by using all three authentication methods.

In this example, when the user attempts to log in to the IX10 device, user authentication will occur in the following order:

1. The user is authenticated by the RADIUS server. If the RADIUS server is unavailable,
2. The user is authenticated by the TACACS+ server. If both the RADIUS and TACACS+ servers are unavailable,
3. The user is authenticated by the IX10 device using local authentication.

This example uses a FreeRadius 3.0 server running on ubuntu, and a TACACS+ server running on ubuntu. Server configuration may vary depending on the platforms or type of servers used in your environment.

Web

1. Configure a user on the RADIUS server:
   a. On the ubuntu machine hosting the FreeRadius server, open the **/etc/freeradius/3.0/users** file:

   ```
   $ sudo gedit /etc/freeradius/3.0/users
   ```

   b. Add a RADIUS user to the **users** file:

   ```
   admin1 Cleartext-Password := "password1"
       Unix-FTP-Group-Names := "admin"
   ```

   In this example:
   - The user's username is **admin1**.
   - The user's password is **password1**.
   - The authentication group on the IX10 device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.

   c. Save and close the **users** file.
2. Configure a user on the TACACS+ server:
   a. On the ubuntu machine hosting the TACACS+ server, open the **/etc/tacacs+/tac_plus.conf** file:

   ```
   $ sudo gedit /etc/tacacs+/tac_plus.conf
   ```

   b. Add a TACACS+ user to the **tac_plus.conf** file:

   ```
   user = admin1 {
       name ="Admin1 for TX64"
       pap = cleartext password1
       service = system {
             groupname = admin
             }
       }
   }
   ```

   In this example:
   - The user's username is **admin1**.
   - The user's password is **password1**.
   - The authentication group on the IX10 device, **admin**, is identified in the **groupname** parameter.

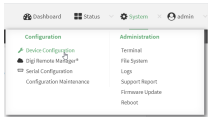
   c. Save and close the **tac_plus.conf** file.
3. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
4. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

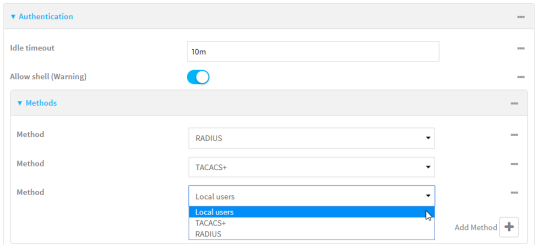
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

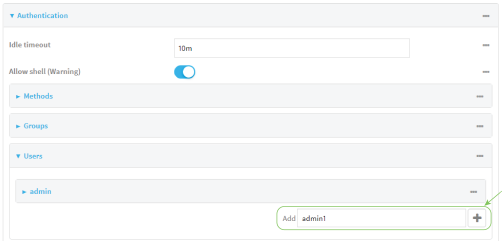


The **Configuration** window is displayed.

5. Configure the authentication methods:
   a. Click **Authentication** > **Methods**.
   b. For **Method**, select **RADIUS**.
   c. For **Add Method**, click to add a new method.
   d. For the new method, select **TACACS+**.
   e. Click to add another new method.
   f. For the new method, select **Local users**.



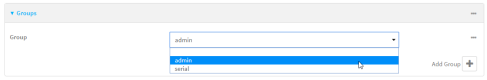
6. Create the local user:
   a. Click **Authentication** > **Users**.
   b. In **Add User:**, type **admin1** and click .



   c. For **password**, type **password1**.

d. Assign the user to the **admin** group:
   i. Click **Groups**.
   ii. For **Add Group**, click .

   iii. For **Group**, select the **admin** group.



a. Verify that the **admin** group has full administrator rights:
   i. Click **Authentication** > **Groups**.
   ii. Click **admin**.
   iii. Verify that the admin group has **Admin access** enabled. If not, click **Admin access** to enable.
   iv. Verify that **Access level** is set to **Full access**. If not, select **Full access**.

7. Click **Apply** to save the configuration and apply the change.

Command line

1. Configure a user on the RADIUS server:
   a. On the ubuntu machine hosting the FreeRadius server, open the **/etc/freeradius/3.0/users** file:

```
$ sudo gedit /etc/freeradius/3.0/users
```

   b. Add a RADIUS user to the **users** file:

```
admin1 Cleartext-Password := "password1"
    Unix-FTP-Group-Names := "admin"
```

   In this example:
   - The user's username is **admin1**.
   - The user's password is **password1**.
   - The authentication group on the IX10 device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.

   c. Save and close the **users** file.
2. Configure a user on the TACACS+ server:
   a. On the ubuntu machine hosting the TACACS+ server, open the **/etc/tacacs+/tac_plus.conf** file:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

b. Add a TACACS+ user to the **tac_plus.conf** file:

```
user = admin1 {
    name ="Admin1 for TX64"
    pap = cleartext password1
    service = system {
        groupname = admin
        }
    }
}
```

In this example:

- The user's username is **admin1**.
- The user's password is **password1**.
- The authentication group on the IX10 device, **admin**, is identified in the **groupname** parameter.

c. Save and close the **tac_plus.conf** file.

3. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

4. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

5. Configure the authentication methods:

   a. Determine the current authentication method configuration:

```
(config)> show auth method
0 local
(config)>
```

   This output indicates that on this example system, only local authentication is configured.

   b. Add RADIUS authentication to the beginning of the list:

```
(config)> add auth method 0 radius
(config)>
```

   c. Add TACACS+ authentication second place in the list:

```
(config)> add auth method 1 tacacs+(config)>
```

   d. Verify that authentication will occur in the correct order:

```
(config)> show auth method
0 radius
1 tacacs+
```

```
2 local
(config)>
```

6. Verify that the **admin** group has full administrator rights:

```
(config)> show auth group admin acl
admin
    enable true
    level full
...
(config)>
```

If **admin** > **enable** is set to false:

```
(config)> auth group admin acl admin enable true
(config)>
```

If **admin** > **level** is set to read-only:

```
(config)> auth group admin acl admin level full
(config)>
```

7. Configure the local user:
   a. Create a local user with the username **admin1**:

```
(config)> add auth user admin1
(config auth user admin1)>
```

   b. Assign a password to the user:

```
(config auth user adminuser)> password password1
(config auth user adminuser)>
```

   c. Assign the user to the **admin** group:

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

8. Save the configuration and apply the change.

```
(config auth user adminuser)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Firewall

This chapter contains the following topics:

Firewall configuration 753
Port forwarding rules 758
Packet filtering 765
Configure custom firewall rules 772
Configure Quality of Service options 774
Web filtering 783

Firewall configuration

Firewall configuration includes the following configuration options:

- **Zones**: A zone is a firewall access group to which network interfaces can be added. You then use zones to configure packet filtering and access control lists for interfaces that are included in the zone. Preconfigured zones include:
  - **Any**: Matches any network interface, even if they are not assigned to this zone.
  - **Loopback**: Zone for interfaces that are used for communication between processes running on the device.
  - **Internal**: Used for interfaces connected to trusted networks. By default, the firewall will allow most access from this zone.
  - **External**: Used for interfaces to connect to untrusted zones, such as the internet. This zone has Network Address Translation (NAT) enabled by default. By default, the firewall will block most access from this zone.
  - **Edge**: Used for interfaces connected to trusted networks, where the device is a client on the edge of the network rather than a router or gateway.
  - **Setup**: Used for interfaces involved in the initial setup of the device. By default, the firewall will only allow this zone to access administration services.
  - **IPsec**: The default zone for IPsec tunnels.
  - **Dynamic routes**: Used for routes learned using routing services.
- **Port forwarding**: A list of rules that allow network connections to the IX10 to be forwarded to other servers by translating the destination address.
- **Packet filtering**: A list of packet filtering rules that determine whether to accept or reject network connections that are forwarded through the IX10.
- **Custom rules**: A script that is run to install advanced firewall rules beyond the scope/capabilities of the standard device configuration.
- **Quality Of Service**: Quality of Service (QOS) options for bandwidth allocation and policy-based traffic shaping and prioritizing.

Create a custom firewall zone

In addition to the preconfigured zones, you can create your custom zones that can be used to configure packet filtering and access control lists for network interfaces.

To create a zone:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

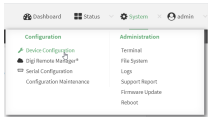
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

   b. Click the **Device ID**.

c. Click **Settings**.
d. Click to expand **Config**.

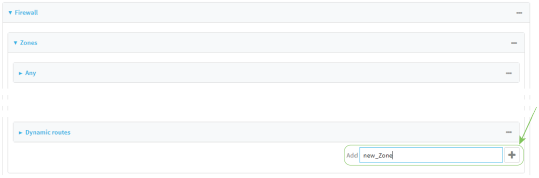
Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

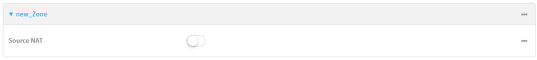


The **Configuration** window is displayed.

3. Click **Firewall** > **Zones**.
4. In **Add Zone**, enter a name for the zone and click .



The firewall configuration window is displayed.



5. (Optional) If traffic on this zone will be forwarded from a private network to the internet, enable Network Address Translation (NAT).
6. Click **Apply** to save the configuration and apply the change.

See Configure the firewall zone for a network interface for information about how to configure network interfaces to use a zone.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the new zone. For example, to add a zone named **my_zone**:

```
(config)> add firewall zone my_zone
(config firewall zone my_zone)>
```

4. (Optional) Enable Network Address Translation (NAT):

```
(config firewall zone my_zone)> src_nat true
(config firewall zone my_zone)>
```

5. Save the configuration and apply the change.

```
(config firewall zone my_zone)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See Configure the firewall zone for a network interface for information about how to configure network interfaces to use a zone.

Configure the firewall zone for a network interface

Firewall zones allow you to group network interfaces for the purpose of packet filtering and access control. There are several preconfigured firewall zones, and you can create custom zones as well. The firewall zone that a network interfaces uses is selected during interface configuration.

This example procedure uses an existing network interface named **ETH** and changes the firewall zone from the default zone, **Internal**, to **External**.

Web

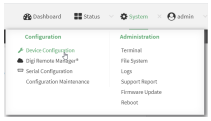
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

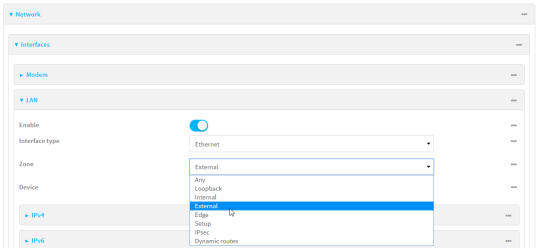
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces** > **ETH**.

4. For **Zone**, select **External**.



5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> network interface eth zone my_zone
(config)>
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a custom firewall zone

You cannot delete preconfigured firewall zones. To delete a custom firewall zone:

Web

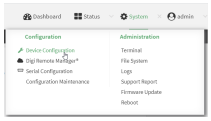
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall** > **Zones**.
4. Click the menu icon (**...**) next to the appropriate custom firewall zone and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **del** command to delete a custom firewall rule. For example:

```
(config)> del firewall zone my_zone
```

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Port forwarding rules

Most computers are protected by a firewall that prevents users on a public network from accessing servers on the private network. To allow a computer on the Internet to connect to a specific server on a private network, set up one or more port forwarding rules. Port forwarding rules provide mapping instructions that direct incoming traffic to the proper device on a LAN.

Configure port forwarding

Required configuration items

- The network interface for the rule.

  Network connections will only be forwarded if their destination address matches the IP address of the selected network interface.
- The public-facing port number that network connections must use for their traffic to be forwarded.
- The IP address of the server to which traffic should be forwarded.
- The port or range of ports to which traffic should be forwarded.

Additional configuration items

- A label for the port forwarding rule.
- The IP version (either IPv4 or IPv6) that incoming network connections must match.
- The protocols that incoming network connections must match.
- A white list of devices, based on either IP address or firewall zone, that are authorized to leverage this forwarding rule.

To configure a port forwarding rule:

Web

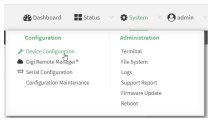
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

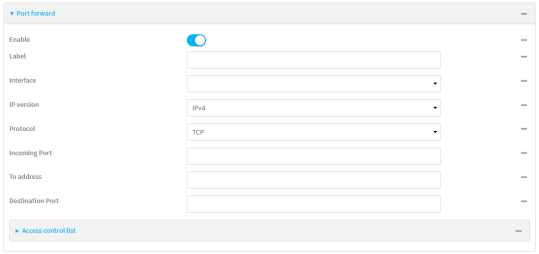
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall** > **Port forwarding**.
4. For **Add port forward**, click .

The port forwarding rule configuration window is displayed.



Port forwarding rules are enabled by default. To disable, toggle off **Enable**.

5. (Optional) Type a **Label** that will be used to identify the rule.
6. For **Interface**, select the network interface for the rule.

   Network connections will only be forwarded if their destination address matches the IP address of the selected network interface.
7. For **IP version**, select either **IPv4** or **IPv6**.

   Network connections will only be forwarded if they match the selected IP version.
8. For **Protocol**, select the type of internet protocol.

   Network connections will only be forwarded if they match the selected protocol.
9. For **Incoming port(s)**, type the public-facing port number that network connections must use for their traffic to be forwarded.
10. For **To Address**, type the IP address of the server to which traffic should be forwarded.
11. For **Destination Port(s)**, type the port number, comma-separated list of port numbers, or range of port numbers on the server to which traffic should be forwarded. For example, to forward traffic to ports one, three, and five through ten, enter: **1, 3, 5-10**.
12. (Optional) Click **Access control list** to create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone:
    - To white list IP addresses:
      a. Click **Addresses**.
      b. For **Add Address**, enter an IP address and click .
      c. Repeat for each additional IP address that should be white listed.

- To specify firewall zones for white listing:
  a. Click **Zones**.
  b. For **Add zone**, click ⅋.
  c. For **Zone**, select the appropriate zone.
  d. Repeat for each additional zone.

13. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> add firewall dnat end
(config firewall dnat 0)>
```

   Port forwarding rules are enabled by default. To disable the rule:

```
(config firewall dnat 0)> enable false
(config firewall dnat 0)>
```

4. Set the network interface for the rule.

```
(config firewall dnat 0)> interface
(config firewall dnat 0)>
```

   Network connections will only be forwarded if their destination address matches the IP address of this network interface.

   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config firewall dnat 0)> interface eth1
(config firewall dnat 0)>
```

5. Set the IP version. Allowed values are **ipv4** and **ipv6**. The default is **ipv4**.

```
(config firewall dnat 0)> ip_version ipv6
(config firewall dnat 0)>
```

6. Set the public-facing port number that network connections must use for their traffic to be forwarded.

```
(config firewall dnat 0)> port port
(config firewall dnat 0)>
```

7. Set the type of internet protocol .

```
(config firewall dnat 0)> protocol value
(config firewall dnat 0)>
```

Network connections will only be forwarded if they match the selected protocol. Allowed values are **custom**, **tcp**, **tcpudp**, or **upd**. The default is **tcp**.

8. Set the IP address of the server to which traffic should be forwarded:
   - For IPv4 addresses:

```
(config firewall dnat 0)> to_address ip-address
(config firewall dnat 0)>
```

   - For IPv6 addresses:

```
(config firewall dnat 0)> to_address6 ip-address
(config firewall dnat 0)>
```

9. Set the public-facing port number(s) that network connections must use for their traffic to be forwarded.

```
(config firewall dnat 0)> to_port value
(config firewall dnat 0)>
```

where *value* is the port number, comma-separated list of port numbers, or range of port numbers on the server to which traffic should be forwarded. For example, to forward traffic to ports one, three, and five through ten, enter **1, 3, 5-10**.

10. (Optional) To create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone, change to the acl node:

```
(config firewall dnat 0)> acl
(config firewall dnat 0 acl)>
```

    - To white list an IP address:
      - For IPv4 addresses:

```
(config firewall dnat 0 acl> add address end ip-address
(config firewall dnat 0 acl)>
```

      - For IPv6 addresses:

```
(config firewall dnat 0 acl> add address6 end ip-address
(config firewall dnat 0 acl)>
```

      Repeat for each appropriate IP address.
    - To specify the firewall zone for white listing:

```
(config firewall dnat 0 acl)> add zone end zone
```

Repeat for each appropriate zone.

To view a list of available zones:

```
(config firewall dnat 0 acl)> .. .. .. zone ?

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules
and access control lists.

 Additional Configuration
 ------------------------------------------------------------------------------
 any
 dynamic_routes
 edge
 external
 internal
 ipsec
 loopback
 setup

(config firewall dnat 0 acl)>
```

11. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a port forwarding rule

To delete a port forwarding rule:

Web

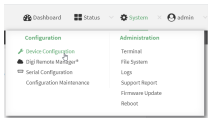
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall** > **Port forwarding**.
4. Click the menu icon (**...**) next to the appropriate port forwarding rule and select **Delete**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Determine the index number of the port forwarding rule you want to delete:

```
(config)> show firewall dnat
0
    acl
        no address
        no zone
    enable true
    interface
    ip_version ipv4
    label IPv4 port forwarding rule
    port 10000
    protocol tcp
    to_address6 10.10.10.10
    to_port 10001

1
    acl
        no address6
        no zone
    enable false
    interface
    ip_version ipv6
```

```
    label IPv6 port forwarding rule
    port 10002
    protocol tcp
    to_address6 c097:4533:bd63:bb12:9a6f:5569:4b53:c29a
    to_port 10003
(config)>
```

4. To delete the rule, use the index number with the **del** command. For example:

```
(config)> del firewall dnat 1
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Packet filtering

Configure packet filtering

Required configuration items

- The action that the packet filtering rule will perform, either **Accept**, **Reject**, or **Drop**.
- The source firewall zone: Packets originating from interfaces on this zone will be monitored by this rule.
- The destination firewall zone: Packets destined for interfaces on this zone will be accepted, rejected, or dropped by this rule.

Additional configuration requirements

- A label for the rule.
- The IP version to be matched, either **IPv4**, **IPv6**, or **Any**.
- The protocol to be matched, one of:
  - **TCP**
  - **UDP**
  - **ICMP**
  - **ICMP6**
  - **Any**

To configure a packet filtering rule:

Web

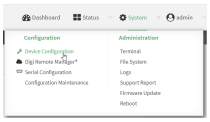
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

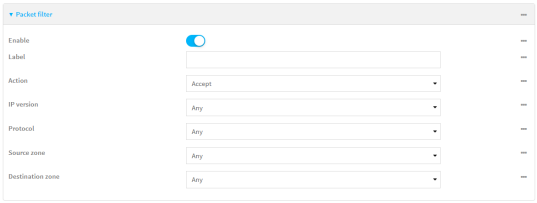
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall** > **Packet filtering**.
   - To create a new packet filtering rule, for **Add packet filter**, click ⅋
   - To edit the default packet filtering rule or another existing packet filtering rule, click to expand the rule.

   The packet filtering rule configuration window is displayed.



   Packet filters are enabled by default. To disable, toggle off **Enable**.
4. (Optional) Type a **Label** that will be used to identify the rule.
5. For **Action**, select one of:
   - **Accept**: Allows matching network connections.
   - **Reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
   - **Drop**: Blocks matching network connections, and does not send a reply.
6. Select the **IP version**.
7. Select the **Protocol**.
8. For **Source zone**, select the firewall zone that will be monitored by this rule for incoming connections from network interfaces that are a member of this zone.

   See Firewall configuration for more information about firewall zones.
9. For **Destination zone**, select the firewall zone. Packets destined for network interfaces that are members of this zone will either be accepted, rejected or dropped by this rule.

   See Firewall configuration for more information about firewall zones.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

To edit the default packet filtering rule or another existing packet filtering rule:

a. Determine the index number of the appropriate packet filtering rule:

```
(config)> show firewall filter
0
   action accept
   dst_zone any
   enable true
   ip_version any
   label Allow all outgoing traffic
   protocol any
   src_zone internal
1
   action drop
   dst_zone internal
   enable true
   ip_version any
   label myfilter
   protocol any
   src_zone external
(config)>
```

b. Select the appropriate rule by using its index number:

```
(config)> firewall filter 1
(config firewall filter 1)>
```

To create a new packet filtering rule:

```
(config)> add firewall filter end
(config firewall filter 1)>
```

Packet filtering rules are enabled by default. To disable the rule:

```
(config firewall filter 1)> enable false
(config firewall filter 1)>
```

3. (Optional) Set the label for the rule.

```
(config firewall filter 1)> label "My filter rule"
(config firewall filter 1)>
```

4. Set the action to be performed by the filter rule.

```
(config firewall filter 1)> action value
(config firewall filter 1)>
```

where *value* is one of:

- **accept**: Allows matching network connections.
- **reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
- **drop**: Blocks matching network connections, and does not send a reply.

5. Set the firewall zone that will be monitored by this rule for incoming connections from network interfaces that are a member of this zone:

   See Firewall configuration for more information about firewall zones.

```
(config firewall filter 1)> src_zone my_zone
(config firewall filter 1)>
```

6. Set the destination firewall zone. Packets destined for network interfaces that are members of this zone will either be accepted, rejected or dropped by this rule.

   See Firewall configuration for more information about firewall zones.

```
(config firewall filter 1)> dst_zone my_zone
(config firewall filter 1)>
```

7. Set the IP version.

```
(config firewall filter 1)> ip_version value
(config firewall filter 1)>
```

   where *value* is one of:

   - **any**
   - **ipv4**
   - **ipv6**
   - The default is **any**.

8. Set the protocol.

```
(config firewall filter 1)> protocol value
(config firewall filter 1)>
```

   where value is one of:

   - **any**
   - **icmp**
   - **icmpv6**
   - **tcp**
   - **upd**

   The default is **any**.

9. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable or disable a packet filtering rule

To enable or disable a packet filtering rule:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

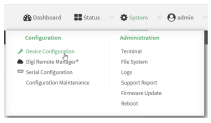
   b. Click the **Device ID**.

   c. Click **Settings**.

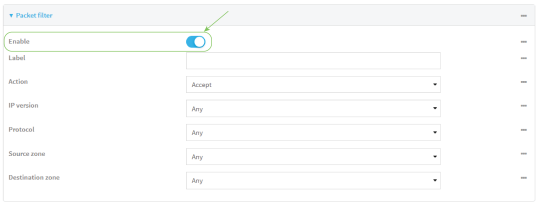
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Firewall** > **Packet filtering**.
4. Click the appropriate packet filtering rule.
5. Click **Enable** to toggle the rule between enabled and disabled.

6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Determine the index number of the appropriate port forwarding rule:

```
(config)> show firewall filter
0
   action accept
   dst_zone any
   enable true
   ip_version any
   label Allow all outgoing traffic
   protocol any
   src_zone internal
1
   action drop
   dst_zone internal
   enable true
   ip_version any
   label My packet filter
   protocol any
   src_zone external
(config)>
```

4. To enable a packet filtering rule, use the index number with the **enable true** command. For example:

```
(config)> firewall filter 1 enable true
```

5. To disable a packet filtering rule, use the index number with the **enable false** command. For example:

```
(config)> firewall filter 1 enable false
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a packet filtering rule

To delete a packet filtering rule:

Web

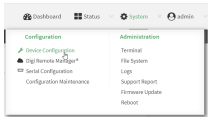
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Firewall** > **Packet filtering**.
4. Click the menu icon (**...**) next to the appropriate packet filtering rule and select **Delete**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Determine the index number of the packet filtering rule you want to delete:

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
```

```
   dst_zone internal
   enable true
   ip_version any
   label My packet filter
   protocol any
   src_zone external
(config)>
```

4. To delete the rule, use the index number with the **del** command. For example:

```
(config)> del firewall filter 1
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure custom firewall rules

Custom firewall rules consist of a script of shell commands that can be used to install firewall rules, ipsets, and other system configuration. These commands are run whenever system configuration changes occur that might cause changes to the firewall.

To configure custom firewall rules:

Web

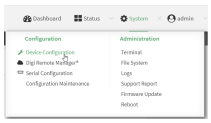
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall** > **Custom rules**.

4. **Enable** the custom rules.
5. (Optional) Enable **Override** to override all preconfigured firewall behavior and rely solely on the custom firewall rules.
6. For **Rules**, type the shell command that will execute the custom firewall rules script.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable custom firewall rules:

```
(config)> firewall custom enable true
(config)>
```

4. (Optional) Instruct the device to override all preconfigured firewall behavior and rely solely on the custom firewall rules:

```
(config)> firewall custom override true
(config)>
```

5. Set the shell command that will execute the custom firewall rules script:

```
(config)> firewall custom rules "shell-command"
(config)>
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure Quality of Service options

Quality of Service (QoS) options allow you to manage the traffic performance of various services, such as Voice over IP (VoIP), cloud computing, traffic shaping, traffic prioritizing, and bandwidth allocation. When configuring QOS, you can only control the queue for outgoing packets on each interface (egress packets), not what is received on the interface (packet ingress).

A QoS *binding* contains the policies and rules that apply to packets exiting the IX10 device on the binding's interface. By default, the IX10 device has two preconfigured QoS bindings, **Outbound** and **Inbound**. These bindings are an example configuration designed for a typical VoIP site:

- **Outbound** provides an example of matching packets as they are routed from the device onto the WAN interface.
- **Inbound** provides an example of matching packets as they are routed from the device onto a LAN interface.

These example bindings are disabled by default.

Enable the preconfigured bindings

Web

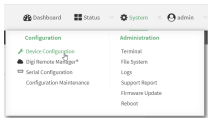
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Firewall** > **Quality of Service**.
4. Click to expand either **Outbound** or **Inbound**.
5. **Enable** the binding.
6. Select an **Interface**.

7. Examine the remaining default settings and modify as appropriate for your network.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable one of the preconfiged bindings:
   - To enable the Outbound binding:

```
(config)> firewall qos 0 enable true
(config)>
```

   - To enable the Inbound binding:

```
(config)> firewall qos 1 enable true
(config)>
```

4. Set the interface for the binding. Use the index number of the binding; for example, to set the interface for the Outbound binding:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config)> firewall qos 0 interface /network/interface/eth1
(config)>
```

5. Examine the remaining default settings and modify as appropriate for your network.
6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Create a new binding

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

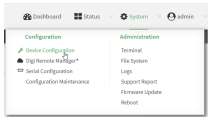
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

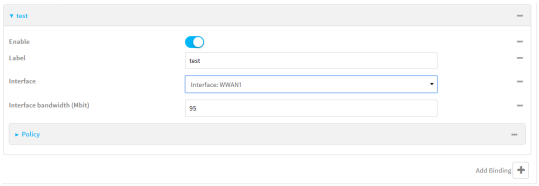
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **Firewall** > **Quality of Service**.
4. For **Add Binding**, click .

   The quality of service binding configuration window is displayed.

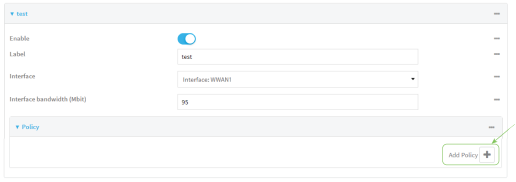
   

5. **Enable** the binding.
6. (Optional) Type a **Label** for the binding.
7. Select an **Interface** to queue egress packets on. The binding will only match traffic that is being sent out on this interface.
8. (Optional) For **Interface bandwidth (Mbit)**, set the maximum egress bandwidth of the interface, in megabits, allocated to this binding. Typically, this should be 95% of the available bandwidth. Allowed value is any integer between **1** and **1000**.
9. Create a policy for the binding:

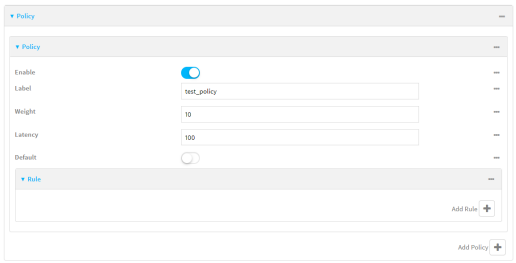
   At least one policy is required for each binding. Each policy can contain up to 30 rules.

a. Click to expand **Policy**.

b. For **Add Policy**, click .



The QoS binding policy configuration window is displayed.



New QoS binding policies are enabled by default. To disable, toggle off **Enable**.

c. (Optional) Type a **Label** for the binding policy.

d. For **Weight**, type a value for the amount of available bandwidth allocated to the policy, relative to other policies for this binding.

The larger the weight, with respect to the other policy weights, the larger portion of the maximum bandwidth is available for this policy. For example, if a binding contains three policies, and each policy contains a weight of 10, each policy will be allocated one third of the total interface bandwidth.

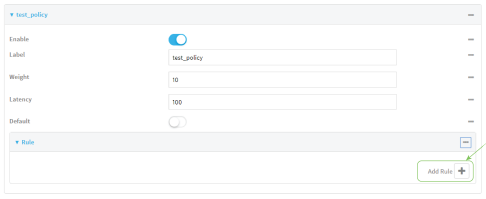
e. For **Latency**, type the maximum delay before the transmission of packets. A lower latency means that the packets will be scheduled more quickly for transmission.

f. Select **Default** to identify this policy as a fall-back policy. The fall-back policy will be used for traffic that is not matched by any other policy. If there is no default policy associated with this binding, packets that do not match any policy rules will be dropped.

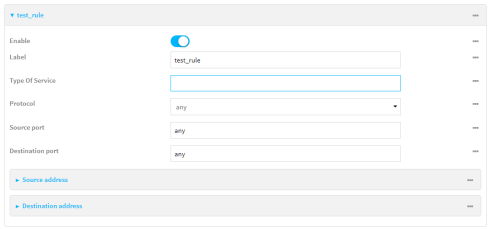
g. If **Default** is disabled, you must configure at least one rule:

i. Click to expand **Rule**.

ii. For **Add Rule**, click .



The QoS binding policy rule configuration window is displayed.



New QoS binding policy rules are enabled by default. To disable, toggle off **Enable**.

iii. (Optional) Type a **Label** for the binding policy rule.

iv. For **Type Of Service**, type the value of the Type of Service (ToS) packet header that defines packet priority. If unspecified, this field is ignored.

See https://www.tucny.com/Home/dscp-tos for a list of common TOS values.

v. For **Protocol**, select the IP protocol matching criteria for this rule.

vi. For **Source port**, type the port, or **any**, as a source traffic matching criteria.

vii. For **Destination port**, type the port, or **any**, as a destination traffic matching criteria.

viii. Click to expand **Source address** and select the **Type**:

- **Any**: Source traffic from any address will be matched.
- **Interface**: Only traffic from the selected **Interface** will be matched.
- **IPv4 address**: Only traffic from the IP address typed in **IPv4 address** will be matched. Use the format ***IPv4_address*[/*netmask*]**, or use **any** to match any IPv4 address.
- **IPv6 address**: Only traffic from the IP address typed in **IPv6 address** will be matched. Use the format ***IPv6_address*[/*prefix_length*]**, or use **any** to match any IPv6 address.
- **MAC address**: Only traffic from the MAC address typed in **MAC address** will be matched.

ix. Click to expand **Destination address** and select the **Type**:

- **Any**: Traffic destined for anywhere will be matched.
- **Interface**: Only traffic destined for the selected **Interface** will be matched.
- **IPv4 address**: Only traffic destined for the IP address typed in **IPv4 address** will be matched. Use the format ***IPv4_address*[/*netmask*]**, or use **any** to match any IPv4 address.
- **IPv6 address**: Only traffic destined for the IP address typed in **IPv6 address** will be matched. Use the format ***IPv6_address*[/*prefix_length*]**, or use **any** to match any IPv6 address.

Repeat to add a new rule. Up to 30 rules can be configured.

10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a binding:

```
(config)> add firewall qos end
(config firewall qos 2)>
```

New binding are enabled by default. To disable:

```
(config firewall qos 2)> enable false
(config firewall qos 2)>
```

4. (Optional) Set a label for the new binding:

```
(config firewall qos 2)> label my_binding
(config firewall qos 2)>
```

5. Set the interface to queue egress packets on. The binding will only match traffic that is being sent out on this interface:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config firewall qos 2)> interface /network/interface/eth1
(config firewall qos 2)>
```

6. (Optional) Set the maximum egress bandwidth of the interface, in megabits, allocated to this binding.

```
(config firewall qos 2)> bandwidth int
(config firewall qos 2)>
```

where *int* is an integer between **1** and **1000**. Typically, this should be 95% of the available bandwidth. The default is **95**.

7. Create a policy for the binding:

   At least one policy is required for each binding. Each policy can contain up to 30 rules.
   a. Change to the policy node of the configuration:

```
(config firewall qos 2)> policy
(config firewall qos 2 policy)>
```

   b. Add a policy:

```
(config firewall qos 2 policy)> add end
(config firewall qos 2 policy 0)>
```

   New QoS binding policies are enabled by default. To disable:

```
(config firewall qos 2 policy 0)> enable false
(config firewall qos 2 policy 0)>
```

c. (Optional) Set a label for the new binding policy:

```
(config firewall qos 2 policy 0)> label my_binding_policy
(config firewall qos 2 policy 0)>
```

d. Set a value for the amount of available bandwidth allocated to the policy, relative to other policies for this binding.

The larger the weight, with respect to the other policy weights, the larger portion of the maximum bandwidth is available for this policy. For example, if a binding contains three policies, and each policy contains a weight of 10, each policy will be allocated one third of the total interface bandwidth.

```
(config firewall qos 2 policy 0)> weight int
(config firewall qos 2 policy 0)>
```

where *int* is any integer between **1** and **65535**. The default is **10**.

e. Set the maximum delay before the transmission of packets. A lower number means that the packets will be scheduled more quickly for transmission.

```
(config firewall qos 2 policy 0)> latency int
(config firewall qos 2 policy 0)>
```

where *int* is any integer, **1** or greater. The default is **100**.

f. To identify this policy as a fall-back policy:

```
(config firewall qos 2 policy 0)> default true
(config firewall qos 2 policy 0)>
```

The fall-back policy will be used for traffic that is not matched by any other policy. If there is no default policy associated with this binding, packets that do not match any policy rules will be dropped. If the policy is not a fall-back policy, you must configure at least one rule:

i. Change to the rule node of the configuration:

```
(config firewall qos 2 policy 0)> rule
(config firewall qos 2 policy 0 rule)>
```

ii. Add a rule:

```
(config firewall qos 2 policy 0 rule)> add end
(config firewall qos 2 policy 0 rule 0)>
```

New QoS binding policy rules are enabled by default. To disable:

```
(config firewall qos 2 policy 0 rule 0)> enable false
(config firewall qos 2 policy 0 rule 0)>
```

iii. (Optional) Set a label for the new binding policy rule:

```
(config firewall qos 2 policy 0 rule 0)> label my_binding_policy_rule
(config firewall qos 2 policy 0 rule 0)>
```

iv. Set the value of the Type of Service (ToS) packet header that defines packet priority. If unspecified, this field is ignored.

```
(config firewall qos 2 policy 0 rule 0)> tos value
(config firewall qos 2 policy 0 rule 0)>
```

where value is a hexadecimal number. See https://www.tucny.com/Home/dscp-tos for a list of common TOS values.

v. Set the IP protocol matching criteria for this rule:

```
(config firewall qos 2 policy 0 rule 0)> protocol value
(config firewall qos 2 policy 0 rule 0)>
```

where *value* is one of **tcp**, **udp**, or **any**.

vi. Set the source port to define a source traffic matching criteria:

```
(config firewall qos 2 policy 0 rule 0)> srcport value
(config firewall qos 2 policy 0 rule 0)>
```

where *value* is the IP port number, a range of port numbers using the format *IP_port-IP_port*, or **any**.

vii. Set the destination port to define a destination matching criteria:

```
(config firewall qos 2 policy 0 rule 0)> dstport value
(config firewall qos 2 policy 0 rule 0)>
```

where *value* is the IP port number, a range of port numbers using the format *IP_port-IP_port*, or **any**.

viii. Set the source address type:

```
(config network qos 2 policy 0 rule 0)> src type value
(config network qos 2 policy 0 rule 0)>
```

where *value* is one of:

- **any**: Source traffic from any address will be matched.

  See Firewall configuration for more information about firewall zones.
- **interface**: Only traffic from the selected interface will be matched. Set the interface:
  i. Use the **?** to determine available interfaces:
  ii. Set the interface. For example:

  ```
  (config network qos 2 policy 0 rule 0)> src interface /network/interface/eth1
  (config network qos 2 policy 0 rule 0)>
  ```
- **address**: Only traffic from the IP address typed in **IPv4 address** will be matched. Set the address that will be matched:

  ```
  (config network qos 2 policy 0 rule 0)> src address value
  (config network qos 2 policy 0 rule 0)>
  ```

where value uses the format ***IPv4_address*[/*netmask*]**, or **any** to match any IPv4 address.

- **address6**: Only traffic from the IP address typed in **IPv6 address** will be matched. Set the address that will be matched:

```
(config network qos 2 policy 0 rule 0)> src address6 value
(config network qos 2 policy 0 rule 0)>
```

where value uses the format ***IPv6_address*[/*prefix_length*]**, or **any** to match any IPv6 address.

- **mac**: Only traffic from the MAC address typed in **MAC address** will be matched. Set the MAC address to be matched:

```
(config network qos 2 policy 0 rule 0)> src mac MAC_address
(config network qos 2 policy 0 rule 0)>
```

ix. Set the destination address type:

```
(config network qos 2 policy 0 rule 0)> dst type value
(config network qos 2 policy 0 rule 0)>
```

where *value* is one of:

- **any**: Traffic destined for anywhere will be matched.

  See Firewall configuration for more information about firewall zones.

- **interface**: Only traffic destined for the selected **Interface** will be matched. Set the interface:

  i. Use the **?** to determine available interfaces:

  ii. Set the interface. For example:

```
(config network qos 2 policy 0 rule 0)> dst interface /network/interface/eth1
(config network qos 2 policy 0 rule 0)>
```

- **address**: Only traffic destined for the IP address typed in **IPv4 address** will be matched. Set the address that will be matched:

```
(config network qos 2 policy 0 rule 0)> src address value
(config network qos 2 policy 0 rule 0)>
```

where value uses the format ***IPv4_address*[/*netmask*]**, or **any** to match any IPv4 address.

- **address6**: Only traffic destined for the IP address typed in **IPv6 address** will be matched. Set the address that will be matched:

```
(config network qos 2 policy 0 rule 0)> src address6 value
(config network qos 2 policy 0 rule 0)>
```

where value uses the format ***IPv6_address*[/*prefix_length*]**, or **any** to match any IPv6 address.

Repeat to add a new rule. Up to 30 rules can be configured.

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Web filtering

Web filtering allows you to control access to services that can be accessed through the IX10 device by forwarding all Domain Name System (DNS) traffic to a web filtering service. This allows the network security administrator to configure a set of policies with the web filtering service that are applied to all routing devices with web filtering enabled. For example, a policy may allow or deny access to a specific service or type of service such as social media, gaming, and so on.

Your IX10 device supports two methods for configuring web filtering:

- Cisco Umbrella (formally known as OpenDNS).
- Manual DNS server entry.

Configure web filtering with Cisco Umbrella

Required configuration items

- Enable web filtering.
- A Cisco Umbrella account.

  See https://umbrella.cisco.com for information about how to create a Cisco Umbrella account. A 14 day trial account is available.
- A customer-specific API token.

Task one: Generate a Cisco Umbrella API token

1. Log into the Cisco Umbrella Dashboard (https://dashboard.umbrella.com).
2. On the menu, select **Admin** > **API Keys**.

   The **API Keys** page displays.
3. Click ✞ (**Create**).
4. Select **Legacy Network Devices**.
5. Click **Create**.
6. Copy the token.

Task two: Configure web filtering

Web

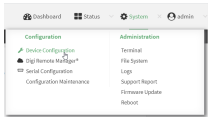
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

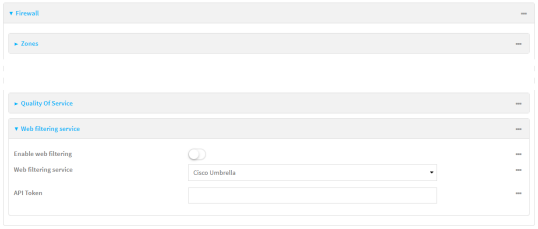
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Firewall** > **Web filtering service**.

   
4. Click **Enable web filtering** to enable.
5. For **Web filtering service**, select **Cisco Umbrella**.
6. Paste the **API token** that was generated in Task one: Generate a Cisco Umbrella API token.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable web filtering:

```
(config)> firewall web-filter enable true
(config)>
```

4. Set the web filter service type to **umbrella**:

```
(config)> firewall web-filter service umbrella
(config)>
```

5. Set umbrella_token to the API token generated in Task one: Generate a Cisco Umbrella API token:

```
(config)> firewall web-filter umbrella_token token
(config)>
```

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Clear the Cisco Umbrella device ID

If the Cisco Umbrella device ID being used by your IX10 is invalid, you can clear the device ID.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, use the rm command to delete the **web-filter-id** file, and confirm the deletion:

```
> rm /etc/config/web-filter-id
rm: remove '/etc/config/web-filter-id'? yes
>
```

3. Restart the web filtering service:

```
> config firewall web-filter enable false
> config firewall web-filter enable true
>
```

Configure web filtering with manual DNS servers

Required configuration items

- Enable web filtering.
- The IP address of one or more DNS servers. Cisco provides two open DNS servers for web filtering:
  - 208.67.222.222
  - 208.67.220.220

> **Note** These two IP addresses do not work with the OpenDNS option. See https://www.opendns.com/setupguide/ for more information about using Cisco DNS servers for web filtering.

To configure web filtering with manual DNS servers:

Web

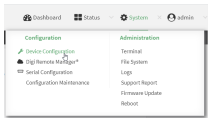
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

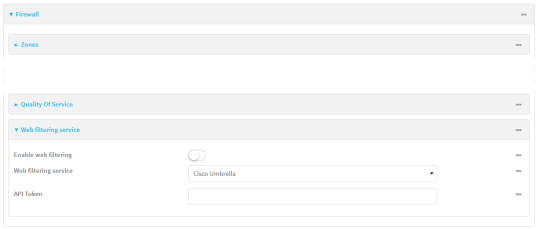
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

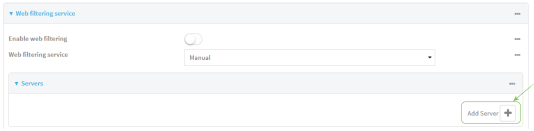
   

   The **Configuration** window is displayed.
3. Click **Firewall** > **Web filtering service**.

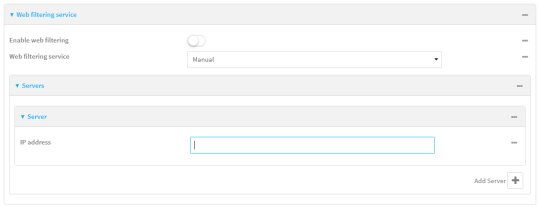
   

4. Click **Enable web filtering** to enable.

5. For **Web filtering service**, select **Manual**.
6. Click to expand **Servers**.
7. Click to add a server.



8. For **IP address**, enter the IP address of the DNS server.



9. (Optional) Repeat for additional DNS servers.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable web filtering:

```
(config)> firewall web-filter enable true
(config)>
```

4. Set the web filter service type to **manual**:

```
(config)> firewall web-filter service manual
(config)>
```

5. Add a DNS server:

```
(config)> add firewall web-filter server end
(config firewall web-filter server 0)>
```

6. Set the DNS server's IP address:

```
(config firewall web-filter server 0)> ip ip_address
(config firewall web-filter server 0)>
```

7. (Optional) Repeat for additional DNS servers.

   For example, to configure manual web-filtering using Cisco's open DNS servers:

   a. Enable web filtering:

   ```
   (config)> firewall web-filter enable true
   (config)>
   ```

   b. Set the web filter service type to **manual**:

   ```
   (config)> firewall web-filter service manual
   (config)>
   ```

   c. Add the first DNS server:

      i. Add the server:

      ```
      (config)> add firewall web-filter server end
      (config firewall web-filter server 0)>
      ```

      ii. Set the server's IP address:

      ```
      (config firewall web-filter server 0)> ip 208.67.222.220
      (config firewall web-filter server 0)>
      ```

   d. Add the second DNS server:

      i. Move back one node in the configuration tree:

      ```
      (config firewall web-filter server 0)> ..
      (config firewall web-filter server)>
      ```

      ii. Add the server:

      ```
      (config firewall web-filter server)> add end
      (config firewall web-filter server 1)>
      ```

      iii. Set the server's IP address:

      ```
      (config firewall web-filter server 1)> ip 208.67.222.222
      (config firewall web-filter server 0)>
      ```

8. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Verify your web filtering configuration

If your web filtering implementation has the service set to Cisco Umbrella, or if it is configured to use manual DNS servers and uses the Cisco open DNS servers, you can verify the web filtering implementation by using the Cisco test site www.internetbadguys.com.

To verify the implementation:

Web

This procedure assumes you have already configured web filtering to use either Cisco Umbrella or the Cisco open DNS servers.

- See Configure web filtering with Cisco Umbrella for information about configuring web filtering with Cisco Umbrella.
- See Configure web filtering with manual DNS servers for information about configuring web filtering to use Cisco open DNS servers.

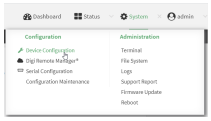
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

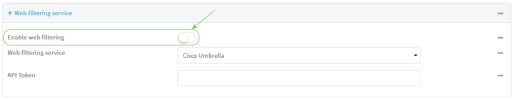
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Disable web filtering:
   a. Click **Firewall** > **Web filtering service**.
   b. Click **Enable web filtering** to disable.

   c. Click **Apply** to save the configuration and apply the change.
4. From a new tab in your browser, attempt to connect to the Cisco test URL http://www.internetbadguys.com.

   The connection should be successful.
5. Return to the IX10 WebUI and enable web filtering:
   a. Click **Firewall** > **Web filtering service**.
   b. Click **Enable web filtering** to enable.
   c. Click **Apply** to save the configuration and apply the change.

6. From your browser, attempt to connect to http://www.internetbadguys.com again.

   The connection attempt should fail with the message, "This site is blocked due to a phishing threat."

Command line

This procedure assumes you have already configured web filtering to use either Cisco Umbrella or the Cisco open DNS servers.

- See Configure web filtering with Cisco Umbrella for information about configuring web filtering with Cisco Umbrella.
- See Configure web filtering with manual DNS servers for information about configuring web filtering to use Cisco open DNS servers.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Disable web filtering:

```
> config firewall web-filter enable false
>
```

3. Attempt to connect to the Cisco test URL http://www.internetbadguys.com by using either a web browser or the **curl** command from a Linux shell:

```
$ curl -I http://www.internetbadguys.com
HTTP/1.1 200 OK
Server: Apache
Content-Type: text/html; charset=UTF-8
Accept-Ranges: bytes
Date: Thu, Jan 11, 2024 12:10:00
X-Varnish: 4201397492
Age: 0
Via: 1.1 varnish
Connection: keep-alive

$
```

   You should receive an "HTTP/1.1 200 OK" message, as highlighted above.

4. Return to the Admin CLI and enable web filtering:

```
> config firewall web-filter enable true
>
```

5. Attempt to connect to http://www.internetbadguys.com again:

```
$ curl -I www.internetbadguys.com
HTTP/1.1 403 Forbidden
Server: openresty/1.9.7.3
Date: Thu, Jan 11, 2024 12:10:00
Content-Type: text/html
```

```
Connection: keep-alive

$
```

You should receive an "HTTP/1.1 403 Forbidden" message, as highlighted above.

Show web filter service information

To view information about the web filter service:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, use the show web-filtercommand to view information about the web-filter service:

```
> show web-filter

 Enabled   : true
 Service   : umbrella
 Device ID  : 0004b5s63f5e2de7aa

>
```

If the device is configured to use Cisco Umbrella for web filtering, a device ID is displayed. The device ID is a unique ID assigned to the device by Cisco Umbrella. If there is a problem with the device ID, you can clear the ID. See Clear the Cisco Umbrella device ID for instructions.

Containers

The IX10 device includes support for LXC Linux containers. LXC containers are a lightweight, operating system level method of virtualization that allows you to run one or more isolated Linux instances on a the same host using the host's Linux kernal.

Note Container support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

This chapter contains the following topics:

Use Digi Remote Manager to deploy and run containers 793
Upload a new LXC container 797
Configure a container 798
Starting and stopping the container 803
View the status of containers 804
Schedule a script to run in the container 805
Create a custom container 808

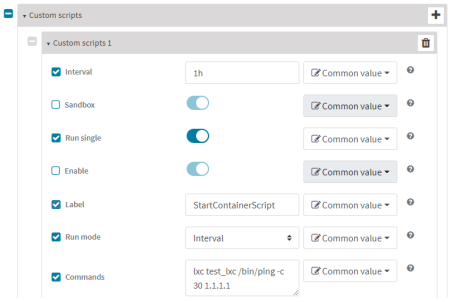
Use Digi Remote Manager to deploy and run containers

Note Container support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

1. In Remote Manager, create a Configuration template. See the Remote Manager User Guide for instructions.
   a. For the **Settings** step:
      - Click **Import from device** and import settings from an appropriate device.
      - Configure a script to run the container:
        i. Click **System**.
        ii. Click **Scheduled tasks** > **Custom scripts**.
        iii. Click to add a custom script.
        iv. Click the **Label** checkbox and type an identifiable label for the script, for example, **StartContainerScript**.
        v. To ensure that the script is always running:
           i. Click the **Run mode** checkbox and select **Interval**.
           ii. Click the **Interval** checkbox and enter a very short interval (for example, one minute).
           iii. Click the **Run single** checkbox, and toggle on to enable.

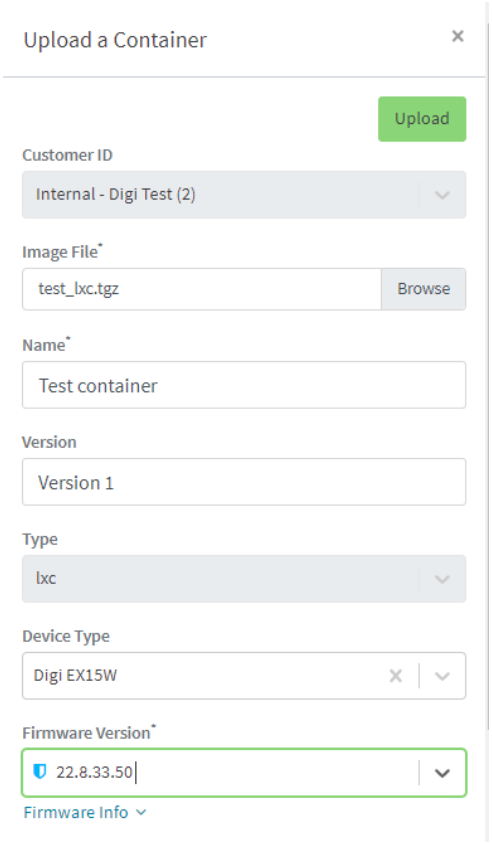
           This will configure the device to regularly check if the script is running, but only run if it is currently not running.
        vi. For **Commands**, type the command to run the script. The command will vary depending on how you want to run the script, and what application you want to run inside the script. For example, to run the ping command inside a container, the command would be:

```
lxc container_name /bin/ping -c 30 1.1.1.1
```



   b. For the **Containers** step:
      i. Click to add a container to the configuration.

      If no containers have been uploaded, or if Click ❽ to upload a container file.



i. Click **Browse** and select the container file.
ii. Type the **Name** of the container.

    The **Name** entered here must be the same name as the container .tgz file. This is absolutely necessary, otherwise the container file will not be properly configured on the local devices.
iii. (Optional) Include a version number for the container.
iv. (Optional) Select the **Device Type** and **Firmware Version** that applies to the container.

    If set, these options will limit the container to only be included in Configuration templates that match the specified device type and firmware version. If these are left blank, the container can be included in any Configuration template.
v. Click **Upload**.
vi. Repeat to upload additional containers.

ii. Select one or more containers to add to the configuration.
iii. Click **Done**.
iv. Click **Save**.
v. Click **Continue**.

c. For the **Automation** step:

i. Click to toggle on **Enable Scanning**.

ii. Click to toggle on **Remediate**.

2. Run a manual configuration scan to apply the container and configuration settings to all applicable devices.
3. Verify that the container is running on a device:

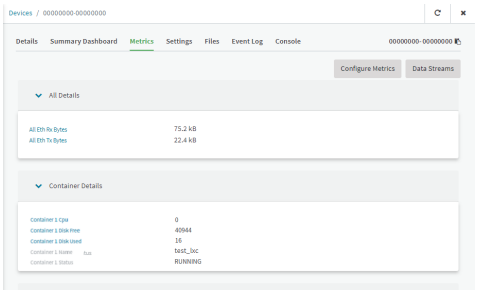
- To verify by using device metrics:

a. From the Remote Manager main menu, click **Management** > **Devices**.

b. Click the **Device ID** to open the device's **Details** page..

c. Click **Metrics**.

d. Information about configured containers is located under the **Container Details** heading.



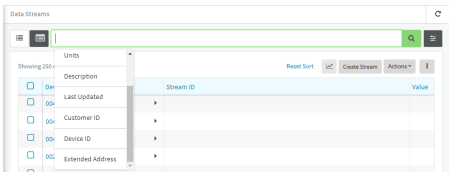
- To verify by using the **Data streams** page:

a. From the Remote Manager main menu, click **Management** > **Data Streams**.

b. Locate the container's data stream:

i. Click to search using advance filtering.

ii. Click in the search text bar and select **Device ID** from the menu.

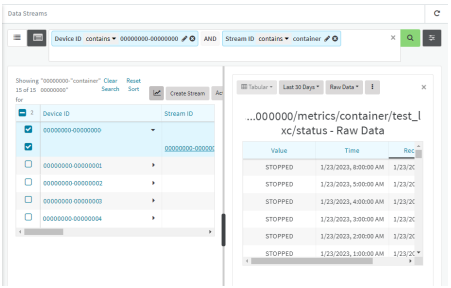


iii. Type the device ID and press the Enter key.

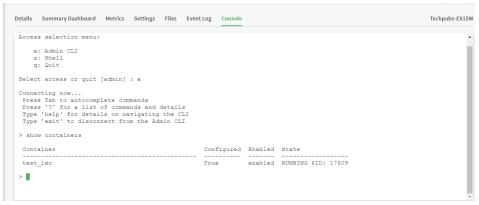
iv. Click in the search text bar again and select **Stream ID** from the menu.

v. Type container and press the Enter key.

vi. Click the **Stream ID** to view container status.



- To verify by using the **show containers** command on the local device:
  a. From the Remote Manager main menu, click **Management** > **Devices**.
  b. Select the device.
  c. From the **Actions** menu, select **Open Console**.
  d. At the prompt, type **show containers**.



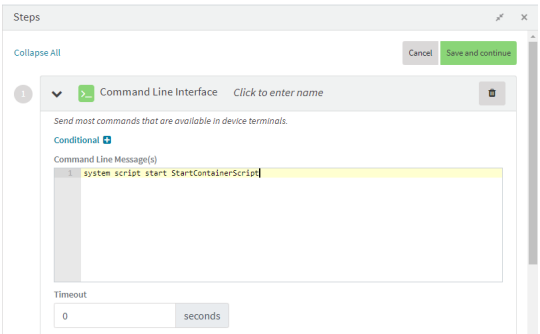
Use an automation to start the container

You can also use an automation to start a container:

1. Follow the steps in the previous procedure, except:
   - For **Run mode**, select **Manual**.
   - Do not set **Interval** or **Run single**.
2. Create an automationthat uses a Command Line Interface step.

   For the **Command Line Message**, use the system script start command, using the label provided for the script in the previous procedure:

```
system script start StartContainerScript
```



Once the automation has been created, you can:

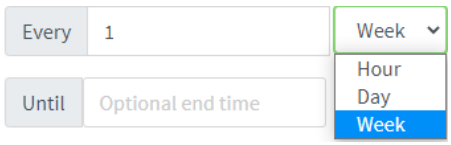
- Run the automation manually.
- Include the automation in a Configuration template as a post-remediation or post-scan step.

  When creating or editing a Configuration template, at the **Automation** page:

  1. For **Post Remediation Options**, click **Run Automation** and select the automation.
  2. For **On Successful Scan Options**, click **Run Automation** and select the automation.
- Include a trigger for the automation.

  When creating or editing an automation, at the **Triggers** page:

  1. Click to enable **Triggered** to configure the automation to be triggered, either on a schedule or by device activity.
     a. To configure the script to be run on a schedule:
        i. Click to enable **By Schedule**.
        ii. Click **Start Time**.
        iii. From the calendar provided, select the date and time that the script should be started for the first time.
        iv. By default, the script will run only once. Click to enable **Repeat** to configure the script to run on a regular basis:



        i. Type or select the number of times, and select the time period.
        ii. (Optional) Click **Until** to select a date and time when the automation schedule will stop repeating.

     b. To configure the automation to be triggered by device activity, click to enable one or more of the following:
        - **Run when a device enters the target scope**
        - **Run when a device in the target scope enters a maintenance window**:
        - **Run when a device in the target scope leaves debug mode**

        Target scope refers to a device that either:
        - Is member of a group that was selected on the **Target** page.
        - Has a tag that was selected on the **Target** page.
        - Is one of the devices included on the **Target** page.

Upload a new LXC container

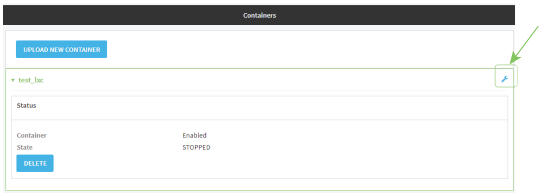
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. From the main menu, click **Status**. Under **Services**, click **Containers**.
2. Click **Upload New Container**.

3. From your local file system, select the container file in *.tgz format.

   You can download a simple example container file, test_lxc.tgz, from the Digi website.
4. **Create Configuration** is selected by default. This will create a configuration on the device for the container when it is installed. If deselected, you will need to create the configuration manually.
5. Click **Apply**.
6. If **Create Configuration** was deselected when the container was created, click ✷ to go to the container configuration.



See Configure a container for further information about configuring the container.

Configure a container

Required configuration items

- The following configuration options are completed automatically if **Create Configuration** was selected when the container was created. See Upload a new LXC container for details:
  - Name of the container.
  - Enable the container.
  - Whether or not the container should use the device's system libraries.
- Determine whether or not the device should including virtual networking capabilities.

Additional configuration items

- If virtual networking is enabled:
  - The bridge to be used to provide network connectivity.
  - A static IP address for the container.
  - The network gateway.
- Serial ports on the device that the container will have access to.

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

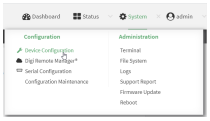
   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.

b. Click the **Device ID**.
c. Click **Settings**.
d. Click to expand **Config**.

Local Web UI:

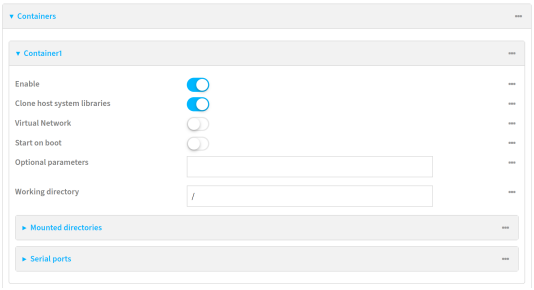
a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System** > **Containers**.
4. For **Add Container**, type the name of the container and click ♑

The Container configuration window is displayed.



New containers are enabled by default. To disable, toggle off **Enable**.

5. **Clone host system libraries** is enabled by default. This allows the container to use the device's system libraries.
6. Enable **Virtual Network** if the container should have network access:
   a. Select a **Network Bridge Device** that will provide access to the container.
   b. (Optional) Enter a static **IP Address** and netmask for the container. This must be a valid IP address for the bridge, or, if left blank, a DHCP server can assign the container an IP address.
   c. (Optional) For **Gateway**, type the IP address of the network gateway.
7. Enable **Start on boot** to configure the container to start when the system boots.
   a. For **Restart timeout**, set the amount of time to wait before restarting the container, if the container ever stops. The default timeout of **0s** means that if the container stops, it will not be restarted.

      Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

      For example, to set **Restart timeout** to ten minutes, enter **10m** or **600s**.
8. (Optional) Type any **Optional parameters** for the container. Parameters are in the format accepted by the lxc utility.

9. (Optional) Type a **Working directory** to configure an initial working directory for the container. The directory is an absolute path within the container and must begin with "/". The default is **/**.
10. (Optional) Click to expand **Mounted directories** to configure system directories that will be mounted inside the container. Any mounted directories need to be accessible to a non-privileged user.
    a. For **Add Directory**, click .
    b. For **Directory**, type the pathname of the directory to be mounted. The leading slash should be removed, so for example to mount the /opt directory, type **opt**.
11. (Optional) Click to expand **Serial ports** to assign serial ports that the container will have access to.
    a. For **Add Port**, click .
    b. For **Port**, select the serial port.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new container:

```
(config)> add system container name
(config system container name)>
```

   where *name* is the

   New access points are enabled by default.
4. New containers are enabled by default. To disable:

```
(config system container name)> enable false
(config system container name)>
```

5. By default, the container will use the device's system libraries. To disable:

```
(config system container name)> dal false
(config system container name)>
```

6. If the device will use virtual networking:
   a. Enable virtual networking:

```
(config system container name)> network true
(config system container name)>
```

b. Set the network bridge device that will be used to provide network access:

i. Use the **?** to determine the available bridges:

```
(config system container name)> bridge ?

Network Bridge Device: Containers require a bridge to access the network. Choose
which bridge to connect the container to.
Format:
  lan1
Current value:

(config system container name)>
```

ii. Set the bridge:

```
(config system container name)> bridge lan1
(config system container name)>
```

c. (Optional) Set the IP address and netmask for the container:

```
(config system container name)> address IP_address/netmask
(config system container name)>
```

d. (Optional) Set the IP address of the network gateway:

```
(config system container name)> gateway IP_address
(config system container name)>
```

7. To configure the container to start when the device boots:

```
(config system container name)> start_on_boot true
(config system container name)>
```

a. Set the amount of time to wait before restarting the container, if the container ever stops:

```
(config system container name)> restart_timeout value
(config system container name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **restart_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config system container name)> restart_timeout 600s
(config system container name)>
```

The default timeout of **0s** means that if the container stops, it will not be restarted.

8. Type any optional parameters for the container:

```
(config system container name)> args parameters
(config system container name)>
```

Parameters are in the format accepted by the lxc utility.

9. (Optional) Set an initial working directory for the container.

```
(config system container name)> workdir /value
(config system container name)>
```

   The directory is an absolute path within the container and must begin with "/". The default is **/**.

10. (Optional) Set any system directories that should be mounted inside the container. Any mounted directories need to be accessible to a non-privileged user.
    a. Add a system directory to be mounted:

```
(config system container name)> system_dirs directory
(config system container name)>
```

       where *directory* is the pathname of the directory to be mounted. The leading slash should be removed, so for example to mount the /opt directory, type **opt**.
    b. Repeat for additional directories.
11. For **Add Directory**, click .
    a. For **Directory**, type the pathname of the directory to be mounted. The leading slash should be removed, so for example to mount the /opt directory, type **opt**.
12. (Optional) Assign serial ports that the container will have access to:
    a. Determine available serial ports:

```
(config system container name)> ... serial

Serial

 Additional Configuration
 ------------------------------------------------------------------------------
port1              Port 1
...

(config system container name)>
```

    b. Add the port:

```
(config system container name)> add ports end port1
(config system container name)>
```

13. Save the configuration and apply the change.

```
(config network wireless client new_client)> save
Configuration saved.
>
```

14. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Starting and stopping the container

Container commands are not available from the Admin CLI. See Authentication groups for information about configuring authentication groups that include shell access.

Note Container support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

Starting the container

There are two methods to start containers:

- Non-persistent: Changes made to the container file system will be lost when the container is stopped.
- Persistent: Changes made to the container file system when not be lost when the container is stopped.

Starting a container in non-persistent mode

To start the container in non-persistent mode:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, type:

   ```
   # lxc container_name
   lxc #
   ```

   where *container_name* is the name of the container as configured on the device. For example:

   ```
   # lxc test_lxc
   lxc #
   ```

This will start the container by using **/bin/sh -l,** which runs the shell and loads the shell profile. The default shell profile includes an **lxc #** prompt.

Starting a container in persistent mode

To start the container in persistent mode, include the **-p** option at the command line. For example:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, type:

   ```
   # lxc test_lxc -p
   lxc #
   ```

This will start the container by using **/bin/sh -l,** which runs the shell and loads the shell profile. The default shell profile includes an **lxc #** prompt.

Starting a container by including an executable

You can supply an executable to run when you start the container, along with any parameters. If you don't supply a parameter, the default behavior is to run the executable by using **/bin/sh -l,** which runs the shell and loads the shell profile. This is useful when you use the **Clone DAL** option when uploading the container, which includes the device's system libraries. In this case, the command without any additional parameters will use the device's shell. See Upload a new LXC container for more information.

Stopping the container

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the lxc shell prompt, type:

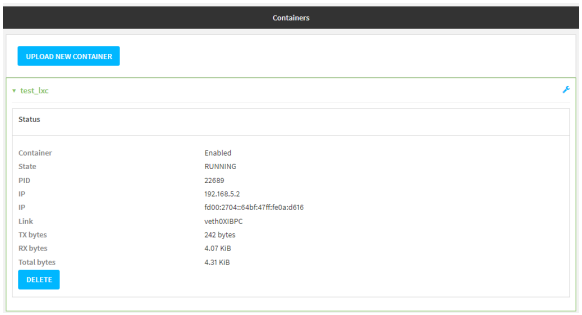
```
lxc # exit
#
```

View the status of containers

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. From the main menu, click **Status**. Under **Services**, click **Containers**.

The **Containers** status page displays.



Command line

Show status of all containers

Use the show containers command with no additional arguments to show the status of all containers on the system:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

```
> show containers

 Container  Configured  Enabled  State
 ---------  ----------  -------  -----------------
 mytest1    True        enabled  STOPPED
 test_lxc   True        enabled  RUNNING PID 19327
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show status of a specific container

Use the show containers container *name* command to show the status of the specified container:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

```
> show containers container test_lxc

 Container  Configured  Enabled  State
 ---------  ----------  -------  -----------------
 test_lxc   True        enabled  RUNNING PID 19327

>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Schedule a script to run in the container

This simple example will:

1. Start the container in non-persistent mode.
2. Execute a ping command every ten seconds from inside the container.

Web

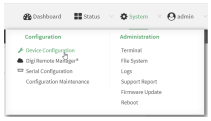
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

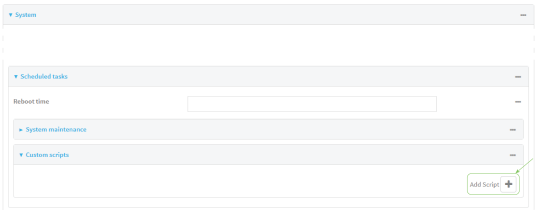
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

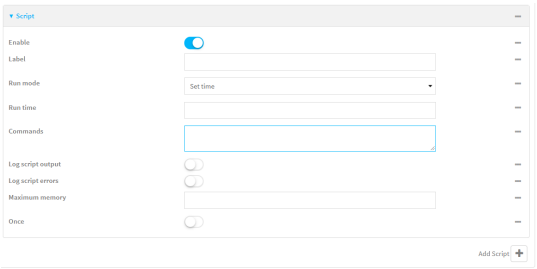
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **System** > **Scheduled tasks** > **Custom scripts**.
4. For **Add Script**, click ♈.



The script configuration window is displayed.



5. (Optional) For **Label**, type **container_script**.
6. For **Run mode**, select **Interval**.
7. For **Interval**, type **10s**.
8. For **Commands**, type the following:

```
lxc container_name /bin/ping -c 1 IP_address
```

For example:

```
lxc test_lxc /bin/ping -c 1 192.168.1.146
```

9. Click to disable **Sandbox**. Sandbox restrictions are not necessary when a container is used.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a script:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

4. Provide a label for the script, for example:

```
(config system schedule script 0)> label test_lxc
(config system schedule script 0)>
```

5. Set the mode to interval:

```
(config system schedule script 0)> when interval
(config system schedule script 0)>
```

6. Set the interval to ten seconds:

```
(config system schedule script 0)> on_interval 10s
(config system schedule script 0)>
```

7. Set the commands that will execute the script:

```
(config system schedule script 0)> commands "lxc script_name /bin/ping -c 1 IP_address"
(config system schedule script 0)>
```

   For example:

```
(config system schedule script 0)> commands "lxc test_lxc /bin/ping -c 1 192.168.1.146"
(config system schedule script 0)>
```

8. Disable the **sandbox**. Sandbox restrictions are not necessary when a container is used.

```
(config system schedule script 0)> sandbox false
(config system schedule script 0)>
```

9. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Create a custom container

This example creates a simple custom container that contains a python script in the /etc directory.

In this example, we will use a simple container file named test_lxc.tgz. You can download test_lxc.tgz from the Digi website.

At the command line of a Linux host, we will unpack the file, add a simple python script, and create a new container file that includes the python script.

Create the custom container file

1. At the command line of a Linux host, unpack the test_lxc.tgz file:

```
$ tar -xfv test_lxc.tgz
rootfs/
rootfs/usr/
rootfs/etc/
rootfs/etc/group
rootfs/etc/profile
rootfs/etc/passwd
rootfs/tmp/
$
```

2. Change to the rootfs/etc directory:

```
$ cd rootfs/etc
$
```

3. Create a file named test.py with the following contents:

```
print("Hello world.\n")
```

4. Change directories to leave the container file structure:

```
$ cd ../..
```

5. Change user and group permissions on all files in the container file structure:

```
$ sudo chown -R 165536 rootfs
$ sudo chgrp -R 165536 rootfs
```

6. Tar and zip the directory structure to create a new container file:

```
$ sudo tar -czvf python_lxc.tgz rootfs
```

If using macOS, include the --disable-copyfile option with this command:

```
$ sudo tar --disable-copyfile -czvf python_lxc.tgz rootfs
```

Test the custom container file

1. Add the new container to your IX10 device:

   Log into the IX10 WebUI as a user with full Admin access rights.

   a. From the main menu, click **Status**. Under **Services**, click **Containers**.
   b. Click **Upload New Container**.
   c. From your local file system, select the container file.

      You can download a simple example container file, test_lxc.tgz, from the Digi website.
   d. **Create Configuration** is selected by default. This will create a configuration on the device for the container when it is installed. If deselected, you will need to create the configuration manually.
   e. Click **Apply**.
2. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions** > **Open Console**. Alternatively, log into the IX10 local command line as a user with shell access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
3. At the shell prompt, type:

```
# lxc python_lxc
lxc #
```

4. Execute the python command:

```
lxc # python /etc/test.py
Hello world.
lxc #
```

System administration

This chapter contains the following topics:

Review device status 811
Configure system information 812
Update system firmware 814
Upgrade cellular modem firmware 820
Reboot your IX10 device 824
Erase device configuration and reset to factory defaults 826
Locate the device by using the Find Me feature 832
Configure a power profile 833
Enable FIPS mode 836
Configuration files 838
Schedule system maintenance tasks 843
Disable device encryption 848
Configure the speed of your Ethernet port 851
Watchdog service 853
Configure the Watchdog service 853
View Watchdog metrics 856

Review device status

You can review the system of your device from either the **Status** page of the Web interface, or from the command line:

Web

To display system information:

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.

   A secondary menu appears, along with a status panel.
2. On the secondary menu, click to display the details panel for the status you want to view.

Command line

To display system information, use the show system command.

- Show basic system information:
  1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
  2. Enter **show system** at the prompt:

```
> show system

Model              : Digi IX10
Serial Number      : IX10xxxxxxxxyyyyxx
SKU                : IX10
Hostname           : IX10
MAC Address        : DF:DD:E2:AE:21:18

Hardware Version   : 50001947-01 1P
Firmware Version   : 25.2
Alt. Firmware Version  : 25.2
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version : 19.7.23.0-15f936e0ed

Current Time       : Thu, Jan 11, 2024 12:10:00 +0000
CPU                : 1.4%
Uptime             : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
Temperature        : 40C
Location           :
Contact            :
```

```
>
```

- Show more detailed system information:
  1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
  2. Enter **show system verbose** at the prompt:

```
> show system verbose

Model              : Digi IX10
Serial Number      : IX10xxxxxxxyyyyxx
SKU                : IX10
Hostname           : IX10
MAC Address        : DF:DD:E2:AE:21:18

Hardware Version   : 50001947-01 1P
Firmware Version   : 25.2
Alt. Firmware Version   : 25.2
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version  : 19.7.23.0-15f936e0ed
Schema Version     : 715

Timezone           : UTC
Current Time       : Thu, Jan 11, 2024 12:10:00 +0000
CPU                : 1.4%
Uptime             : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
Load Average       : 0.01, 0.03, 0.02
RAM Usage          : 119.554MB/1878.984MB(6%)
Temperature        : 40C
Location           :
Contact            :
Disk
----
Disk /etc/config Usage   : 18.421MB/4546.371MB(0%)
Disk /var/log_mnt Usage  : 0.104MB/14.868MB(1%)
Disk /opt Usage    : 215.739MB/458.328MB(50%)
Disk /tmp Usage    : 0.003MB/120.0MB(0%)
Disk /var Usage    : 0.816MB/32.0MB(3%)

>
```

Configure system information

You can configure information related to your IX10 device, such as providing a name and location for the device.

Configuration items

- A name for the device.
- The name of a contact for the device.
- The location of the device.
- A description of the device.
- A banner that will be displayed when users access terminal services on the device.

To enter system information:

Web

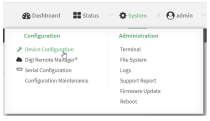
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **System**.
4. For **Name**, type a name for the device. This name will appear in log messages and at the command prompt.
5. For **Contact**, type the name of a contact for the device.
6. For **Location**, type the location of the device.
7. For **Banner**, type a banner message that will be displayed when users log into terminal services on the device.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set a name for the device. This name will appear in log messages and at the command prompt.

```
(config)> system name 192.168.3.1
192.168.3.1(config)>
```

4. Set the contact for the device:

```
192.168.3.1(config)> system contact "Jane User"
192.168.3.1(config)>
```

5. Set the location for the device:

```
192.168.3.1(config)> system location "9350 Excelsior Blvd., Suite 700, Hopkins, MN"
192.168.3.1(config)>
```

6. Set the banner for the device. This is displayed when users access terminal services on the device.

```
192.168.3.1(config)> system banner "Welcome to the Digi IX10."
192.168.3.1(config)>
```

7. Save the configuration and apply the change.

```
192.168.3.1(config)> save
Configuration saved.
192.168.3.1>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Update system firmware

The IX10 operating system firmware images consist of a single file with the following naming convention:

***platform-version*.bin**

For example, **IX10-25.2.54.xxx**

Manage firmware updates using Digi Remote Manager

If you have a network of many devices, you can use Digi Remote Manager **Profiles** to manage firmware updates. Profiles ensure all your devices are running the correct firmware version and that all newly installed devices are updated to that same version. For more information, see the **Profiles** section of the *Digi Remote Manager User Guide*.

Python and DAL OS firmware updates

Make sure to check the Python version you are using and that it is compatible with the DAL OS firmware version to which you want to upgrade. You may need to update any Python scripts you have so they are compatible with the Python running on the DAL OS firmware version you choose. See Python versions and corresponding DAL OS firmware versions.

Certificate management for firmware images

The system firmware files are signed to ensure that only Digi-approved firmware load onto the device. The IX10 device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

Downgrading

Downgrading to an earlier release of the firmware may result in the device configuration being erased.

Downgrading from firmware version 22.2.9.x

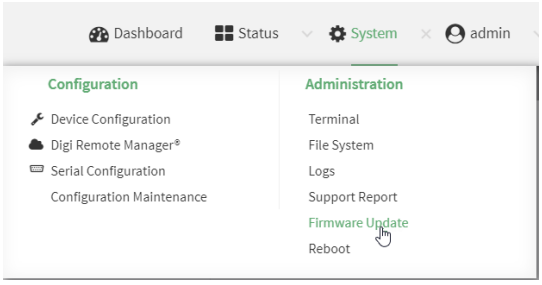
Beginning with firmware version 22.2.9.x, the IX10 device uses certificate-based communication for enhanced security when connecting to Digi Remote Manager. If you downgrade your firmware from version 22.2.9.x to version 21.11.x or previous, your device will no longer be able to communicate with Remote Manager.

To remedy this issue, select the device in Remote Manager and select **Actions** > **Reset Device Certificate**.

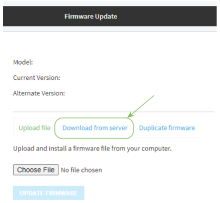
Update firmware over the air (OTA) from the Digi firmware server

Web

1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Download from server**.



4. For **Version:**, select the appropriate version of the device firmware.
5. Click **Update Firmware**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. >Use the **system firmware ota check** command to determine if new modem firmware is available on the Digi firmware repository.

```
> system firmware ota check
Current firmware version is 23.9.74.0
Checking for latest IX10 firmware...
Newest firmware version available to download is '25.2'
Device firmware update from '23.9.74.0' to '25.2' is needed
>
```

3. Use the **modem firmware ota list** command to list available firmware on the Digi firmware repository.

```
> system firmware ota list
23.9.74.0
25.2
>
```

4. Perform an OTA firmware update:
   - To perform an OTA firmware update by using the most recent available firmware from the Digi firmware repository:
     a. Update the firmware:

```
> system firmware ota update
Downloading firmware version '25.2'...
Downloaded firmware /tmp/cli_firmware.bin remaining
Applying firmware version '25.2'...
41388K
netflash: got "/tmp/cli_firmware.bin", length=42381373
netflash: authentication successful
netflash: vendor and product names are verified.
netflash: programming FLASH device /dev/flash/image1
41408K 100%
Firmware update completed, reboot device
>
```

     b. Reboot the device:

```
> reboot
>
```

- To perform an OTA firmware update by using a specific version from the Digi firmware repository, use the **version** parameter to identify the appropriate firmware version as determined by using **system firmware ota list** command. For example:
  a. Update the firmware:

```
> system firmware ota update version 25.2
Downloading firmware version '25.2'...
Downloaded firmware /tmp/cli_firmware.bin remaining
Applying firmware version '25.2'...
41388K
netflash: got "/tmp/cli_firmware.bin", length=42381373
netflash: authentication successful
netflash: vendor and product names are verified.
netflash: programming FLASH device /dev/flash/image1
41408K 100%
Firmware update completed, reboot device
>
```

  b. Reboot the device:

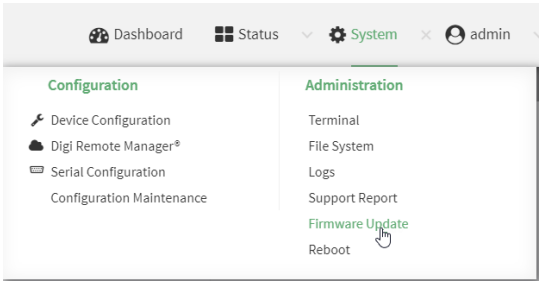
```
> reboot
>
```

Update firmware from a local file

Web

1. Download the IX10 operating system firmware from the Digi Support FTP site to your local machine.

   Log into the IX10 WebUI as a user with full Admin access rights.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Choose file**.
4. Browse to the location of the firmware on your local file system and select the file.
5. Click **Update Firmware**.

Command line

1. Download the IX10 operating system firmware from the Digi Support FTP site to your local machine.

2. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

3. Load the firmware image onto the device. We recommend using the /tmp directory.

   ```
   > scp host hostname-or-ip user username remote remote-path local local-path to local
   ```

   where:

   - *hostname-or-ip* is the hostname or IP address of the remote host.
   - *username* is the name of the user on the remote host.
   - *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
   - *local-path* is the location on the IX10 device where the copied file will be placed.

   For example:

   ```
   > scp host 192.168.4.1 user admin remote /home/admin/bin/IX10-25.2.bin local /tmp/ to local
   admin@192.168.4.1's password: adminpwd
   IX10-25.2.bin              100%   36MB   11.1MB/s      00:03
   >
   ```

4. Verify that the firmware file has been successfully uploaded to the device:

   ```
   > ls /tmp
   -rw-r--r--   1 root    root     37511229 May 16 20:10 IX10-25.2.bin
   -rw-r--r--   1 root    root         2580 May 16 16:44 blank.json
   ...
   >
   ```

5. Update the firmware by entering the system firmware update command, specifying the path and file name to the firmware file:

   ```
   > system firmware update file /tmp/IX10-25.2.bin
   36632K
   netflash: got "/tmp/IX10-25.2.bin", length=37511229
   netflash: authentication successful
   netflash: programming FLASH device /dev/flash/image
   36633K 100%
   Firmware update completed, reboot device
   >
   ```

6. Reboot the device to run the new firmware image using the reboot command.

   ```
   > reboot
   Rebooting system
   >
   ```

7. Once the device has rebooted, log into the IX10's command line as a user with Admin access and verify the running firmware version by entering the show system command.

```
> show system

Hostname          : IX10
FW Version        : 25.2
MAC             : 0040FF800120
Model           : Digi IX10
Current Time        : Thu, Jan 11, 2024 12:10:00 +0000
Uptime          : 42 seconds (42s)

>
```

Dual boot behavior

By default, the IX10 device stores two copies of firmware in two flash memory banks:

- The current firmware version that is used to boot the device.
- A copy of the firmware that was in use prior to your most recent firmware update.

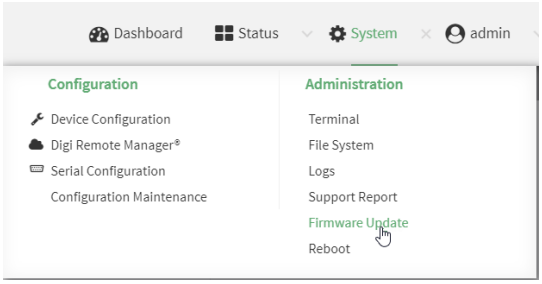
When the device reboots, it will attempt to use the current firmware version. If the current firmware version fails to load after three consecutive attempts, it is marked as invalid and the device will use the previous firmware version stored in the alternate memory bank.

If the device consistently loses power during the boot process, this may result in the current firmware being marked as invalid and the device downgrading to a previous version of the firmware. As a result of this behavior, you can use the following procedure to guarantee that the same firmware is stored in both memory banks:

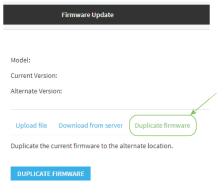
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



2. Click **Duplicate firmware**.



3. Click **Duplicate Firmware**.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Duplicate the firmware:

```
> system duplicate-firmware
>
```

Upgrade cellular modem firmware

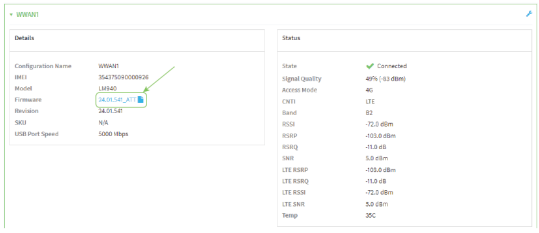
You can upgrade modem firmware by downloading firmware from the Digi firmware repository, or by uploading firmware from your local storage onto the device. You can also schedule modem firmware updates. See Schedule system maintenance tasks for details.

Note Before attempting to update cellular module firmware, you should either ensure that there is a SIM card in the module, or disable **SIM failover**. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.

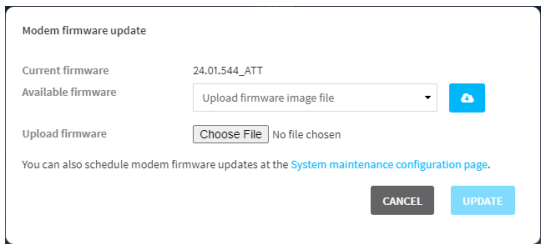
Web

1. (Optional) Download the appropriate modem firmware from the Digi repository to your local machine.

   Log into the IX10 WebUI as a user with full Admin access rights.
2. From the main menu, click **Status** > **Modems**.
3. Click the modem firmware version.



The **Modem firmware update** window opens.



4. To update using firmware from the Digi firmware repository:
   a. Click to view available versions.
   b. For Available firmware, select the firmware.
5. To update using firmware from your local file system:
   a. Click **Choose File**.
   b. Select the firmware.
6. To schedule firmware updates, click **System maintenance configuration page**. See Schedule system maintenance tasks for details.
7. Click **Update**.

Command line

Update modem firmware over the air (OTA)

You can update your modem firmware by querying the Digi firmware repository to determine if there is new firmware available for your modem and performing an OTA modem firmware update:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **modem firmware ota check** command to determine if new modem firmware is available on the Digi firmware repository.

```
> modem firmware ota check

Checking for latest ATT firmware ...
Retrieving modem firmware list ...
Newest firmware version available to download is '24.01.5x4_ATT'
Modem firmware update from '24.01.544_ATT' to '24.01.5x4_ATT' is needed
24.01.5x4_ATT
24.01.544_ATT

>
```

3. Use the **modem firmware ota list** command to list available firmware on the Digi firmware repository.

```
> modem firmware ota list

Retrieving modem firmware list ...
25.20.664_CUST_044_3
25.20.666_CUST_067_1
25.20.663_CUST_040

>
```

4. Perform an OTA firmware update:
   - A firmware bundle includes images for each carrier supported by a specific modem. To perform an OTA update by choosing a firmware bundle based on the type of modem in your device:

     ```
     modem firmware bundle ota [check|list|download|update]
     ```

   - To perform an OTA firmware update by using the most recent available modem firmware from the Digi firmware repository, type:

     ```
     > modem firmware ota update

     Checking for latest Generic firmware ...
     Retrieving modem firmware list ...
     Newest firmware version available to download is '25.20.666_CUST_067_1'
     Retrieving download location for modem firmware '25.20.666_CUST_067_1' ...

     >
     ```

   - To perform an OTA firmware update by using a specific version from the Digi firmware repository, use the **version** parameter to identify the appropriate firmware version as determined by using **modem firmware ota list** command. For example::

     ```
     > modem firmware ota update version 24.01.5x4_ATT

     Retrieving download location for modem firmware '24.01.5x4_ATT' ...
     Downloading modem firmware '24.01.5x4_ATT' to '/opt/LE910C4_NF/Custom_Firmware' ...
     Modem firmware '24.01.5x4_ATT' downloaded
     Updating modem firmware ...
     Programming modem firmware ...

     Found modem ...
     Validate modem firmware ...
     Getting ready for update ...
     Stopping services ...
     Running update pass 1 of 3 ...
     Restarting services ...
     ----------------------------
     Successfully updated firmware
     Modem firmware update complete

     >
     ```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Update modem firmware by using a local firmware file

You can update your modem firmware by uploading a modem firmware file to your IX10 device. Firmware should be uploaded to /opt/*MODEM_MODEL*/Custom_Firmware, for example, /opt/LM940/Custom_Firmware.

Modem firmware can be downloaded from Digi here. Follow instructions on this page to determine the cellular module used by your device. After downloading, use tar or a similar unzipping tool to extract the firmware prior to uploading to the device. Note that the firmware file may not have a tar.gz extension, but it is a tar file and can be unzipped with tar or a similar tool. See Use the scp command for information about uploading files to the IX10 device.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the **modem firmware check** command to determine if new modem firmware is available on local device.

```
> modem firmware check

Checking for latest ATT firmware in flash ...
Newest firmware version available in flash is '05.05.58.00_ATT_005.026_000'
Modem firmware up to date
05.05.58.00_ATT_005.026_000

> modem firmware check
```

3. Use the **modem firmware list** command to list available firmware on the IX10 device.

```
>  modem firmware list

ATT, 24.01.544_ATT, current
Generic, 24.01.514_Generic, image
Verizon, 24.01.524_Verizon, image
ATT, 24.01.544_ATT, image
Sprint, 24.01.531-B003_Sprint, image

>
```

4. To perform a firmware update by using a local file, use the **version** parameter to identify the appropriate firmware version as determined using the **modem firmware check** or **modem firmware list** command. For example, to update a Telit modem to firmware version 24.01.5x4_ATT:

```
>  modem firmware update version 24.01.5x4_ATT name [modem_name]

Updating modem firmware ...

----------------------------
Successfully updated firmware
Modem firmware update complete

>
```

   Or, to update a Sierra modem firmware using the firmware files loaded into the /opt/MODEM_MODEL/Custom_Firmware directory:

```
> modem firmware update version /opt/MODEM_MODEL/Custom_Firmware name [modem_name]
Updating modem firmware...

------------------------------
Successfully updated firmware
Modem firmware update complete

>
```

Where **[modem_name]** is the name of the modem you would like to update (e.g. modem, wwan1, wwan2). If you don't know the modem name, you can use tab-completion in the above command, or run the **show modem** CLI command to see a list of available modems in the device.

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Reboot your IX10 device

You can reboot the IX10 device immediately or schedule a reboot for a specific time every day.

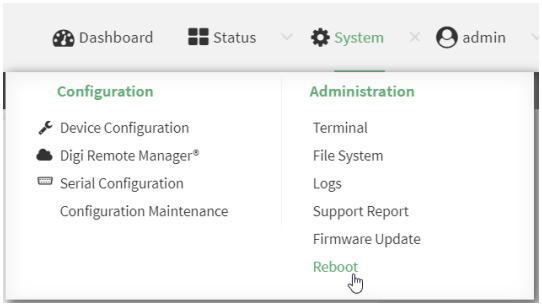
Note You may want to save your configuration settings to a file before rebooting. See Save configuration to a file.

Reboot your device immediately

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. From the main menu, click **System**.
2. Click **Reboot**.



3. Click **Reboot** to confirm that you want to reboot the device.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the prompt, type:

```
> reboot
```

Schedule reboots of your device

Web

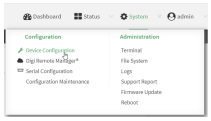
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Select **System** > **Scheduled tasks**.
4. For **Reboot time**, enter the time of the day that the device should reboot, using the format *HH*:*MM*. The device will reboot at this time every day.

   If **Reboot time** is set, but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See System time synchronization for information about configuring NTP servers. If **Reboot window** is set, the reboot will occur during a random time within the reboot window.
5. For **Reboot window**, enter the maximum random delay that will be added to **Reboot Time**.

   Allowed values are any number of hours, minutes, or seconds, and take the format ***number*** {**h|m|s**}.

   For example, to set **parameter name** to ten minutes, enter **10m** or **600s**.
   The default is **10m**, and the maximum allowed time is **24h**.
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```

3. Set the reboot time:

   ```
   (config>> system schedule reboot_time time
   (config)>
   ```

   where *time* is the time of the day that the device should reboot, using the format *HH:MM*. For example, the set the device to reboot at two in the morning every day:

   ```
   (config>> system schedule reboot_time 02:00
   (config)>
   ```

   If **reboot_time** is set, but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See System time synchronization for information about configuring NTP servers. If **reboot_window** is set, the reboot will occur during a random time within the reboot window.

4. Set the maximum random delay that will be added to **reboot_time**:

   ```
   (config>> system schedule reboot_window value
   (config)>
   ```

   where *value* is any number of hours, minutes, or seconds, and takes the format ***number*** {**h|m|s**}.

   For example, to set **reboot_window** to ten minutes, enter either **10m** or **600s**:

   ```
   (config)> system schedule reboot_window 600s
   (config)>
   ```

5. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Erase device configuration and reset to factory defaults

You can erase the device configuration in the WebUI, at the command line, or by using the **ERASE** button on the device. Erasing the device configuration performs the following actions:

- Clears all configuration settings. When the device restarts, it uses the factory default configuration.
- Deletes all user files including Python scripts.
- Clears event and system log files.

Additionally, if the **ERASE** button is used to erase the configuration, pressing the **ERASE** button a second time immediately after the device has rebooted:

- Erases all automatically generated certificates and keys.
- With firmware release 22.2.9.x and newer, erases the client-side certificate used for communication with Digi Remote Manager.

  If you are using Digi Remote Manager with firmware release 22.2.9.x and newer, by default the device uses a client-side certificate for communication with Remote Manager. If the client-side certificate is erased, you must use the Remote Manager interface to reset the certificate.
- If your device uses a custom factory default, the custom factory default will be removed and the device will reboot using standard factory default settings.

You can also reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command.

Reset the device by using the ERASE button

1. Locate the **ERASE** button on your device.

2. Press the **ERASE** button perform a device reset. The **ERASE** button has the following modes:
   - **Configuration reset**:
     - Press and release the **ERASE** button.
     - The device reboots automatically and resets to factory defaults. This does not remove any automatically generated certificates and keys.
   - **Full device reset**:
     - After the device reboots from the first button press, immediately press and release the **ERASE** button again.
     - The device reboots again and resets to factory defaults, as well as also removing generated certificates and keys.
   - **Firmware reversion**: Press and hold the **ERASE** button and then power on the device to boot the version of firmware that was used prior to the current version.

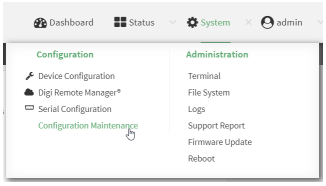
3. After resetting the device:
   a. Connect to the IX10 by using the serial port or by using an Ethernet cable to connect the IX10 **ETH** port to your PC.
   b. Log into the IX10:

      User name: Use the default user name: **admin**.

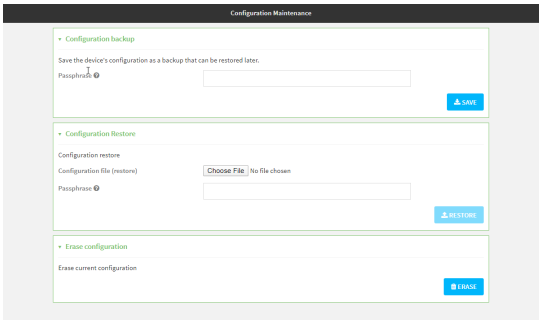
      Password: Use the unique password printed on the bottom label of the device (or the printed label included in the package).
   c. (Optional) Reset the default password for the admin account. See Change the default password for the admin user for further information.

Web

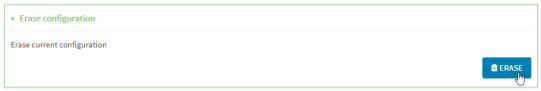
1. Log into the IX10 WebUI as a user with full Admin access rights.
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



3. In the **Erase configuration** section, click **ERASE**.



4. Click **CONFIRM**.
5. After resetting the device:
   a. Connect to the IX10 by using the serial port or by using an Ethernet cable to connect the IX10 **ETH** port to your PC.
   b. Log into the IX10:

      User name: Use the default user name: **admin**.

      Password: Use the unique password printed on the bottom label of the device (or the printed label included in the package).

c. (Optional) Reset the default password for the admin account. See Change the default password for the admin user for further information.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

```
> system factory-erase
```

   A confirmation message appears.
3. Type `yes` to confirm that you want all configurations deleted, the factory configuration reset, and the device rebooted.
4. After resetting the device:
   a. Connect to the IX10 by using the serial port or by using an Ethernet cable to connect the IX10 **ETH** port to your PC.
   b. Log into the IX10:

      User name: Use the default user name: **admin**.

      Password: Use the unique password printed on the bottom label of the device (or the printed label included in the package).
   c. (Optional) Reset the default password for the admin account. See Change the default password for the admin user for further information.

Reset the device with the revert command

You can reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, enter **revert**:

```
(config)> revert
(config)>
```

4. Set the password for the admin user prior to saving the changes:

```
(config)> auth user admin password pwd
(config)>
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Custom factory default settings

You can configure your IX10 device to use a custom factory default configuration file. This way, when you erase the device's configuration, the device will reset to your custom configuration rather than to the original factory defaults.

Required configuration items

- Custom factory default configuration (*bin*) file.

Configure the IX10 device to use custom factory default settings

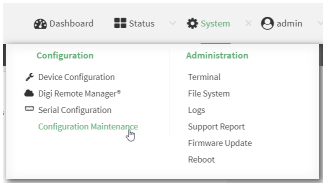
Web

Log into the IX10 WebUI as a user with full Admin access rights.

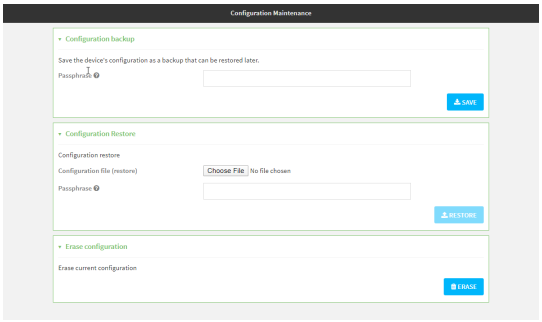
1. Configure your IX10 device to match the desired custom factory default configuration.

   For example, you may want to configure the device to use a custom APN or a particular network configuration, so that when you reset the device to factory defaults, it will automatically have your required network configuration.

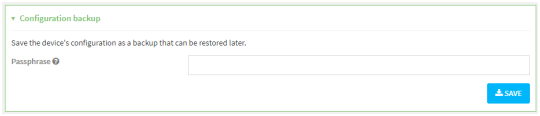
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



3. In the **Configuration backup** section, click **SAVE**.

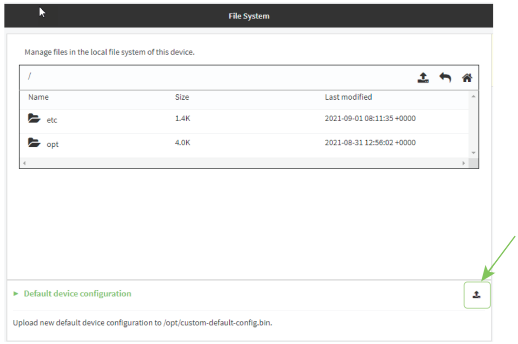


   Do not set a **Passphrase** for the configuration backup. The file will be downloaded using your browser's standard download process.

4. After the configuration backup file has been downloaded, rename the file to:

   custom-default-config.bin

5. Upload the file to the device:
   a. From the main menu, select **System** > **Filesystem**.
   b. Under **Default device configuration**, click ❽.



   c. Select the file from your local file system.

6. Reboot the device.

Note After configuring a device to use custom factory default settings, wait five minutes after restoring to defaults before:

- Powering off the device.
- Performing any additional configuration restoration activities.

If you do not wait five minutes after restoring to custom factory defaults before performing these activities, the device will clear the custom factory defaults and reboot to standard factory defaults.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. The table below lists the available commands.

Commands	Description

system custom-default-config file *[file name]*	Set the file you specify as the custom factory default configuration file (custom-default-config.bin). The SHA file is also created. Where *filename* is the name of the file created using the *system backup* command.
system custom-default-config current	Save the current configuration as a *custom-default-config.bin* file. The SHA file is also created.
system custom-default-config remove	Remove the *custom-default-config.bin* and SHA files.

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Note After configuring a device to use custom factory default settings, wait five minutes after restoring to defaults before:

- Powering off the device.
- Performing any additional configuration restoration activities.

If you do not wait five minutes after restoring to custom factory defaults before performing these activities, the device will clear the custom factory defaults and reboot to standard factory defaults.

Clear the custom factory default settings

After configuring the device to use custom factory default settings, to clear the custom default configuration and reset the device to standard factory defaults:

1. Press the device's ERASE button.
2. Wait for the device to reboot.
3. Press the ERASE button a second time.

You must press the ERASE the second time within five minutes of the first in order to clear the custom default configuration.

Locate the device by using the Find Me feature

Use the **Find Me** feature to cause LEDs on the device to blink, which can help you to identify the specific device.

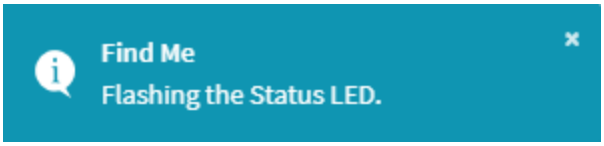
To use this feature:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

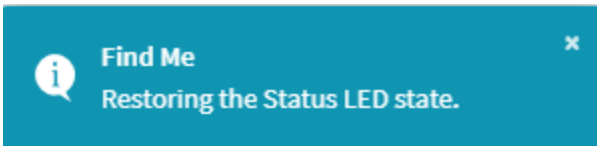
1. On the menu, click **System**. Under **Administration**, click **Find Me**.

   A notification message appears, noting that the LED is flashing on the device. Click the **x** in the message to close it.



2. On the menu, click **System** again. Ablue circle next to **Find Me** is blinking, indicating that the **Find Me** feature is active.
3. To deactivate the **Find Me** feature, click **System** and click **Find Me** again.

   A notification message appears, noting that the LED is no longer flashing on the device. Click the **x** in the message to close it.



Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To activate the **Find Me** feature, at the prompt, type the following at the command prompt:

```
> system find-me on
>
```

3. To deactivate the **Find Me** feature, type the following at the command prompt:

```
> system find-me off
>
```

4. To determine the status of the **Find Me** feature, type the following at the command prompt:

```
> system find-me status
off
>
```

Configure a power profile

A power profile is a group of settings that determine how the system will behave in terms of power consumption during standard operating mode. You can choose to preserve power, performance or to balance both. You can also disable the IX10's LEDs to save power and reduce light pollution.

To change the active power profile:

Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.

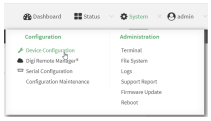
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

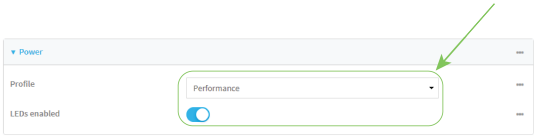
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **System** > **Power** to display the power settings.



4. The **Profile** setting displays the active power profile and allows you to change it. The available options are:
   - **Performance**: The CPU clock frequency is scaled up to work in the highest available frequency and provide a better system performance.
   - **Auto**: The CPU clock frequency is dynamically scaled up and down to provide better performance during high demanding conditions and also to save power during inactivity periods.
   - **Power save**: The CPU clock frequency is scaled down to work in the lowest available frequency and save power.
   - **Manual**: Allows you to manually set the working frequency of the CPU. When this option is selected, the setting **Custom frequency** is available to set the CPU working frequency manually:
     - 198 MHz
     - 396 MHz
     - 528 MHz
     - 792 MHz
5. Toggle off **LEDs enabled** to disable all LEDs on the device except for the Power LED, which will remain lit green, indicating that the device has power. If disabled, one or more LEDs will flash periodically to indicate that the device is still active.
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```

3. Set the profile you prefer:

   ```
   (config)> system power profile profile_name
   (config)>
   ```

   where *profile_name* is one of:

   - **auto**: The CPU clock frequency is dynamically scaled up and down to provide better performance during high demanding conditions and also to save power during inactivity periods.
   - **manual**: Allows you to manually set the working frequency of the CPU.
   - **performance**: The CPU clock frequency is scaled up to work in the highest available frequency and provide a better system performance.
   - **powersave**: The CPU clock frequency is scaled down to work in the lowest available frequency and save power.

   The default is **performance**.

4. If **profile** is set to **manual**, set the CPU working frequency:

   ```
   (config)> system power custom_freq frequency
   (config)>
   ```

   where *frequency* is one of:

   - **198000**
   - **396000**
   - **528000**
   - **792000**

   The default is **792000**.

5. Set **leds_enabled** to **false** to disable all LEDs on the device except for the Power LED, which will remain lit green, indicating that the device has power:

   ```
   (config)> system power leds_enabled false
   (config)>
   ```

   If disabled, one or more LEDs will flash periodically to indicate that the device is still active.

6. Save the configuration and apply the change.

   ```
   (config)> save
   Configuration saved.
   >
   ```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable FIPS mode

You can enable your device to be Federal Information Processing Standard (FIPS) 140-2 compliant.

With FIPs 140-2 compliance, only FIPS 140-2 cipher and MAC algorithms are available. As a result, features like stunnel, ssh, and openvpn are limited in what they can use. For example, in FIPS mode ssh will only offer and negotiate AES based ciphers.

When the FIPS setting is changed, the device will reboot automatically. Disabling FIPS after it has been enabled will cause the current configuration to be erased.

Web

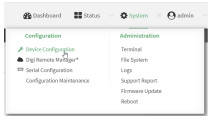
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

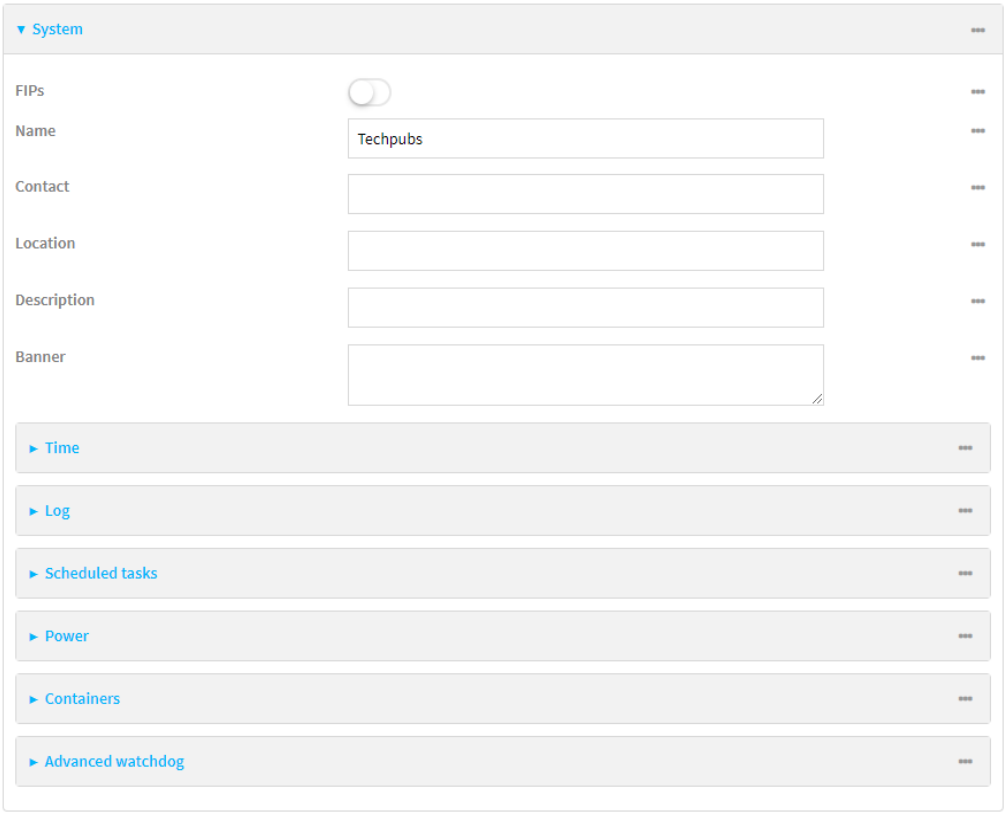
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Expand **System**.



4. Click to enable **FIPs**.
5. Click **Apply** to save the configuration and apply the change. The the device will reboot automatically.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enable FIPS:

```
(config)> system fips true
>
```

3. Save the change. The the device will reboot automatically.

```
(config)> save
>
```

Configuration files

The IX10 configuration file, /etc/config/accns.json, contains all configuration changes that have been made to the device. It does not contain the complete device configuration; it only contains changes to the default configuration. Both the default configuration and the changes contained in the accns.json file are applied when the device reboots.

Save configuration changes

When you make changes to the IX10 configuration, the changes are not automatically saved. You must explicitly save configuration changes, which also applies the changes. If you do not save configuration changes, the system discards the changes.

Web

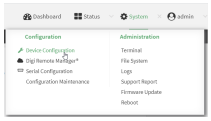
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Make any necessary configuration changes.
4. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Make any necessary configuration changes.
4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Save configuration to a file

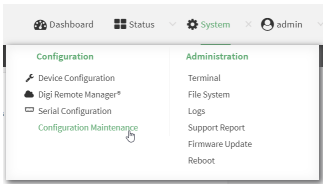
You can save your IX10 device's configuration to a file and use this file to restore the configuration, either to the same device or to similar devices.

Web

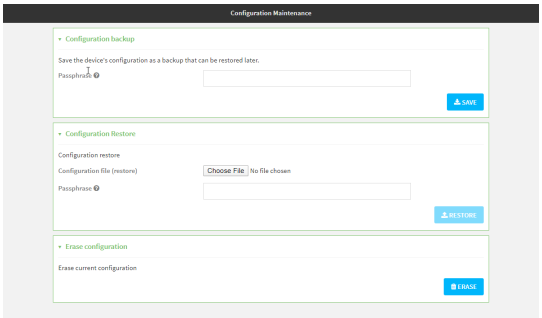
This procedure creates a binary archive file containing the device's configuration, certificates and keys, and other information.

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



2. In the **Configuration backup** section:
   a. (Optional) To encrypt the configuration using a passphrase, for **Passphrase (save/restore)**, enter the passphrase.
   b. Click **SAVE**.

The file will be downloaded using your browser's standard download process.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

   ```
   > system backup path [passphrase passphrase] type type
   ```

   where
   - *path* is the location on the IX10's filesystem where the configuration backup file should be saved.
   - *passphrase* (optional) is a passphrase used to encrypt the configuration backup.
   - *type* is the type of backup, either:
     - **archive**: Creates a binary archive file containing the device's configuration, certificates and keys, and other information.
     - **cli-config**: Creates a text file containing only the configuration changes.

   For example:

   ```
   > system backup /etc/config/scripts/ type archive
   ```
3. (Optional) Use **scp** to copy the file from your device to another host:

   ```
   > scp host hostname-or-ip user username remote remote-path local local-path to remote
   ```

   where:
   - *hostname-or-ip* is the hostname or IP address of the remote host.
   - *username* is the name of the user on the remote host.
   - *remote-path* is the location on the remote host where the file will be copied.
   - *local-path* is the path and filename on the IX10 device.

   For example:

   ```
   > scp host 192.168.4.1 user admin remote /home/admin/bin/ local /etc/config/backup-archive-0040FF800120-19.05.17-19.01.17.bin to remote
   ```

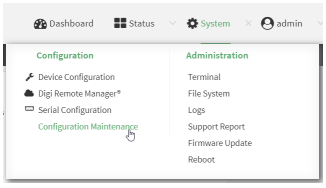
Restore the device configuration

You can restore a configuration file to your IX10 device by using a backup from the device, or a backup from a similar device.

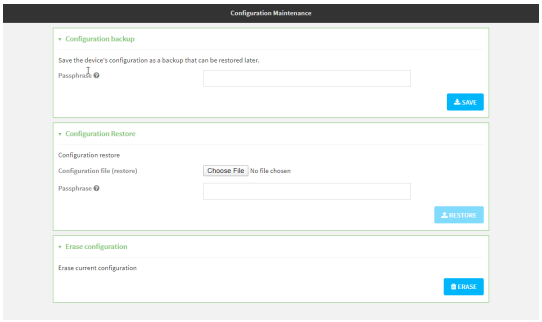
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



2. In the **Configuration Restore** section:
   a. If a passphrase was used to create the configuration backup, for **Passphrase (save/restore)**, enter the passphrase.
   b. Under **Configuration Restore**, click **Choose File**.
   c. Browse to the system firmware file location on your local computer and select the file.
   d. Click **RESTORE**.
3. Click **CONFIRM**.

   The configuration will be restored and the device will be rebooted.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. If the configuration backup is on a remote host, use **scp** to copy the file from the host to your device:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

   where:

   - *hostname-or-ip* is the hostname or IP address of the remote host.
   - *username* is the name of the user on the remote host.
   - *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
   - *local-path* is the location on the IX10 device where the copied file will be placed.

For example:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/backup-archive-0040FF800120-25.2-19.23.42.bin local /opt to local
```

3. Enter the following:

```
> system restore filepath [passphrase passphrase]
```

where

- *filepath* is the the path and filename of the configuration backup file on the IX10's filesystem (*local-path* in the previous step).
- *passphrase* (optional) is the passphrase to restore the configuration backup, if a passphrase was used when the backup was created.

For example:

```
> system restore /opt/backup-archive-0040FF800120-25.2-19.23.42.bin
```

Schedule system maintenance tasks

You can configure tasks to be run during a specified maintenance window. When the device is within its maintenance window, firmware updates and Digi Remote Manager configuration checks will be performed.

You can also schedule custom scripts to run during the maintenance window. See Configure scripts to run automatically for more information.

Required configuration items

- Events that trigger the maintenance window to begin.
- Whether all configured triggers, or only one of the triggers, must be met.
- The tasks to be performed. Options are:
  - Firmware updates.
  - Digi Remote Manager configuration check.
- Whether the device will check for updates to the device firmware.
- Whether the device will check for updates to the modem firmware.
- The frequency (daily, weekly, or monthly) that checks for firmware updates will run.

Web

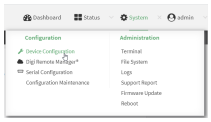
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

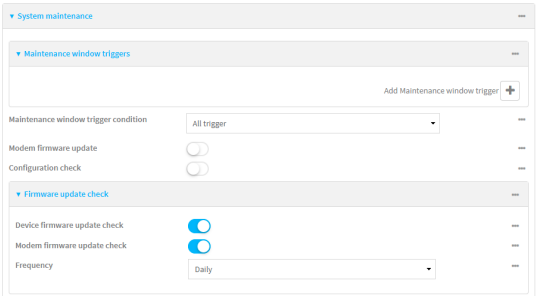
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

3. Click **System** > **Scheduled tasks** > **System maintenance**.



4. Click to expand **Maintenance window triggers**.
5. Click to add a maintenance window trigger.

6. For **Maintenance window trigger type**, select one of the following:
   - **Check if interface is up**, for **Test Interface**, select the interface.
   - **Time period for maintenance window**:
     a. Click to expand **Maintenance window**.
     b. For **Start time**, type the time of day that the maintenance window should start, using the syntax *HH*:*MM*. If **Start time** is not set, maintenance tasks are not scheduled and will not be run.

        The behavior of **Start time** varies depending on the setting of **Duration window**, which is configured in the next step.

        - If **Duration window** is set to **Immediately**, all scheduled tasks will begin at the exact time specified in **Start time**.
        - If **Duration window** is set to **24 hours**, **Start time** is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting **Duration window** to **24 hours** can potentially overstress the device and should be used with caution.
        - If **Duration window** is set to any value other than to **Immediately** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
        - If **Duration window** is set to one or more hours, the minutes field in **Start time** is ignored and the duration window will begin at the beginning of the specified hour.

     c. For **Duration window**, select the amount of time that the maintenance tasks will be run. If **Immediately** is selected, all scheduled tasks will begin at the exact time specified in **Start time**.
     d. For **Frequency**, select whether the maintenance window will be started every day, or once per week.

- If **Check if Python Out-of-Service** is set, the maintenance window will only start if the Python Out-of-Service is set. See Use Python to set the maintenance window for further information.

7. If **Central Management** is disabled, click **Device firmware update** to instruct the system to look for any updated device firmware during the maintenance window. If updated firmware is found, it will then be installed. This options is only available if **Central Management** is disabled; see Central management for more information.
8. The **Modem firmware update** option, which is only available if **Central Management** is disabled, is not used with the IX10.
9. If **Central Management** is disabled, click to enable **Modem firmware update** to instruct the system to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. Modem firmware update looks for updated firmware both on the local device and over the network, using either a WAN or cellular connection. This options is only available if **Central Management** is disabled; see Central management for more information.
10. (Optional) Configure automated checking for device and modem firmware updates:
    a. Click to expand **Firmware update check**.
    b. **Device firmware update check** is enabled by default. This enables the automated checking for device firmware updates.
    c. **Modem firmware update check** is enabled by default. This enables the automated checking for modem firmware updates.

    Note The **Modem firmware update** option is not used with theIX10. Any selection is ignored.

    d. For **Frequency**, select how often automated checking for device and modem firmware should take place. Allowed values are **Daily**, **Weekly**, and **Monthly**. The default is **Daily**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure a system maintenance trigger:
   a. Add a trigger:

```
(config)> add system schedule maintenance trigger end
(config)>
```

b. Set the type of trigger:

```
(config add system schedule maintenance trigger)> type value
(config)>
```

where *value* is one of:

- **interface_up**: If **interface_up** is set:
  i. Set the interface:

  ```
  (config add system schedule maintenance trigger)> interface value
  (config)>
  ```

  ii. i. Use the **?** to determine available interfaces:
  ii. Set the interface. For example:

  ```
  (config system schedule maintenance trigger 0)> interface
  /network/interface/eth1
  (config system schedule maintenance trigger 0)>
  ```

- **out_of_service**: The maintenance window will only start if the Python Out-of-Service is set. See Use Python to set the maintenance window for further information.
- **time**: Configure a time period for the maintenance window:
  i. Configure the time of day that the maintenance window should start, using the syntax *HH*:*MM*. If the start time is not set, maintenance tasks are not scheduled and will not be run.

  ```
  (config system schedule maintenance trigger 0)> time from HH:MM
  (config system schedule maintenance trigger 0)>
  ```

  The behavior of the start time varies depending on the setting of the duration length, which is configured in the next step.
  - If the duration length is set to **0**, all scheduled tasks will begin at the exact time specified in the start time.
  - If the duration length is set to **24 hours**, the start time is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting the duration length to **24 hours** can potentially overstress the device and should be used with caution.
  - If the duration length is set to any value other than to **0** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
  - If the duration length is set to one or more hours, the minutes field in the start time is ignored and the duration window will begin at the beginning of the specified hour.

  ii. Configure the duration length (the amount of time that the maintenance tasks will be run). If **0** is used, all scheduled tasks will begin at the start time, defined in the previous step.

```
(config system schedule maintenance trigger 0)> length num
(config system schedule maintenance trigger 0)>
```

where *num* is any whole number between **0** and **24**.

iii. Configure the frequency that the maintenance tasks should be run:

```
(config system schedule maintenance trigger 0)> frequency value
(config system schedule maintenance trigger 0)>
```

where *value* is either **daily** or **weekly**. **Daily** is the default.

4. If **Central Management** is disabled, configure the device to look for any updated device firmware during the maintenance window. If updated firmware is found, it will then be installed. The device will look for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

   This options is only available if **Central Management** is disabled; see Central management for more information.

```
(config)> system schedule maintenance device_fw_update true
(config)>
```

5. If **Central Management** is disabled, configure the device to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. The device will look for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

   This options is only available if **Central Management** is disabled; see Central management for more information.

```
(config)> system schedule maintenance modem_fw_update true
(config)>
```

6. (Optional) Configure automated checking for device and modem firmware updates:
   a. **Device firmware update check** is enabled by default. This enables to automated checking for device firmware updates. To disable:

```
(config)> system schedule maintenance firmware_update_check device false
(config)>
```

   b. **Modem firmware update check** is enabled by default. This enables to automated checking for modem firmware updates.

```
(config)> system schedule maintenance firmware_update_check modem false
(config)>
```

   c. Set how often automated checking for device and modem firmware should take place:

```
(config)> system schedule maintenance frequency value
(config)>
```

   where *value* is either **daily**, **weekly**, or **monthly**. **daily** is the default.

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

7. (Optional) Configure automated checking for device and modem firmware updates:
   a. **Device firmware update check** is enabled by default. This enables to automated checking for device firmware updates. To disable:

```
(config)> system schedule maintenance firmware_update_check device false
(config)>
```

   b. **Modem firmware update check** is enabled by default. This enables to automated checking for modem firmware updates.

```
(config)> system schedule maintenance firmware_update_check modem false
(config)>
```

   c. Set how often automated checking for device and modem firmware should take place:

```
(config)> system schedule maintenance frequency value
(config)>
```

   where *value* is either **daily**, **weekly**, or **monthly**. **daily** is the default.

8. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable device encryption

You can disable the cryptography on your IX10 device. This can be used to ship unused devices from overseas without needing export licenses from the country from which the device is being shipped.

When device encryption is disabled, the following occurs:

- The device is reset to the default configuration and rebooted.
- After the reboot:
  - Access to the device via the WebUI and SSH are disabled.
  - All internet connectivity is disabled, including WAN and WWAN. Connectivity to central management software is also disabled.

- All IP networks and addresses are disabled except for the default 192.168.210.1/24 network on the local LAN Ethernet port. DHCP server is also disabled.

  The device can only be accessed by using telnet from a local machine connecting to the 192.168.210.1/24 network.

Disabling device encryption is not available in the WebUI. It can only be performed from the Admin CLI.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Disable encryption with the following command:

```
> system disable-cryptography
>
```

3. Type **exit** to exit the Admin CLI.

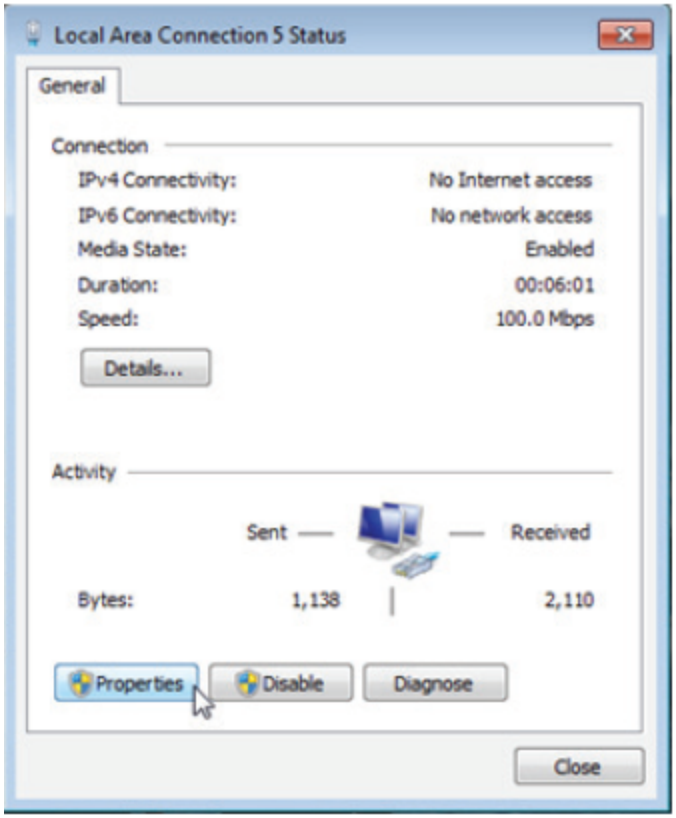
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Re-enable cryptography after it has been disabled.

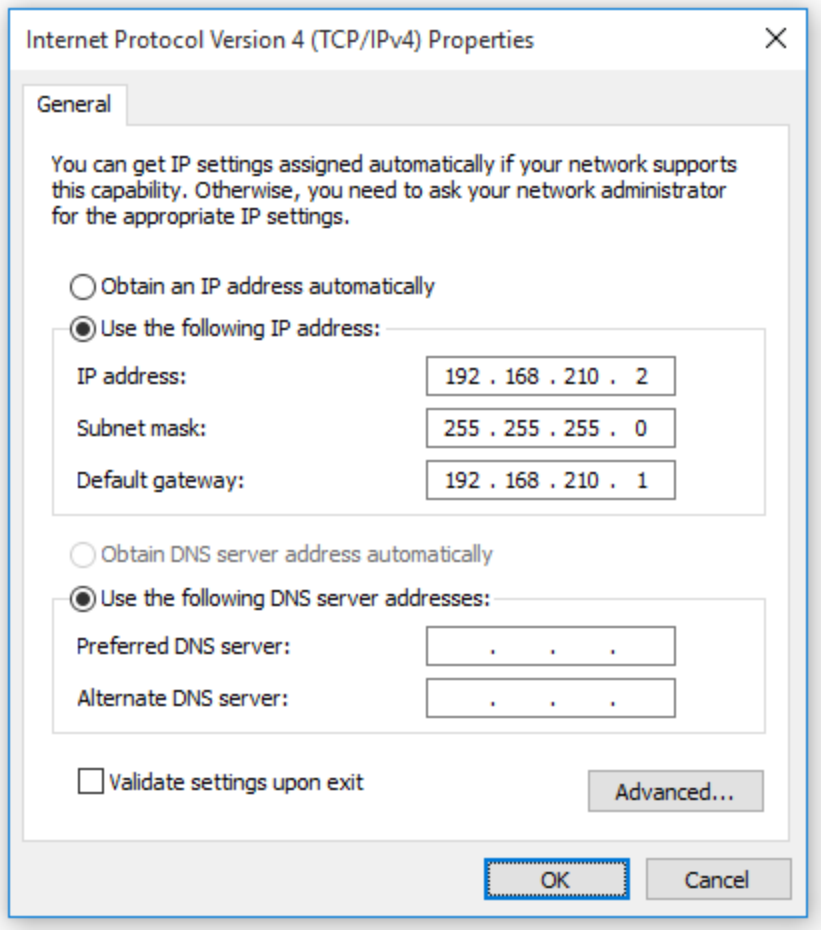
To re-enable cryptography:

1. Configure your PC network to connect to the 192.168.210 subnet. For example, on a Windows PC:

a. Select the **Properties** of the relevant network connection on the Windows PC.



b. Click the **Internet Protocol Version 4 (TCP/IPv4)** parameter.
c. Click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog appears.
d. Configure with the following details:
    - **IP address** for PC: 192.168.210.2
    - **Subnet**: 255.255.255.0
    - **Gateway**: 192.168.210.1



2. Connect the PC's Ethernet port to the Ethernet port on your IX10 device.
3. Open a telnet session and connect to the IX10 device at the IP address of 192.168.210.1.
4. Log into the device:
   - Username: **admin**
   - Password: The default unique password for your device is printed on the device label.
5. At the shell prompt, type:

```
# rm /etc/config/.nocrypt
# flatfsd -i
```

This will re-enable encryption and leave the device at its factory default setting.

Configure the speed of your Ethernet port

You can configure the speed of your IX10 device's Ethernet port.

Web

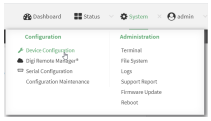
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Network** > **Device** > **ETH**.
4. For **Speed**, select the appropriate speed for the Ethernet port, or select **Auto** to automatically detect the speed. The default is **Auto**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> network device eth_port value
```

   where:

   - *eth_port* is the name of the Ethernet port (for example, **eth**)
   - *value* is one of:
     - **10**—Sets the speed to 10 Mbps.
     - **100**—Sets the speed to 100 Mbps.
     - **1000**—Sets the speed to 1 Gbps. Available only for devices with Gigabit Ethernet ports.

auto—Configures the device to automatically determine the best speed for the Ethernet port.

The default is **auto**.

4. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Watchdog service

The Watchdog service can monitor the operation of your device, test the system for problems, and automatically restart that device if it detects a fault or failure. You can also see metrics for the Watchdog service and performance results of the tests performed.

When the Watchdog service has been enabled, the service name and green check mark displays in the dashboard.

Configure the Watchdog service

To configure the Watchdog service on your IX10:

Web

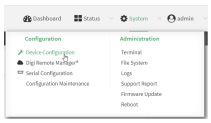
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **System** > **Advanced Watchdog**.
4. The watchdog is enabled by default. To disable, click to toggle off **Enable**.

5. For **Watchdog test interval**, type the amount of time between running system tests.

   Allowed values are any number of days, hours, minutes, or seconds, and take the format ***number***{**d|h|m|s**}.

   For example, to set **Watchdog test interval** to ten minutes, enter **10m** or **600s**.

   The maximum is two days (**2d**), and the default is five minutes (**5m**).
6. Type or select the **Number of test failures before a reboot**.
7. Configure the tests that the watchdog will perform:
   a. Click to expand **Fault detection tests**.
   b. Click to expand **Memory usage**.
      i. The memory check is enabled by default. To disable, click the **Enable memory check** toggle.
      ii. For **RAM usage threshold to trigger a warning**, type or select the percentage of RAM usage that will trigger a warning. The minimum value is **60** percent, the maximum is **100** percent. The default is **90** percent.
      iii. Type or select the **Percentage of system memory used before triggering a reboot**. The minimum value is **60** percent, the maximum is **100** percent. The default is **95** percent.
      iv. To log memory usage with every watchdog memory usage test, click to enable **Log memory usage every interval**.
   c. Click to expand **Interface tests**.
      i. Click the **Enable interface(s) down check** toggle to enable. The system periodically checks the interfaces you configure here and, after the specified amount of time, reboots them.
      ii. Click to expand **Check interface(s)**.
      iii. Click to add a new interface.
      iv. For **Interface**, choose the interface you want to test.
   d. Click to expand **Modem down**. This configuration is enabled by default.
      i. Click the **Enable modem check** toggle to disable.
      ii. Click the **Enable modem power cycle** toggle if you want the modem to be power cycled after an initial timeout instead of this timeout being reported as a failure.
      iii. For **Downtime**, type the amount of time the modem is down before it is reported.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The watchdog is enabled by default. To disable:

```
(config)> system watchdog enable false
(config)>
```

4. Set the amount of time between running system tests:

```
(config)> system watchdog interval value
(config)>
```

where *value* is any number of days, hours, minutes, or seconds, and takes the format ***number*** {**d|h|m|s**}.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> system watchdog interval 600s
(config)>
```

The maximum is two days (**2d**), and the default is five minutes (**5m**).

5. Set the number of test failures before the system reboots:

```
(config)> system watchdog num_failures int
(config)>
```

6. Configure the tests that the watchdog will perform:
   a. The memory check is enabled by default. To disable:

```
(config)> system watchdog tests memory enable false
(config)>
```

   b. Set the percentage of RAM usage that will trigger a warning:

```
(config)> system watchdog tests memory max_memory_warning int
(config)>
```

   The minimum value is **60** percent, the maximum is **100** percent. The default is **90** percent.
   c. Set the percentage of RAM usage that will trigger a reboot of the device:

```
(config)> system watchdog tests memory max_memory_critical int
(config)>
```

   The minimum value is **60** percent, the maximum is **100** percent. The default is **95** percent.
   d. To log memory usage with every watchdog memory usage test, enable **log_memory**:

```
(config)> system watchdog tests memory log_memory true
(config)>
```

   e. To have the interface(s) checked and rebooted after the specified amount of time:

```
(config)> system watchdog tests interfaces interfaces add [value]
(config)>
```

   with *value* being the name of the interface.

f. To have the modem power cycled after an initial timeout instead of this timeout being reported as a failure:

```
(config)> system watchdog tests modem
(config)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

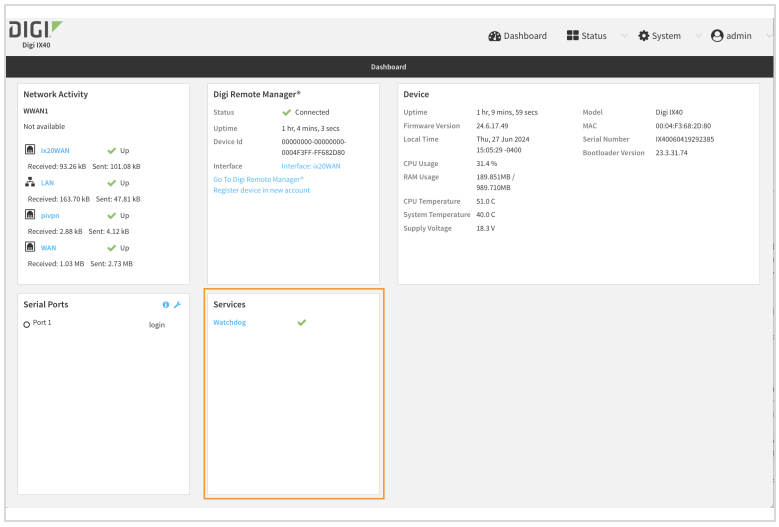
View Watchdog metrics

To view metrics for the Watchdog service and the tests performed:

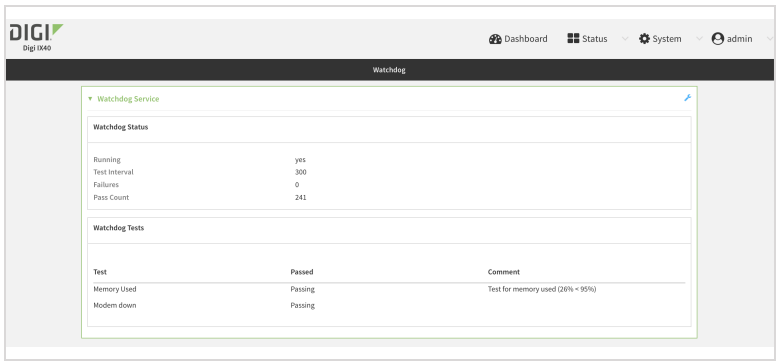
Web

In the local Web UI of your IX10:

1. Log in to the local Web UI of your device as a user with full Admin access rights.
2. To access the Watchdog Service page:
   From the Dashboard of the device:
   a. In the **Services** card, you can see the operational status of the Watchdog service.



b. Click **Watchdog** to view metrics.

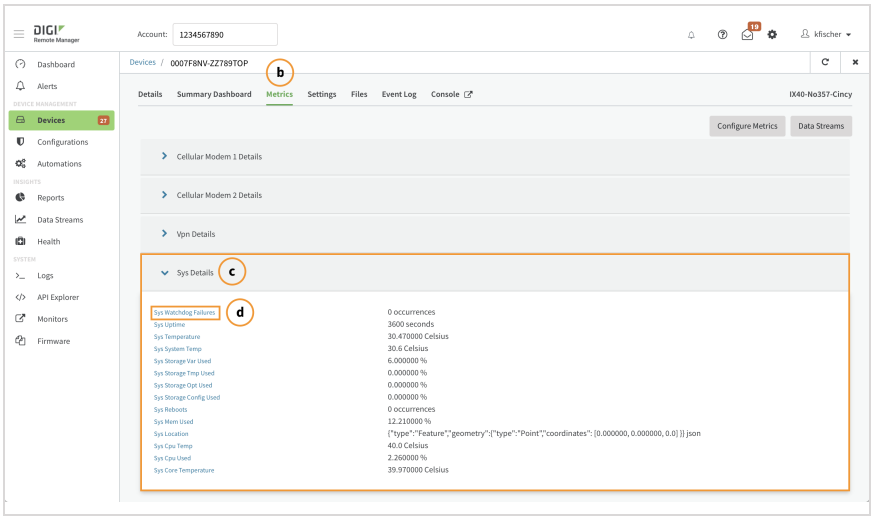


From the menu:

Click **Status** > **Services** > **Watchdog** to see the page.

In Digi Remote Manager, to view the test failures:

a. Click **Devices**, and select a device from the list.
b. Click **Metrics**.
c. Click to expand **Sys Details**.
d. Click **Sys Watchog Failures**.



A new window opens and displays a chart showing the test failures and when they occurred.

Command line

To view the results of the Watchdog tests:

1. Access the Command Line Interface for your IX10, from either the local web UI as an administrator with full access rights or from Digi Remote Manager.
2. At the prompt, type

```
show watchdog
```

All tests that were performed, as well as their status are listed.

3. Type **exit** to exit the CLI.

Monitoring

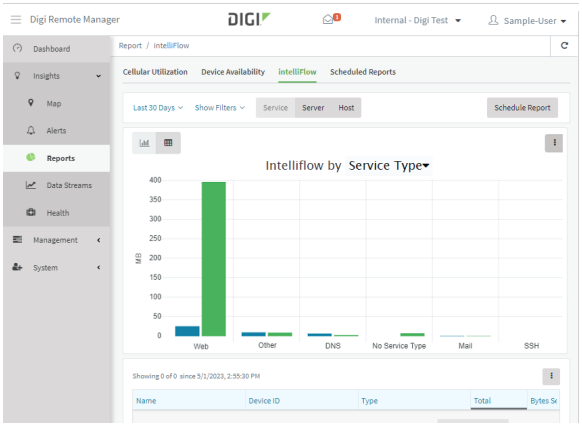
This chapter contains the following topics:

intelliFlow 860
Configure NetFlow Probe 872

intelliFlow

Digi intelliFlow is a reporting and graphical presentation tool for visualizing your network's data usage and network traffic information.

intelliFlow can be enabled on Digi Remote Manager to provide a full analysis of all Digi devices on your network. Contact your Digi sales representative for information about enabling intelliFlow on Remote Manager.



IntelliFlow is also available on the local device for device-specific visualization of network use. To use intelliFlow on the local device, you must have access to the local WebUI. Once you enable intelliFlow, the **Status** > **intelliFlow** option is available in the main menu. By default, intelliFlow is disabled on the local device.

On the local device, intelliFlow provides charts on the following information:

- System utilisation
- Top data usage by host
- Top data usage by server
- Top data usage by service
- Host data usage over time

intelliFlow charts are dymanic; at any point, you can click inside the chart to drill down to view more granular information, and menu options allow you to change various aspects of the information being displayed.

This section contains the following topics:

Enable intelliFlow 861
Configure service types 863
Configure domain name groups 865
Use intelliFlow to display average CPU and RAM usage 868
Use intelliFlow to display top data usage information 869
Use intelliFlow to display data usage by host over time 871

Enable intelliFlow

Required configuration items

- Enable intelliFlow.

Additional configuration items

- The firewall zone for internal clients being monitored by intelliFlow.

To enable intelliFlow:

Web

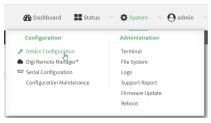
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

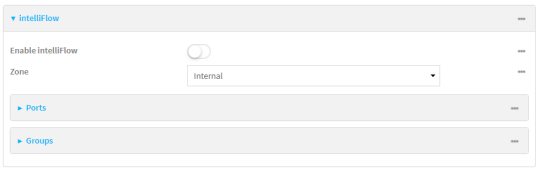
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Monitoring** > **intelliFlow**.
   The intelliFlow configuration window is displayed.

4. Click **Enable intelliFlow**.
5. For **Zone**, select the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone.
6. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable IntelliFlow:

```
(config)> monitoring intelliflow enable true
```

4. Set the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone:

   a. Determine available zones:

```
(config)> monitoring intelliflow zone ?

Zone: The firewall zone which is assigned to the network interface(s) that
intelliFlow will see as internal clients.  intelliFlow relies on an internal to
external relationship, where the internal clients are present on the zone specified.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Default value: internal
Current value: internal

(config)>
```

   b. Set the zone to be used by IntelliFlow:

```
(config)> monitoring intelliflow zone my_zone
```

5. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure service types

The service type is used to categorize several ports under one service. For example, port numbers 80, 443, and 8080 are included in the **Web** service type.

There are several predefined service types:

- Web: Ports 80, 443, and 8080.
- FTP: Ports 20, 21, 989, and 990.
- SSH: Port 22.
- Telnet: Ports 23 and 992.
- Mail: Ports 25, 110, 143, 220, 993 and 995.
- DNS: Port 53.
- IRC: Ports 194 and 994.
- RSYNC: Ports 873.

You can add and remove ports from the predefined service port types, and you can also define your own service types. For example, to define a service type called "MyService" using ports 9000 and 9001:

Web

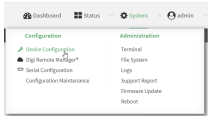
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

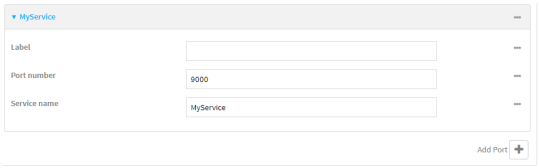
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Monitoring** > **intelliFlow**.
4. Click to expand **Ports**.

5. At the bottom of the list of ports, click to add a port.

6. **Label** is optional.
7. For **Port number**, type **9000**.
8. For **Service name**, type **MyService**.



9. Click to add a another port.
10. For **Port number**, type **9001**.
11. For **Service name**, type **MyService**.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a port:

```
(config)> add monitoring intelliflow ports end
(config monitoring intelliflow ports 20)>
```

4. Set the port number:

```
(config monitoring intelliflow ports 20)> port 9000
(config monitoring intelliflow ports 20)>
```

5. Set the service type:

```
(config monitoring intelliflow ports 20)> service MyService
(config monitoring intelliflow ports 20)>
```

6. Add another port:

```
(config monitoring intelliflow ports 20)> add .. end
(config monitoring intelliflow ports 21)>
```

7. Set the port number:

```
(config monitoring intelliflow ports 21)> port 9001
(config monitoring intelliflow ports 21)>
```

8. Set the service type:

```
(config monitoring intelliflow ports 21)> service MyService
(config monitoring intelliflow ports 21)>
```

9. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure domain name groups

Domain name groups are used to categorize serveral domains names in one group. For example, digi.com and devicecloud.com could be grouped together in an intelliFlow group called Digi.

Web

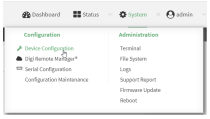
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

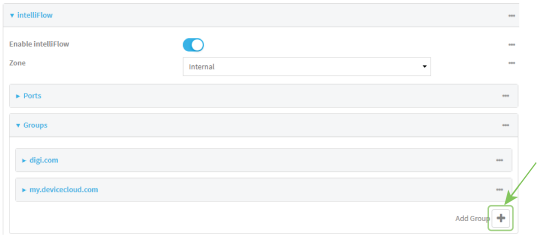
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring** > **intelliFlow** > **Groups**.
4. Click to add a domain.



5. **Label** is optional.
6. For **Domain name**, type **digi.com**.
7. For **Group**, type **Digi**.
8. Click to add a another port.
9. For **Domain name**, type **devicecloud.com**.
10. For **Group**, type **Digi**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a group:

```
(config)> add monitoring intelliflow groups end
(config monitoring intelliflow groups 1)>
```

4. Set the domain name:

```
(config monitoring intelliflow groups 1)> domian digi.com
(config monitoring intelliflow groups 1)>
```

5. Set the group name:

```
(config monitoring intelliflow groups 1)> group Digi
(config monitoring intelliflow groups 1)>
```

6. Add another port:

```
(config monitoring intelliflow groups 1)> add .. end
(config monitoring intelliflow groups 2)>
```

7. Set the port number:

```
(config monitoring intelliflow groups 2)> domain devicecloud.com
(config monitoring intelliflow groups 2)>
```

8. Set the service type:

```
(config monitoring intelliflow groups 2)> group Digi
(config monitoring intelliflow groups 2)>
```

9. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Use intelliFlow to display average CPU and RAM usage

This procedure is only available from the WebUI.

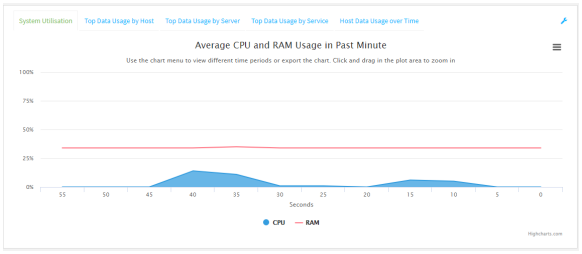
To display display average CPU and RAM usage:

Web

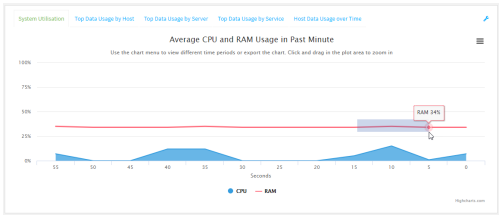
Log into the IX10 WebUI as a user with full Admin access rights.

1. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
2. From the menu, click **Status** > **intelliFlow**.

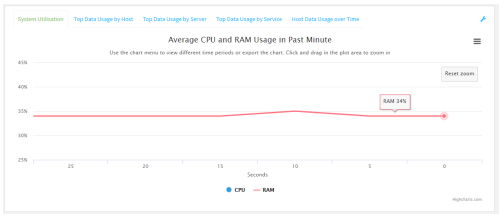
The System Utilisation chart is displayed:



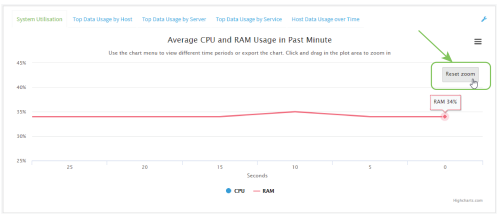
- Display more granular information:
  1. Click and drag over an area in the chart to zoom into that area and provide more granular information.



  2. Release to display the selected portion of the chart:



3. Click **Reset zoom** to return to the original display:

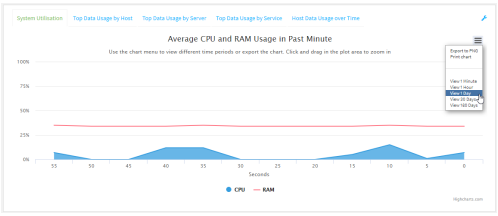


- Change the time period displayed by the chart.

  By default, the **System utilisation** chart displays the average CPU and RAM usage over the last minute. You can change this to display the average CPU and RAM usage:

  - Over the last hour.
  - Over the last day.
  - Over the last 30 days.
  - Over the last 180 days.

  1. Click the menu icon (☰).
  2. Select the time period to be displayed.



- Save or print the chart.

  1. Click the menu icon (☰).
  2. To save the chart to your local filesystem, select **Export to PNG**.
  3. To print the chart, select **Print chart**.

Use intelliFlow to display top data usage information

With intelliFlow, you can display top data usage information based on the following:

- Top data usage by host
- Top data usage by server
- Top data usage by service

To generate a top data usage chart:

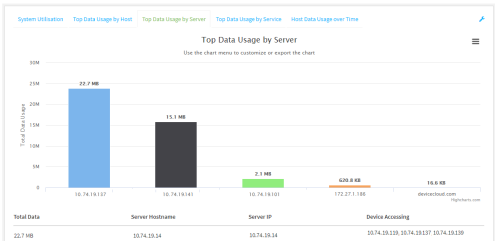
Web

Log into the IX10 WebUI as a user with full Admin access rights.

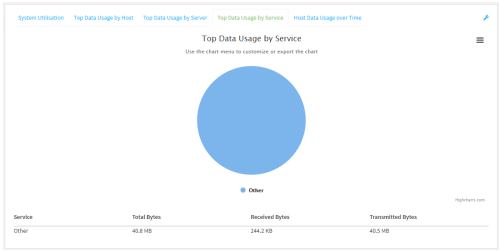
1. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
2. From the menu, click **Status** > **intelliFlow**.

3. Display a data usage chart:
   - To display the **Top Data Usage by Host** chart, click **Top Data Usage by Host**.

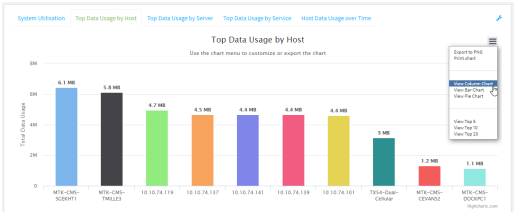
   - To display the **Top Data Usage by Server** chart, click **Top Data Usage by Server**.



   - To display the **Top Data Usage by Service** chart, click **Top Data Usage by Service**.

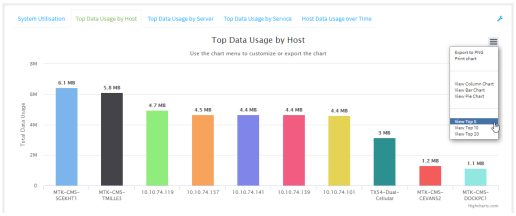


4. Change the type of chart that is used to display the data:
   a. Click the menu icon (☰).
   b. Select the type of chart.



5. Change the number of top users displayed.
   You can display the top five, top ten, or top twenty data users.

a. Click the menu icon ( ).
b. Select the number of top users to displayed.



6. Save or print the chart.
   a. Click the menu icon ( ).
   b. To save the chart to your local filesystem, select **Export to PNG**.
   c. To print the chart, select **Print chart**.

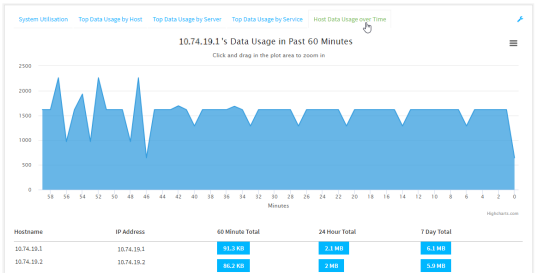
Use intelliFlow to display data usage by host over time

To generate a chart displaying a host's data usage over time:

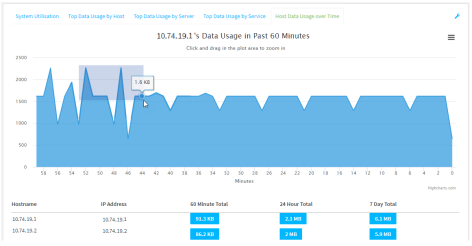
Web

Log into the IX10 WebUI as a user with full Admin access rights.

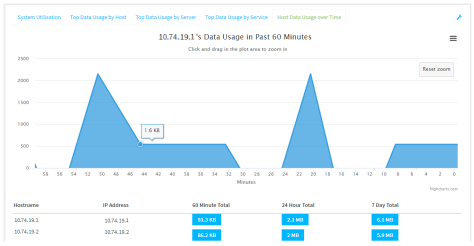
1. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
2. From the menu, click **Status** > **intelliFlow**.
3. Click **Host Data Usage Over Time**.



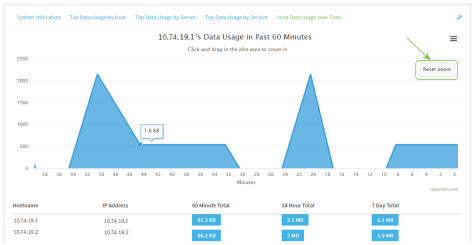
- Display more granular information:
  a. Click and drag over an area in the chart to zoom into that area and provide more granular information.



b. Release to display the selected portion of the chart:



c. Click **Reset zoom** to return to the original display:



- Save or print the chart.
  a. Click the menu icon ( ).
  b. To save the chart to your local filesystem, select **Export to PNG**.
  c. To print the chart, select **Print chart**.

Configure NetFlow Probe

NetFlow probe is used to probe network traffic on the IX10 device and export statistics to NetFlow collectors.

Required configuration items

- Enable NetFlow.
- The IP address of a NetFlow collector.

Additional configuration items

- The NetFlow version.
- Enable flow sampling and select the flow sampling technique.
- The number of flows from which the flow sampler can sample.
- The number of seconds that a flow is inactive before it is exported to the NetFlow collectors.
- The number of seconds that a flow is active before it is exported to the NetFlow collectors.
- The maximum number of simultaneous flows.
- A label for the NetFlow collector.
- The port of the NetFlow collector.
- Additional NetFlow collectors.

To probe network traffic and export statistics to NetFlow collectors:

Web

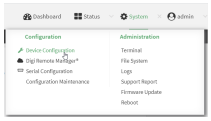
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

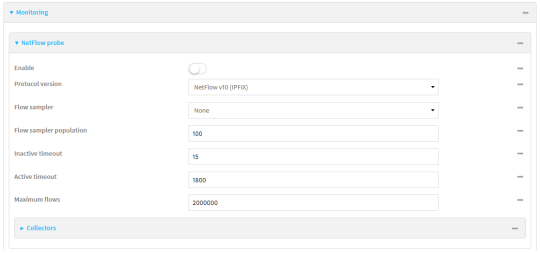
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **Monitoring** > **NetFlow probe**.

4. **Enable** NetFlow probe.
5. **Protocol version:** Select the **Protocol version**. Available options are:
   - **NetFlow v5**—Supports IPv4 only.
   - **NetFlow v9**—Supports IPv4 and IPv6.
   - **NetFlow v10 (IPFIX)**—Supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

   The default is **NetFlow v10 (IPFIX)**.
6. Enable **Flow sampler** by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows. Available options are:
   - **None**—No flow sampling method is used. Each flow is accounted.
   - **Deterministic**—Selects every *n*th flow, where *n* is the value of **Flow sampler population**.

- **Random**—Randomly selects one out of every *n* flows, where *n* is the value of **Flow sampler population**.
- **Hash**—Randomly selects one out of every *n* flows using the hash of the flow key, where *n* is the value of **Flow sampler population**.

7. For **Flow sampler population**, if you selected a flow sampler, enter the number of flows for the sampler. Allowed value is any number between **2** and **16383**. The default is **100**.
8. For **Inactive timeout**, type the the number of seconds that a flow can be inactive before sent to a collector. Allowed value is any number between **1** and **15**. The default is **15**.
9. For **Active timeout**, type the number of seconds that a flow can be active before sent to a collector. Allowed value is any number between **1** and **1800**. The default is **1800**.
10. For **Maximum flows**, type the maximum number of flows to probe simultaneously. Allowed value is any number between **0** and **2000000**. The default is **2000000**.
11. Add collectors:
    a. Click to expand **Collectors**.
    b. For **Add Collector**, click .
    c. (Optional) Type a **Label** for the collector.
    d. For **Address**, type the IP address of the collector.
    e. (Optional) For **Port**, enter the port number used by the collector. The default is 2055.

    Repeat to add additional collectors.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable NetFlow:

```
(config)> monitoring netflow enable true
(config)>
```

4. Set the protocol version:

```
(config)> monitoring netflow protocol version
                                (config)>
```

   where *version* is one of:

   - **v5**—NetFlow v5 supports IPv4 only.
   - **v9**—NetFlow v9 supports IPv4 and IPv6.
   - **v10**—NetFlow v10 (IPFIX) supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

The default is **v10**.

1. Enable flow sampling by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows.

```
(config)> monitoring netflow sampler type
(config)>
```

where *type* is one of:

- **none**—No flow sampling method is used. Each flow is accounted.
- **deterministic**—Selects every *n*th flow, where *n* is the value of the flow sample population.
- **random**—Randomly selects one out of every *n* flows, where *n* is the value of the flow sample population.
- **hash**—Randomly selects one out of every *n* flows using the hash of the flow key, where *n* is the value of the flow sample population.

5. If you are using a flow sampler, set the number of flows for the sampler:

```
(config)> monitoring netflow sampler_population value
(config)>
```

where *value* is any number between **2** and **16383**. The default is **100**.

6. Set the number of seconds that a flow can be inactive before sent to a collector:

```
(config)> monitoring netflow inactive_timeout value
(config)>
```

where *value* is any is any number between **1** and **15**. The default is **15**.

7. Set the number of seconds that a flow can be active before sent to a collector:

```
(config)> monitoring netflow active_timeout value
(config)>
```

where *value* is any is any number between **1** and **1800**. The default is **1800**.

8. Set the maximum number of flows to probe simultaneously:

```
(config)> monitoring netflow max_flows value
(config)>
```

where *value* is any is any number between **0** and **2000000**. The default is **2000000**.

9. Add collectors:
   a. Add a collector:

```
(config)> add monitoring netflow collector end
(config monitoring netflow collector 0)>
```

   b. Set the IP address of the collector:

```
(config monitoring netflow collector 0)> address ip_address
(config monitoring netflow collector 0)>
```

c. (Optional) Set the port used by the collector:

```
(config monitoring netflow collector 0)> port port
(config monitoring netflow collector 0)>
```

d. (Optional) Set a label for the collector:

```
(config monitoring netflow collector 0)> label "This is a collector."
(config monitoring netflow collector 0)>
```

Repeat to add additional collectors.

10. Save the configuration and apply the change.

```
(config monitoring netflow collector 0)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

File system

This chapter contains the following topics:

The IX10 local file system 878
Display directory contents 878
Create a directory 879
Display file contents 880
Copy a file or directory 880
Move or rename a file or directory 881
Delete a file or directory 882
Upload and download files 883

The IX10 local file system

The IX10 local file system has approximately TBD of space available for storing files, such as Python programs, alternative configuration files and firmware versions, and release files, such as cellular module images. The writable directories within the file system are:

- /tmp
- /opt
- /etc/config

Files stored in the /tmp directory do not persist across reboots. Therefore, /tmp is a good location to upload temporary files, such as files used for firmware updates. Files stored in /opt and /etc/config do persist across reboots, but are deleted if a factory reset of the system is performed. See Erase device configuration and reset to factory defaults for more information.

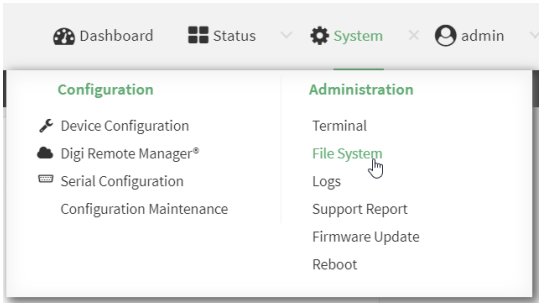
Display directory contents

To display directory contents by using the WebUI or the Admin CLI:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.

2. Highlight a directory and click ⏎ to open the directory and view the files in the directory.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type **ls** ***/path/dir_name***. For example, to display the contents of the **/etc/config** directory:

```
> ls /etc/config
-rw-r--r--   1 root    root        856 Nov 20 20:12 accns.json
drw-------   2 root    root        160 Sep 23 04:02 analyzer
drwxr-xr-x   3 root    root        224 Sep 23 04:02 cc_acl
-rw-r--r--   1 root    root         47 Sep 23 04:02 dhcp.leases
...
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Create a directory

Command line

This procedure is not available through the WebUI. To make a new directory, use the mkdir command, specifying the name of the directory.

For example:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type **mkdir** ***/path/dir_name***. For example, to create a directory named **temp** in **/etc/config**:

```
> mkdir /etc/config/temp
>
```

3. Verify that the directory was created:

```
> ls /etc/config
...
-rw-r--r--   1 root    root       1436 Aug 12 21:36 ssl.crt
-rw-------   1 root    root       3895 Aug 12 21:36 ssl.pem
-rw-r--r--   1 root    root         10 Aug  5 06:41 start
drwxr-xr-x   2 root    root        160 Aug 25 17:49 temp
>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Display file contents

This procedure is not available through the WebUI. To display the contents of a file by using the Admin CLI, , use the more command, specifying the name of the directory.

For example:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **more /*path*/*filename***. For example, to view the content of the file **accns.json** in **/etc/config**:

```
> more /etc/config/accns.json
{
  "auth":
    "user": {
      "admin": {
        "password": "$2a$05$W1sls1oxsadf/n4J0XT.Rgr6ewr1yerHtXQdbafsatGswKg0YUm"
      }
    }
  },
  "schema": {
    "version": "461"
  }
}
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Copy a file or directory

This procedure is not available through the WebUI. To copy a file or directory by using the Admin CLI, use the cp command, specifying the existing path and filename followed by the path and filename of the new file, or specifying the existing path and directory name followed by the path and directory name of the new directory.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type **cp /*path*/*filename*|*dir_name* /*path*[*filename*]|*dir_name***. For example:
   - To copy the file **/etc/config/accns.json** to a file named **backup_cfg.json** in a directory named **/etc/config/test**, enter the following:

     ```
     > cp /etc/config/accns.json /etc/config/test/backup_cfg.json
     >
     ```

   - To copy a directory named **/etc/config/test** to **/opt**:

     ```
     > cp /etc/config/test/ /opt/
     >
     ```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Move or rename a file or directory

This procedure is not available through the WebUI. To move or rename a file or directory by using the Admin CLI, use the mv command.

Command line

To rename a file named **test.py** in **/etc/config/scripts** to **final.py**:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type:

   ```
   > mv /etc/config/scripts/test.py /etc/config/scripts/final.py
   >
   ```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

To move **test.py** from **/etc/config/scripts** to **/opt**:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type:

   ```
   > mv /etc/config/scripts/test.py /opt/
   >
   ```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

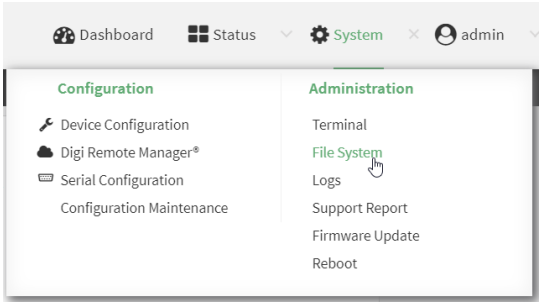
Delete a file or directory

To delete a file or directory by using the WebUI or the Admin CLI:

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



   The **File System** page appears.

2. Highlight the directory containing the file to be deleted and click to open the directory.
3. Highlight the file to be deleted and click .
4. Click **OK** to confirm.

Command line

To delete a file named **test.py** in **/etc/config/scripts**:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type:

```
> rm /etc/config/scripts/test.py
rm: remove '/etc/config/scripts/test.py'? yes
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

To delete a directory named **temp** from **/opt**:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type:

```
> rm /opt/temp/
rm: descend into directory '/opt/temp'? yes
rm: remove directory '/opt/temp'? yes
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Upload and download files

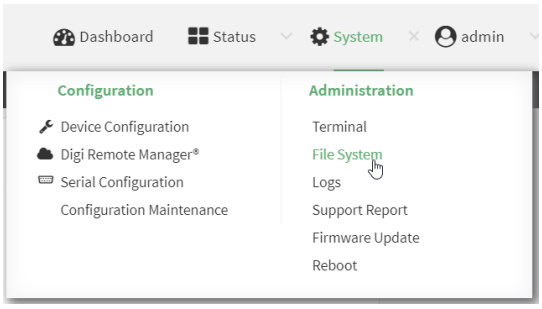
You can download and upload files by using the WebUI or from the command line by using the scp Secure Copy command, or by using a utility such as SSH File Transfer Protocol (SFTP) or an SFTP application like FileZilla.

Upload and download files by using the WebUI

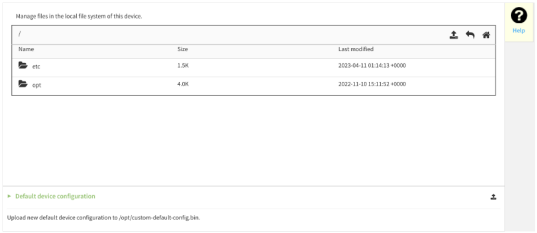
Upload files

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



   The **File System** page appears.

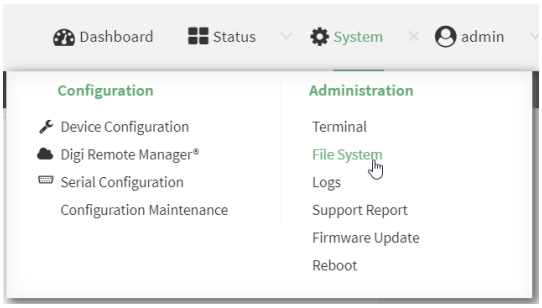


2. Highlight the directory to which the file will be uploaded and click to open the directory.
3. Click ❽ (upload).
4. Browse to the location of the file on your local machine. Select the file and click **Open** to upload the file.

Download files

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.

2. Highlight the directory to which the file will be uploaded and click to open the directory.
3. Highlight the appropriate file and click (download).

Upload and download files by using the Secure Copy command

Copy a file from a remote host to the IX10 device

To copy a file from a remote host to the IX10 device, use the scp command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
- *local-path* is the location on the IX10 device where the copied file will be placed.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the /etc/config directory on the IX10 device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/IX10-25.2.bin local /etc/config/scripts to local
admin@192.168.4.1's password: adminpwd
IX10-25.2.bin              100%   36MB   11.1MB/s      00:03
>
```

Transfer a file from the IX10 device to a remote host

To copy a file from the IX10 device to a remote host, use the scp command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX10 device.

For example:

To copy a support report from the IX10 device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

   ```
   > system support-report path /var/log/
   Saving support report to /var/log/support-report-0040D0133536-24-01-12-12:10:00.bin
   Support report saved.
   >
   ```

2. Use the **scp** command to transfer the report to a remote host:

   ```
   > scp host 192.168.4.1 user admin remote /home/admin/temp/ local /var/log/support-report-
   00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
   admin@192.168.4.1's password: adminpwd
   support-report-0040D0133536-24-01-12-12:10:00.bin
   >
   ```

Upload and download files using SFTP

Transfer a file from a remote host to the IX10 device

This example uploads firmware from a remote host to the IX10 device with an IP address of **192.168.2.1**, using the username **ahmed**:

```
$ sftp ahmed@192.168.2.1
Password:
Connected to 192.168.2.1
sftp> put IX10-25.2
Uploading IX10-25.2 to IX10-25.2
IX10-25.2                                     100%  24M  830.4KB/s   00:00
sftp> exit
$
```

Transfer a file from the IX10 device to a remote host

This example downloads a file named **test.py** from the IX10 device at the IP address of **192.168.2.1** with a username of **ahmed** to the local directory on the remote host:

```
$ sftp ahmed@192.168.2.1
Password:
Connected to 192.168.2.1
sftp> get test.py
Fetching test.py to test.py
test.py                                       100%  254    0.3KB/s   00:00
sftp> exit
$
```

Diagnostics

This chapter contains the following topics:

Perform a speedtest 888
Generate a support report 888
View system and event logs 893
Configure syslog servers 897
Configure options for the event and system logs 899
Configure an email notification for a system event 904
Configure an SNMP trap for a system event 905
Analyze network traffic 906
Use the ping command to troubleshoot network connections 924
Use the traceroute command to diagnose IP routing problems 924

Perform a speedtest

To perform a speedtest:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **iperf** command to generate the report:

   ```
   > iperf host
   ```

   where *host* is the hostname or IP address of a speedtest host. For example:

   ```
   > iperf speedtest.accns.com
   Tx (upload) average: 50.1110 Mbps
   Tx latency: 31.45 ms
   Rx (download) average: 44.7588 Mbps
   Rx latency: 30.05 ms
   >
   ```
3. To output the result in json format, use the **output** parameter:

   ```
   > iperf host output json
   {"tx_avg": "51.8510", "tx_avg_units": "Mbps", "tx_latency": "31.07",
   "tx_latency_units": "ms", "rx_avg": "39.5770", "rx_avg_units": "Mbps",
   "rx_latency": "34.19", "rx_latency_units": "ms" }
   >
   ```
4. To change the size of the speedtest packet, use the **size** parameter:

   ```
   > iperf host size int
   ```
5. By default, the speedtest uses *nuttcp* for the mode. To change this setting from *nuttcp* to *iperf*, use the **mode** parameter:

   ```
   > iperf host mode iperf
   ```
6. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

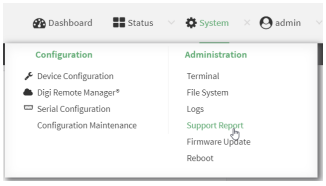
Generate a support report

To generate and download a support report:

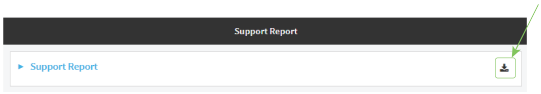
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Administration**, click **Support Report**.



2. Click to generate and download the support report.



Attach the support report to any support requests.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **system support-report** command to generate the report:

```
> system support-report path /var/log/
Saving support report to /var/log/support-report-0040D0133536-24-01-12-12:10:00.bin
Support report saved.
>
```

3. Use the **scp** command to transfer the report to a remote host:

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local /var/log/support-report-
00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-24-01-12-12:10:00.bin
>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See Support report overview for an overview of what is contained in the support report.

Support report overview

Generating a Support Report

Support reports provide a snapshot of a device's current settings and connection status at the time of the report's generation. The relevant log files are packaged into a **.bin** file that can be downloaded from the local (web) UI. For more information about generating support reports, see Generate a support report.

Note Information logged on the device will be erased when the device is powered off or rebooted to avoid unnecessary wear to the flash memory. See Configure options for the event and system logs for more information on how to enable persistent system logs.

Use 7-Zip or any other file-archiving utility to extract a support report. Its contents are organized into the following directories:

/etc

This folder most notably contains a running list of the cellular connections that have been registered by the device's radio.

Directory	Filename	Notes
/etc	version	Active firmware version
/etc/config	mn.json	Cellular connections logged as having been engaged by the radio; establishes previous APN associations

/opt

Information stored here persists between reboots and system resets.

Directory	Filename	Notes
/opt/log_last	messages	With persistent system logs enabled, syslog info will be stored in the /opt directory which isn't erased after reboots or system resets

/tmp

Output from a series of diagnostic queries is stored in a randomly generated sub-directory within /tmp. When combing through these logs, pay particular attention to config_dump-public (to verify local device settings) and mmcli-dump (to validate the cellular connection status).

Directory	Filename	Notes
/tmp/#*		*# is generated at random
	arp_-nv	The table of IP-address to MAC-address translations used by the address resolution protocol (ARP)
	arptables_-nvv_-L	The tables of ARP packet filter rules in the Linux kernel
	cat_procmeminfo	A breakdown of memory utilization at the time when the support report was generated
	config_dump-public	The device's current settings, scrubbed of passwords and preshared keys
	conntrack_-L	A list of all currently tracked connections through the system

Directory	Filename	Notes
	conntrack_-S	A summary of currently tracked connections
	date	Local system time. If the device isn't online when the support report is generated, the date will be based on the date/month/year that the firmware running on the device was created (e.g. 18.4.54.41 was created 2018-07-05)
	df_-h	A report of the file system disk space usage
	event_list	A list of events leveraged for syslog messages
	fw_printenv	The entire environment for the bootloader U-Boot
	ip_addr_list	IP addresses listed per interface
	ip_route_list	Default routing information per interface
	ip6tables_-nv_-L	A list of IPv6 routing tables
	ip6tables_-nv_-L_-t_mangle	Firewall table used when handling mangled/fragmented IPv6 packets
	ip6tables_-nv_-L_-t_nat	Firewall table used to direct NAT'd traffic
	iptables_-nv_-L	A list of IPv4 firewall tables
	iptables_-nv_-L_-t_mangle	Firewall table used when handling mangled/fragmented IPv4 packets
	iptables_-nv_-L_-t_nat	Firewall table used to direct NAT'd traffic
	s_-RlhA_etcconfig	An index of items in /etc/config (and its sub-directories)
	ls_-RlhA_opt	An index of items in /opt (and its sub-directories)
	ls_-RlhA_tmp	An index of items in /tmp (and its sub-directories)
	ls_-RlhA_var	An index of items in /var (and its sub-directories)
	mmcli-dump	A repository of critical information about the cellular radio based off of the cited modem-manager output and defined set of AT commands
	netstat_-i	Interface statistics for transmitted/ received packets
	netstat_-na	List of both listening and non-listening network sockets on the device
	ps_l	A snapshot of the current processes running at the time of generating the report

Directory	Filename	Notes
	runt_json	Storage for active/ engaged system variables
	sprite_config_ dump	Not used for cellular devices
	ubus-dump	A log of ubus calls for network devices and interfaces
	uptime	The device's uptime at the time of generating the report, along with CPU load averages for the past 1, 5, and 15 minutes

/var/log

The running system log is stored in "messages" until reaching a set line count (1,000 lines by default). Once this limit is exceeded, that file is renamed to "messages.0" and a new running log is written to the now-empty "messages" log.

Directory	Filename	Notes
/var/log	messages	Current syslog information
	messages.0	Rollover syslog information

/var/run

This directory can be disregarded for most troubleshooting/ diagnostic purposes.

Directory	Filename	Notes
/var/run	all files	Runtime settings for the device -- referenced in the syslog data gathered in /tmp (see above)

View system and event logs

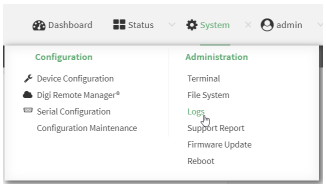
See Configure options for the event and system logs for information about configuring the information displayed in event and system logs.

View System Logs

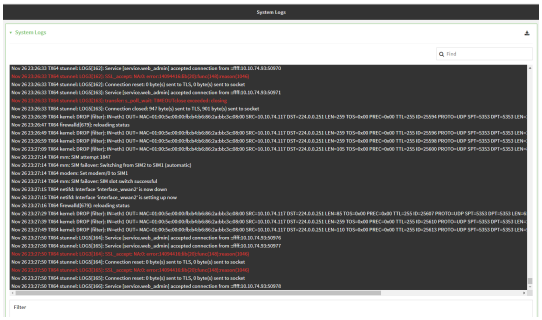
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System** > **Logs**.

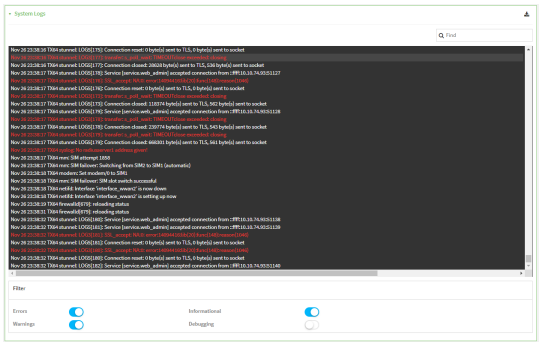


The system log displays:

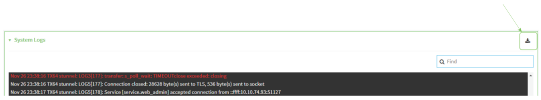


2. Limit the display in the system log by using the **Find** search tool.

3. Use filters to configure the types of information displayed in the system logs.



4. Click to download the system log.



Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the show log command at the Admin CLI prompt:

```
> show log

Timestamp      Message
-------------  ------------------------------------------------------------
Nov 26 21:54:34  IX10 netifd: Interface 'interface_wan' is setting up now
Nov 26 21:54:35  IX10 firewalld[621]: reloading status
...
>
```

3. (Optional) Use the **show log number *num*** command to limit the number of lines that are displayed. For example, to limit the log to the most recent ten lines:

```
> show log number 10

Timestamp      Message
-------------  ------------------------------------------------------------
Nov 26 21:54:34  IX10 netifd: Interface 'interface_wan' is setting up now
Nov 26 21:54:35  IX10 firewalld[621]: reloading status
...
>
```

4. (Optional) Use the **show log filter *value*** command to limit the number of lines that are displayed. Allowed values are **critical**, **warning**, **info**, and **debug**. For example, to limit the event list to only info messages:

```
> show log filter info

Timestamp      Type   Category  Message
-------------- ------- --------- ------------------------------------------
Nov 26 22:01:26  info   user     name=admin~service=cli~state=opened~remote=192.168.1.2
Nov 26 22:01:25  info   user     name=admin~service=cli~state=closed~remote=192.168.1.2
...
>
```

5. Type **exit** to exit the Admin CLI.

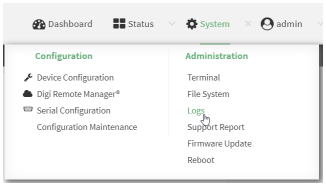
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

View Event Logs

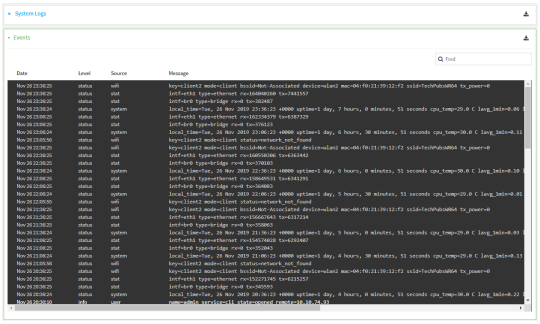
Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the main menu, click **System** > **Logs**.



2. Click **System Logs** to collapse the system logs viewer, or scroll down to **Events**.
3. Click **Events** to expand the event viewer.



4. Limit the display in the event log by using the **Find** search tool.

5. Click to download the event log.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the show event command at the Admin CLI prompt:

```
> show event

Timestamp       Type    Category  Message
----------------- ------- --------- -------------------------------------------
Nov 26 21:42:37  status  stat     intf=eth1~type=ethernet~rx=11332435~tx=5038762
Nov 26 21:42:35  status  system   local_time=Thu, 08 Aug 2019 21:42:35 +0000~uptime=3 hours, 0
minutes, 48 seconds
...
>
```

3. (Optional) Use the **show event number *num*** command to limit the number of lines that are displayed. For example, to limit the event list to the most recent ten lines:

```
> show event number 10

Timestamp       Type    Category  Message
----------------- ------- --------- -------------------------------------------
Nov 26 21:42:37  status  stat     intf=eth1~type=ethernet~rx=11332435~tx=5038762
Nov 26 21:42:35  status  system   local_time=Thu, 08 Aug 2019 21:42:35 +0000~uptime=3 hours, 0
minutes, 48 seconds
...
>
```

4. (Optional) Use the **show event table *value***command to limit the number of lines that are displayed. Allowed values are **error**, **info**, and **status**. For example, to limit the event list to only info messages:

```
> show event table info

Timestamp       Type    Category  Message
----------------- ------- --------- -------------------------------------------
Nov 26 22:01:26  info    user     name=admin~service=cli~state=opened~remote=192.168.1.2
Nov 26 22:01:25  info    user     name=admin~service=cli~state=closed~remote=192.168.1.2
...
>
```

5. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure syslog servers

You can configure remote syslog servers for storing event and system logs.

Web

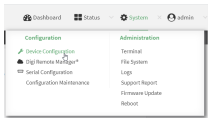
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

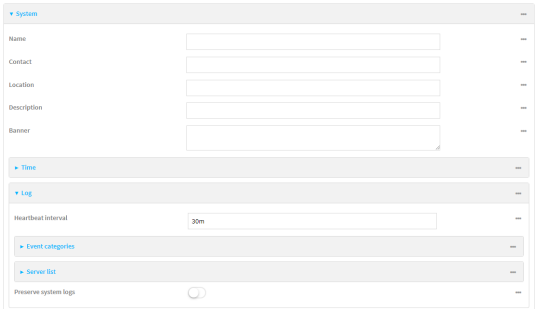
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

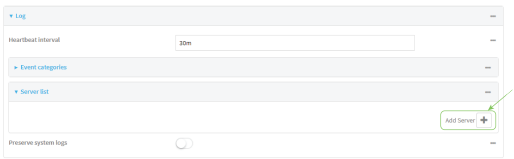
   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

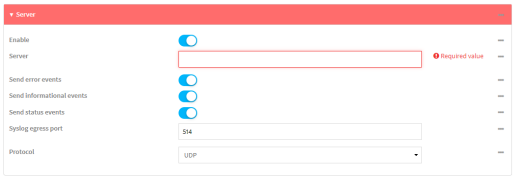
   The **Configuration** window is displayed.
3. Click **System** > **Log**.

4. Add and configure a remote syslog server:
   a. Click to expand **Server list**.
   b. For **Add Server**, click

The log server configuration window is displayed.



Log servers are enabled by default. To disable, toggle off **Enable**.

c. Type the host name or IP address of the **Server**.

d. Select the event categories that will be sent to the server. By default, all event categories are enabled. You can disable logging for error, informational, and status event categories by clicking to toggle off the category.

e. For **Syslog egress port**, type the port number to use for the syslog server. The default is **514**.

f. For **Protocol**, select the IP protocol to use for communication with the syslog server. Available options are **TCP** and **UPD**. The default is **UPD**.

5. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) To configure remote syslog servers:

   a. Add a remote server:

```
(config)> add system log remote end
(config system log remote 0)>
```

   b. Enable the server:

```
(config system log remote 0)> enable true
(config system log remote 0)>
```

   c. Set the host name or IP address of the server:

```
(config system log remote 0)> server hostname
(config system log remote 0)>
```

   d. The event categories that will be sent to the server are automatically enabled when the server is enabled.

- To disable informational event messages:

```
(config system log remote 0)> info false
(config system log remote 0)>
```

- To disable status event messages:

```
(config system log remote 0)> status false
(config system log remote 0)>
```

- To disable informational event messages:

```
(config system log remote 0)> error false
(config system log remote 0)>
```

4. Set the port number to use for the syslog server:

```
(config system log remote 0)> port value
(config system log remote 0)>
```

   where *value* is any integer between **1** and **65535**. The default is **514**.

5. Set the IP protocol to use for communication with the syslog server:

```
(config system log remote 0)> protocol value
(config system log remote 0)>
```

   where *value* is either **tcp** or **udp**. The default is **udp**.

6. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure options for the event and system logs

The default configuration for event and system logging is:

- The heartbeat interval, which determines the amount of time to wait before sending a heartbeat event if no other events have been sent, is set to 30 minutes.
- All event categories are enabled.

To change or disable the heartbeat interval, or to disable event categories, and to perform other log configuration:

Web

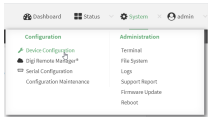
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

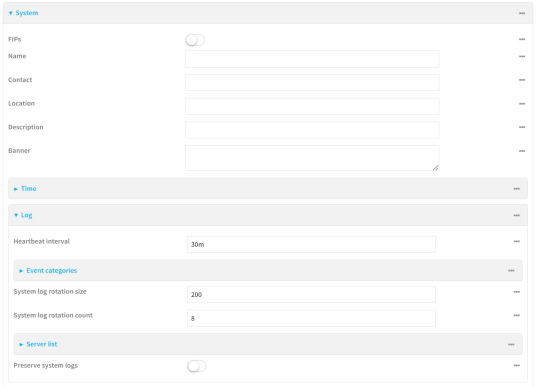
   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.
3. Click **System** > **Log**.

4. (Optional) To change the **Heartbeat interval** from the default of 30 minutes, type a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent.

   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

   For example, to set **Heartbeat interval** to ten minutes, enter **10m** or **600s**.

   To disable the **Heartbeat interval**, enter **0s**.
5. (Optional) To disable event categories, or to enable them if they have been disabled:

   a. Click to expand **Event Categories**.
   b. Click an event category to expand.

c. Depending on the event category, you can enable or disable different types of events.

- **Enable error events**: Enable to generate an event whenever an error occurs.
- **Enable status events**: Enable to generate periodic reports of the current status. These events are generated at specific time intervals, rather than when changes occur, and are only sent if a change has occurred since the previous report. Status events may also be generated in response to remote control commands.
- **Status interval**: The minimum time interval between periodic status events. The limitation does not apply to events generated in response to remove control commands. Set this field to blank to only send events generated in response to remote control command.

  Syntax: *number*{**w**|**d**|**h**|**m**|**s**}

  Default: 30m (30 minutes)

  This field works with the **Enable status events** option.
- **Enable informational events**: Enable to generate an event whenever a significant change occurs.
- **Enable email notifications**: Enable to email a system log event notification to a specified email address. The email address must also be specified before a notification can be sent. To configure, see Configure an email notification for a system event.
- **Enable SNMP traps**: Enable to save system log event information to an SNMP trap. At least one SNMP destination must be defined before event information can be saved. To configure, see Configure an SNMP trap for a system event.

6. (Optional) See Configure syslog servers for information about configuring remote syslog servers to which log messages will be sent.
7. (Optional) To change the system log settings from the defaults, type in a new value.
   - **System log rotation size**: Specify the maximum size (measured in kilobytes) the system log file can reach before log rotation. When the specified size is reached, the system log rotates.

     Default is **200** kb. Minimum is **10** kb.
   - **System log rotation count**: Specify the number of system log files to keep.

     Default is **8**. Minimum is **1**; maximum is **20**.
8. Enable **Preserve system logs** to save the current session's system log after a reboot.

   By default, the IX10 device erases system logs each time the device is powered off or rebooted.

   Note You should only enable **Preserve system logs** temporarily to debug issues. Once you are finished debugging, immediately disable **Preserve system logs** to avoid unnecessary wear to the flash memory.
9. (Optional) Configure **Email notifications** to send an email notification of a system event. See Configure an email notification for a system event.
10. (Optional) Configure **SNMP traps** destinations for a IX10 to save system event information. See Configure an SNMP trap for a system event.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) To change the heartbeat interval from the default of 30 minutes, set a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent.

```
(config)> system log heartbeat_interval value
(config)>
```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **the heartbeat interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> system log heartbeat_interval 600s
(config)>
```

   To disable the heartbeat interval, set the value to **0s**

4. Enable preserve system logs functionality to save the current session's system log after a reboot. By default, the IX10 device erases system logs each time the device is powered off or rebooted.

   Note You should only enable **Preserve system logs** temporarily to debug issues. Once you are finished debugging, immediately disable **Preserve system logs** to avoid unnecessary wear to the flash memory.

```
(config)> system log persistent true
(config)>
```

5. (Optional) To disable event categories, or to enable them if they have been disabled:
   a. Use the question mark (**?**) to determine available event categories:

```
(config)> system log event ?

Event categories: Settings to enable individual event categories.

 Additional Configuration
 ------------------------------------------------------------------------------
arping              ARP ping
config              Configuration
dhcpserver            DHCP server
firmware            Firmware
```

```
location          Location
modem             Modem
netmon            Active recovery
network           Network interfaces
openvpn           OpenVPN
portal            Captive portal
remote            Remote control
restart           Restart
serial            Serial
sms               SMS commands
speed             Speed
stat              Network statistics
user              User
watchdog          Watchdog

wol               Wake-On-LAN

(config)> system log event
```

b. Depending on the event category, you can enable or disable informational events, status events, and error events. Some categories also allow you to set the status interval, which is the time interval between periodic status events. For example, to configure DHCP server logging:

   i. Use the question mark (**?**) to determine what events are available for DHCP server logging configuration:

```
(config)> system log event dhcpserver ?
...
DHCP server: Settings for DHCP server events. Informational events are generated
when a lease is obtained or released. Status events report the current list of
leases.

 Parameters            Current Value
 ------------------------------------------------------------------------------
 info                  true        Enable informational events
 status                true        Enable status events
 status_interval       30m         Status interval

(config)> system log event dhcpserver
```

   ii. To disable informational messages for the DHCP server:

```
(config)> system log event dhcpserver info false
(config)>
```

   iii. To change the status interval:

```
(config)> system log event dhcpserver status_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **the status interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> system log event dhcpserver status_interval 600s
(config)>
```

6. (Optional) See Configure syslog servers for information about configuring remote syslog servers to which log messages will be sent.
7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure an email notification for a system event

You can configure the IX10 to send an email notification of a system event.

Step 1: Configure the SMTP server that is used to send email notifications when a system log event occurs by enabling the **Email notifications** system log feature.

Step 2: Review the system log event categories and select the type of information that you want to save to the system log: errors, informational events, or status events, depending on the event category. To ensure the notification is sent, enable the **Enable email notification** option for the event category.

1. Log in to the web UI.
2. Click **System** > **Device Configuration**. The **Configuration** page displays.
3. Expand **System** > **Log**.
4. Expand **Email notifications**.
5. Click **Enable**. The slider is blue when enabled.
   a. From the **Server type** list box, select the method used to connect and authenticate with the SMTP server.
   b. In the **SMTP server name** field, enter the host name or IP address of the SMTP server.
   c. In the **SMTP server port** field, enter the TCP port of the SMTP server.
   d. In the **Server user name** field, enter the server login name.
   e. In the **Server password** field, enter the server password.
   f. In the **Email from address** field, enter the email address that should be placed in the **From** field on an email.
   g. the **Email to address** field, enter the email address that should be place in the **To** field on an email.
   h. In the **Email subject** field, enter the text for the subject line of the email.
6. Click **Apply** to save the configuration and apply the change.

7. Review the system log event categories and select the type of information that you want to save to the system log, and enable the **Enable email notification** option. To configure these options, see Configure options for the event and system logs.

Configure an SNMP trap for a system event

You can configure an SNMP trap destination for a IX10 to save system event information.

Step 1: Configure an SNMP trap by enabling the **SNMP traps** system log feature.

Step 2: Review the system log event categories and select the type of information that you want to save to the system log and the SNMP trap: errors, informational events, or status events, depending on the event category. To ensure the log information is saved to an SNMP trap, enable the **Enable SNMP traps** option for the event category.

1. Log in to the web UI.
2. Click **System** > **Device Configuration**. The **Configuration** page displays.
3. Expand **System** > **Log**.
4. Expand **SNMP traps**.
5. Click **Enable**. The slider is blue when enabled.
6. Add a destination.
   a. Click **Add Destination**.
   b. In the **Host Name** field, enter the host name or IP address of the SNMP destination.
   c. In the **Port** field, enter the UDP port of the SNMP destination. The default is **162**.
   d. In the **Community name** field, enter the SNMP destination community name. The default is **public**.
   e. Repeat this process to add an additional destination, if needed.
7. Click **Apply** to save the configuration and apply the change.
8. Review the system log event categories and select the type of information that you want to save to the system log, and enable the **Enable SNMP traps** option. To configure these options, see Configure options for the event and system logs.

Analyze network traffic

The IX10 device includes a network analyzer tool that captures data traffic on any interface and decodes the captured data traffic for diagnostics. You can capture data traffic on multiple interfaces at the same time and define capture filters to reduce the captured data. You can capture up to 10 MB of data traffic in two 5 MB files per interface.

To perform a more detailed analysis, you can download the captured data traffic from the device and view it using a third-party application.

Note Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See Save captured data traffic to a file.

This section contains the following topics:

Configure packet capture for the network analyzer 907
Example filters for capturing data traffic 916
Capture packets from the command line 917
Stop capturing packets 918
Show captured traffic data 919
Save captured data traffic to a file 920
Download captured data to your PC 921
Clear captured data 922

Configure packet capture for the network analyzer

To use the network analyzer, you must create one or more packet capture configuration.

Required configuration items

- The interface used by this packet capture configuration.

Additional configuration items

- The filter expression for this packet capture configuration.
- Schedule the analyzer to run based on a specified event or at a particular time:
  - The events or time that will trigger the analyzer to run, using this capture configuration.
  - The amount of time that the analyzer session will run.
  - The frequency with which captured events will be saved.

To configure a packet capture configuration:

Web

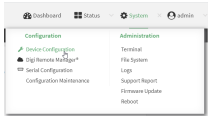
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

   Remote Manager:

   a. Locate your device as described in Use Digi Remote Manager to view and manage your device.
   b. Click the **Device ID**.
   c. Click **Settings**.
   d. Click to expand **Config**.

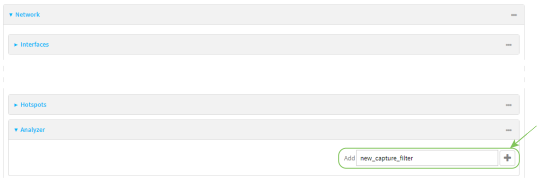
   Local Web UI:

   a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

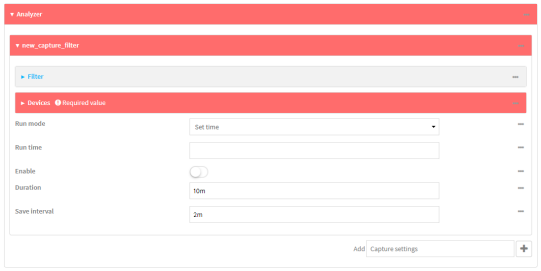
   

   The **Configuration** window is displayed.
3. Click **Network** > **Analyzer**.

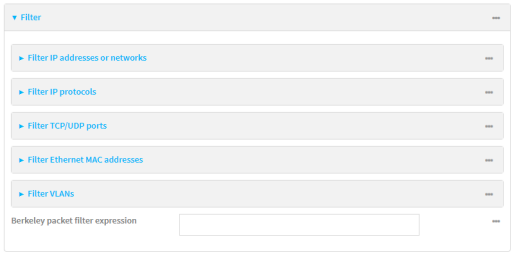
4. For **Add Capture settings**, type a name for the capture filter and click ♑



The new capture filter configuration is displayed.

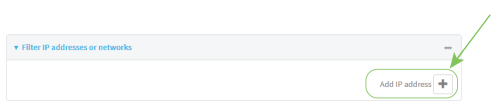


5. (Optional) Add a filter type:
   a. Click to expand **Filter**.



   You can select from preconfigured filters to determine which types of packets to capture or ignore, or you can create your own Berkeley packet filter expression.

   b. To create a filter that either captures or ignores packets from a particular IP address or network:
      i. Click to expand **Filter IP addresses or networks**.
      ii. Click ♑ to add an IP address/network.



      iii. For **IP address or network**, type the IPv4 or IPv6 address (and optional netmask).
      iv. For **Source or destination IP address**, select whether the filter should apply to packets when the IP address/network is the source, the destination, or both.
      v. Click **Ignore this IP address or network** if the filter should ignore packets from this IP address/network. By default, is option is disabled, which means that the filter will capture packets from this IP address/network.
      vi. Click ♑ to add additional IP address/network filters.

c. To create a filter that either captures or ignores packets that use a particular IP protocol:
   i. Click to expand **Filter IP protocols**.
   ii. Click to add an IP protocol.
   iii. For **IP protocol to capture or ignore**, select the protocol. If **Other protocol** is selected, type the number of the protocol.
   iv. Click **Ignore this protocol** if the filter should ignore packets that use this protocol. By default, is option is disabled, which means that the filter will capture packets that use this protocol.
   v. Click to add additional IP protocols filters.

d. To create a filter that either captures or ignores packets from a particular port:
   i. Click to expand **Filter TCP/UDP port**.
   ii. Click to add a TCP/UDP port.
   iii. For **IP TCP/UDP port to capture or ignore**, type the number of the port to be captured or ingored.
   iv. For **TCP or UDP port**, select the type of transport protocol.
   v. For **Source or destination TCP/UDP port**, select whether the filter should apply to packets when the port is the source, the destination, or both.
   vi. Click **Ignore this TCP/UDP port** if the filter should ignore packets that use this port. By default, is option is disabled, which means that the filter will capture packets that use this port.
   vii. Click to add additional port filters.

e. To create a filter that either captures or ignores packets from one or more specified MAC addresses:
   i. Click to expand **Filter Ethernet MAC addresses**.
   ii. Click to add a MAC address.
   iii. For **Ethernet MAC address**, type the MAC address to be captured or ingored.
   iv. For **Source or destination Ethernet MAC address**, select whether the filter should apply to packets when the Ethernet MAC address is the source, the destination, or both.
   v. Click **Ignore this MAC address** if the filter should ignore packets that use this port. By default, is option is disabled, which means that the filter will capture packets that use this port.
   vi. Click to add additional MAC address filters.

f. To create a filter that either captures or ignores packets from one or more VLANs:
   i. Click to expand **Filter VLANs**.
   ii. Click to add a VLAN.
   iii. For **The VLAN to capture or ignore**, type the number of the VLAN.
   iv. Click **Ignore this VLAN** if the filter should ignore packets that use this port. By default, is option is disabled, which means that the filter will capture packets that use this port.
   v. Click to add additional VLAN filters.

g. For **Berkeley packet filter expression**, type a filter using Berkeley Packet Filter (BPF) syntax. See Example filters for capturing data traffic for examples of filters using BPF syntax.

6. Add one or more interface to the capture filter:
   a. Click to expand **Device**.
   b. Click to add an interface to the capture setting instance.

   c. For **Device**, select an interface.
   d. Repeat to add additional interfaces to the capture filter.
7. (Optional) For **Berkeley packet filter expression**, type a filter using Berkeley Packet Filter (BPF) syntax. See Example filters for capturing data traffic for examples of filters using BPF syntax.
8. (Optional) Schedule the analyzer to run, using this capture filter, based on a specified event or at a particular time:
   a. For **Run mode**, select the mode that will be used to run the capture filter. Available options are:
      - **On boot**: The capture filter will run once each time the device boots.
      - **Interval**: The capture filter will start running at the specified interval, within 30 seconds after the configuration change is saved.
        - If **Interval** is selected, in **Interval**, type the interval.

          Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

          For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
      - **Set time**: Runs the capture filter at a specified time of the day.
        - If **Set Time** is selected, specify the time that the capture filter should run in **Run time**, using the format *HH:MM*.
      - **During system maintenance**: The capture filter will run during the system maintenance time window.
   b. **Enable** the capture filter schedule.
   c. For **Duration**, type the amount of time that the scheduled analyzer session will run.

      Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

      For example, to set **Duration** to ten minutes, enter **10m** or **600s**.
   d. For **Save interval**, type the frequency with which captured events will be saved.

      Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

      For example, to set **Save interval** to ten minutes, enter **10m** or **600s**.
9. Click **Apply** to save the configuration and apply the change.

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

   ```
   > config
   (config)>
   ```

3. Add a new capture filter:

   ```
   (config)> add network analyzer name
   (config network analyzer name)>
   ```

4. Add an interface to the capture filter:

   ```
   (config network analyzer name)> add device end device
   (config network analyzer name)>
   ```

   Determine available devices and the proper syntax.

   To determine available devices and proper syntax, use the space bar autocomplete feature:

   ```
   (config network analyzer name)> add device end <space>
   (config network analyzer name)> add interface end /network/
   ```

   Repeat to add additional interfaces.

5. (Optional) Set a filter for the capture filter:
   a. To create a filter that either captures or ignores packets from a particular IP address or network:
      i. Add a new IP address/network filter:

      ```
      (config network analyzer name)> add filter address end
      (config network analyzer name filter address 0)>
      ```

      ii. Set the IPv4 or IPv6 address (and optional netmask):

      ```
      (config network analyzer name filter address 0)> address ip_address[/netmask]
      (config network analyzer name filter address 0)>
      ```

      iii. Set whether the filter should apply to packets when the IP address/network is the source, the destination, or both:

      ```
      (config network analyzer name filter address 0)> match value
      (config network analyzer name filter address 0)>
      ```

      where *value* is one of:

      - **source**: The filter will apply to packets when the IP address/network is the source.
      - **destination**: The filter will apply to packets when the IP address/network is the destination.

- **either**: The filter will apply to packets when the IP address/network is either the source or the destination.

iv. (Optional) Set the filter should ignore packets from this IP address/network:

```
(config network analyzer name filter address 0)> ignore true
(config network analyzer name filter address 0)>
```

By default, is option is set to **false**, which means that the filter will capture packets from this IP address/network.

v. Repeat these steps to add additional IP address filters.

b. To create a filter that either captures or ignores packets that use a particular IP protocol:

i. Add a new IP protocol filter:

```
(config network analyzer name)> add filter protocol end
(config network analyzer name filter protocol 0)>
```

ii. Use the **?** to determine available protocols and the appropriate format:

```
(config network analyzer name filter protocol 0)> protocol ?

IP protocol to capture or ignore: IP protocol to capture or ignore.
Format:
  ah
  esp
  gre
  icmp
  icmpv6
  igmp
  ospf
  other
  tcp
  udp
  vrrp
Current value:

(config network analyzer name filter protocol 0)>
```

iii. Set the protocol:

```
(config network analyzer name filter protocol 0)> protocol value
(config network analyzer name filter protocol 0)>
```

iv. If other is set for the protocol, set the number of the protocol:

```
(config network analyzer name filter protocol 0)> protocol_other value
(config network analyzer name filter protocol 0)>
```

where *value* is an integer between 1 and 255 and represents the the number of the protocol.

v. (Optional) Set the filter should ignore packets from this protocol:

```
(config network analyzer name filter protocol 0)> ignore true
(config network analyzer name filter protocol 0)>
```

By default, is option is set to **false**, which means that the filter will capture packets from this protocol.

vi. Repeat these steps to add additional protocol filters.

c. To create a filter that either captures or ignores packets from a particular port:

i. Add a new port filter:

```
(config network analyzer name)> add filter port end
(config network analyzer name filter port 0)>
```

ii. Set the transport protocol that should be filtered for the port:

```
(config network analyzer name filter port 0)> protocol value
(config network analyzer name filter port 0)>
```

where *value* is one of **tcp**, **udp**, or **either**. The default is either.

iii. Set whether the filter should apply to packets when the port is the source, the destination, or both:

```
(config network analyzer name filter port 0)> match value
(config network analyzer name filter port 0)>
```

where *value* is one of:

- **source**: The filter will apply to packets when the port is the source.
- **destination**: The filter will apply to packets when the port is the destination.
- **either**: The filter will apply to packets when the port is either the source or the destination.

iv. (Optional) Set the filter should ignore packets from this port:

```
(config network analyzer name filter port 0)> ignore true
(config network analyzer name filter port 0)>
```

By default, is option is set to **false**, which means that the filter will capture packets from this port.

v. Repeat these steps to add additional port filters.

d. To create a filter that either captures or ignores packets from one or more specified MAC addresses:

i. Add a new MAC address filter:

```
(config network analyzer name)> add filter mac_address end
(config network analyzer name filter mac_address 0)>
```

ii. Set the MAC address that should be be captured or ignored:

```
(config network analyzer name filter mac_address 0)> address value
(config network analyzer name filter mac_address 0)>
```

where *value* is the MAC address to be filtered, using colon-hexadecimal notation with lower case, for example, **00:aa:11:bb:22:cc**.

iii. Set whether the filter should apply to packets when the MAC address is the source, the destination, or both:

```
(config network analyzer name filter mac_address 0)> match value
(config network analyzer name filter mac_address 0)>
```

where *value* is one of:

- **source**: The filter will apply to packets when the MAC address is the source.
- **destination**: The filter will apply to packets when the MAC address is the destination.
- **either**: The filter will apply to packets when the MAC address is either the source or the destination.

iv. (Optional) Set the filter should ignore packets from this port:

```
(config network analyzer name filter mac_address 0)> ignore true
(config network analyzer name filter mac_address 0)>
```

By default, is option is set to **false**, which means that the filter will capture packets from this MAC address.

v. Repeat these steps to add additional MAC addresses.

e. To create a filter that either captures or ignores packets from one or more specified VLANs:

i. Add a new VLAN filter:

```
(config network analyzer name)> add filter vlan end
(config network analyzer name filter vlan 0)>
```

ii. Set the VLAN that should be be captured or ignored:

```
(config network analyzer name filter vlan 0)> vlan value
(config network analyzer name filter vlan 0)>
```

where *value* is number o the VLAN.

iii. (Optional) Set the filter should ignore packets from this VLAN:

```
(config network analyzer name filter vlan 0)> ignore true
(config network analyzer name filter vlan  0)>
```

By default, is option is set to **false**, which means that the filter will capture packets from this MAC address.

iv. Repeat these steps to add additional VLANs.

f. To create a filter using Berkeley Packet Filter (BPF) syntax:

```
(config network analyzer name)> filter custom value
(config network analyzer name)>
```

where *value* is a filter using Berkeley Packet Filter (BPF) syntax. Values that contain spaces must be enclosed in double quotes (").

See Example filters for capturing data traffic for examples of filters using BPF syntax.

6. (Optional) Schedule the analyzer to run, using this capture filter, based on a specified event or at a particular time:
   a. Enable scheduling for this capture filter:

```
(config network analyzer name)> schedule enable true
(config network analyzer name)>
```

   b. Set the mode that will be used to run the capture filter:

```
(config network analyzer name)> when mode
(config network analyzer name)>
```

   where *mode* is one of the following:

   - **boot**: The script will run once each time the device boots.
   - **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected, set the interval:

```
(config add network analyzer name)> on_interval value
(config add network analyzer name)>
```

     where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

     For example, to set **on_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network analyzer name)> on_interval 600s
(config network analyzer name)>
```

   - **set_time**: Runs the script at a specified time of the day. If **set_time** is set, set the time that the script should run, using the format *HH*:*MM*:

```
(config network analyzer name)> run_time HH:MM
(config network analyzer name)>
```

   - **maintenance_time**: The script will run during the system maintenance time window.

   c. Set the amount of time that the scheduled analyzer session will run:

```
(config network analyzer name)> duration value
(config network analyzer name)>
```

   where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

   For example, to set **duration** to ten minutes, enter either **10m** or **600s**:

```
(config network analyzer name)> save_interval 600s
(config network analyzer name)>
```

d. Set the frequency with which captured events will be saved:

```
(config network analyzer name)> save_interval value
(config network analyzer name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number***{**w|d|h|m|s**}.

For example, to set **save_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network analyzer name)> save_interval 600s
(config network analyzer name)>
```

7. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Example filters for capturing data traffic

The following are examples of filters using Berkeley Packet Filter (BPF) syntax for capturing several types of network data. See https://biot.com/capstats/bpf.html for detailed information about BPF syntax.

Example IPv4 capture filters

- Capture traffic to and from IP host 192.168.1.1:

```
ip host 192.168.1.1
```

- Capture traffic from IP host 192.168.1.1:

```
ip src host 192.168.1.1
```

- Capture traffic to IP host 192.168.1.1:

```
ip dst host 192.168.1.1
```

- Capture traffic for a particular IP protocol:

```
ip proto protocol
```

where *protocol* is a number in the range of **1** to **255** or one of the following keywords: **icmp**, **icmp6**, **igmp**, **pim**, **ah**, **esp**, **vrrp**, **udp**, or **tcp**.

- Capture traffic to and from a TCP port 80:

```
ip proto tcp and port 80
```

- Capture traffic to UDP port 53:

```
ip proto udp and dst port 53
```

- Capture traffic from UDP port 53:

```
ip proto udp and src port 53
```

- Capture to and from IP host 10.0.0.1 but filter out ports 22 and 80:

```
ip host 10.0.0.1 and not (port 22 or port 80)
```

Example Ethernet capture filters

- Capture Ethernet packets to and from a host with a MAC address of 00:40:D0:13:35:36:

```
ether host 00:40:D0:13:35:36
```

- Capture Ethernet packets from host 00:40:D0:13:35:36:

```
ether src 00:40:D0:13:35:36:
```

- Capture Ethernet packets to host 00:40:D0:13:35:36:

```
ether dst 00:40:D0:13:35:36
```

Capture packets from the command line

You can start packet capture at the command line with the analyzer start command. Alternatively, you can schedule the network analyzer to run based on a specified event or at a particular time. See Configure packet capture for the network analyzer for information about scheduling packet capturing.

Additional analyzer commands allow you to:

- Stop capturing packets.
- Save captured data traffic to a file.
- Clear captured data.

Required configuration items

- A configured packet capture. See Configure packet capture for the network analyzer for packet capture configuration information.

To start packet capture from the command line:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

   ```
   > analyzer start name capture_filter
   >
   ```

   where *capture_filter* is the name of a packet capture configuration. See Configure packet capture for the network analyzer for more information.

   To determine available packet capture configurations, use the **?**:

   ```
   > analyzer start name ?

   name: Name of the capture filter to use.
   Format:
    test_capture
    capture_ping

   > analyzer start name
   ```

You can capture up to 10 MB of data traffic in two 5 MB files per interface.

Note Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See Save captured data traffic to a file.

Stop capturing packets

You can stop packet capture at the command line with the analyzer stop command.

To stop packet capture from the command line:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

   ```
   > analyzer stop name capture_filter
   >
   ```

   where *capture_filter* is the name of a packet capture configuration. See Configure packet capture for the network analyzer for more information.

   To determine available packet capture configurations, use the **?**:

   ```
   > analyzer stop name ?
   ```

```
name: Name of the capture filter to use.
Format:
 test_capture
 capture_ping

> analyzer stop name
```

Show captured traffic data

To view captured data traffic, use the show analyzer command. The command output show the following information for each packet:

- The packet number.
- The timestamp for when the packet was captured.
- The length of the packet and the amount of data captured.
- Whether the packet was sent or received by the device.
- The interface on which the packet was sent or received.
- A hexadecimal dump of the packet of up to 256 bytes.
- Decoded information of the packet.

To show captured data traffic:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

```
> show analyzer name capture_filter

Packet 1 : Sept-29-2023 12:10:00.287682, Length 60 bytes (Captured Length 60 bytes)

Received on interface eth1

   00 40 ff 80 01 20 b4 b6  86 21 b5 73 08 00 45 00   .@... .. .!.s..E.
   00 28 3d 36 40 00 80 06  14 bc 0a 0a 4a 82 0a 0a   .(=6@... ....J..
   4a 48 cd ae 00 16 a4 4b  ff 5f ee 1f d8 23 50 10   JH.....K ._...#P.
   08 02 c7 40 00 00 00 00  00 00 00 00               ...@.... ....

  Ethernet Header
    Destination MAC Addr : 00:40:D0:13:35:36
    Source MAC Addr      : fb:03:53:05:11:2f
    Ethernet Type        : IP (0x0800)
  IP Header
    IP Version           : 4
    Header Length        : 20 bytes
    ToS                  : 0x00
```

```
    Total Length       : 40 bytes
    ID                 : 15670 (0x3d36)
    Flags              : Do not fragment
    Fragment Offset    : 0 (0x0000)
    TTL                : 128 (0x80)
    Protocol           : TCP (6)
    Checksum           : 0x14bc
    Source IP Address  : 10.10.74.130
    Dest. IP Address   : 10.10.74.72
  TCP Header
    Source Port        : 52654
    Destination Port   : 22
    Sequence Number    : 2756443999
    Ack Number         : 3995064355
    Data Offset        : 5
    Flags              : ACK
    Window             : 2050
    Checksum           : 0xc740
    Urgent Pointer     : 0
  TCP Data
    00 00 00 00 00 00                  ......

>
```

where *capture_filter* is the name of a packet capture configuration. See Configure packet capture for the network analyzer for more information.

To determine available packet capture configurations, use the **?**:

```
> show anaylzer name ?

 name: Name of the capture filter to use.
 Format:
   test_capture
   capture_ping

> show anaylzer name
```

Save captured data traffic to a file

Data traffic is captured to RAM and when the device reboots, the data is lost. To retain the captured data, first save the data to a file and then upload the file to a PC.

To save captured traffic data to a file, use the analyzer save command:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Type the following at the Admin CLI prompt:

```
> analyzer save filename filename path path
>
```

where:

- *filename* is the name of the file that the captured data will be saved to.

  Determine filenames already in use:

  Use the tab autocomplete feature to determine filenames that are currently in use:

```
> analyzer save name <tab>
test1_analyzer_capture    test2_analyzer_capture
> analyzer save name
```

- *path* is the path and filename to save captured traffic to. If a relative path is provided, /etc/config/analyzer will be used as the root directory for the path and file.

To transfer the file to your PC, see Download captured data to your PC.

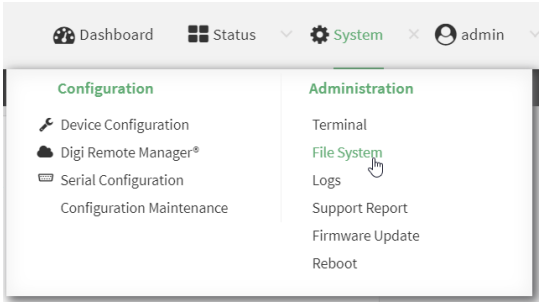
Download captured data to your PC

After saving captured data to a file (see Save captured data traffic to a file), you can download the file from the WebUI or from the command line by using the scp (secure copy file) command.

Web

Log into the IX10 WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.

2. Highlight the **analyzer** directory and click to open the directory.
3. Select the saved analyzer report you want to download and click (download).

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type **scp** to use the Secure Copy program to copy the file to your PC:

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

   where:

   - *hostname-or-ip* is the hostname or IP address of the remote host.
   - *username* is the name of the user on the remote host.
   - *remote-path* is the location on the remote host where the file will be copied.
   - *local-path* is the path and filename on the IX10 device.

   For example:

   To download the traffic saved in the file **/etc/config/analyzer/eth0.pcpng** to a PC with the IP **192.168.210.2**, for a user named **maria**, to the **/home/maria** directory:

```
> scp host 192.168.210.2 user maria remote /home/maria local /etc/config/analyzer/eth0.pcpng to
remote

maria@192.168.210.2's password:
eth0.pcpng                    100%   11KB 851.3KB/s   00:00
```

Clear captured data

To clear captured data traffic in RAM, use the analyzer clear command:

Command line

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

```
> analyzer clear name capture_filter
>
```

   where *capture_filter* is the name of a packet capture configuration. See Configure packet capture for the network analyzer for more information.

   To determine available packet capture configurations, use the **?**:

```
> anaylzer clear name ?

name: Name of the capture filter to use.
Format:
```

```
test_capture
capture_ping

> anaylzer clear name
```

Note You can remove data traffic saved to a file using the rm command.

Use the ping command to troubleshoot network connections

Use the ping command troubleshoot connectivity problems.

Ping to check internet connection

To check your internet connection:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type the ping command followed by the host name or IP address of the server to be pinged:

```
> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=10.7 ms
...
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Stop ping commands

To stop pings when the number of pings to send (the **count** parameter) has been set to a high value, enter **Ctrl+C**.

Use the traceroute command to diagnose IP routing problems

Use the **traceroute** command to diagnose IP routing problems. This command traces the route to a remote IP host and displays results. The **traceroute** command differs from ping in that traceroute shows where the route fails, while ping simply returns a single error on failure.

See the traceroute command description for command syntax and examples. The **traceroute** command has several parameters. Only **host** is required.

- **host**: The IP address of the destination host.
- **bypass**: Send directly to a host on an attached network.
- **debug**: Enable socket level debugging.
- **dontfragment**: Do not fragment probe packets.
- **first_ttl**: Specifies with what TTL to start. (Default: 1)
- **gateway**: Route the packet through a specified gateway.
- **icmp**: Use ICMP ECHO for probes.
- **interface**: Specifies the interface.

- **ipchecksums**: Calculate ip checksums.
- **max_ttl**: Specifies the maximum number of hops. (Default: 30)
- **nomap**: Do not map IP addresses to host names
- **nqueries**: Sets the number of probe packets per hop. (Default: 3)
- **packetlen**: Total size of the probing packet. (Default: -1)
- **pausemsecs**: Minimal time interval between probes (Default: 0)
- **port**: Specifies the destination port. (Default: -1)
- **src_addr**: Chooses an alternative source address.
- **tos**: Set Type of Service. (Default: -1)
- **verbose**: Verbose output.
- **waittime**: Max wait for a response to a probe. (Default: 5)

Example

This example shows using **traceroute** to verify that the IX10 device can route to host **8.8.8.8** (www.google.com) through the default gateway. The command output shows that **15** routing hops were required to reach the host:

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, use the **traceroute** command to view IP routing information:

```
> traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 52 byte packets
 1  192.168.8.1 (192.168.8.1)  0 ms  0 ms  0 ms
 2  10.10.10.10 (10.10.10.10)  0 ms  2 ms  2 ms
 3  * 10.10.8.23 (10.10.8.23)  1 ms  1 ms
 4  96.34.84.22 (96.34.84.22)  1 ms  1 ms  1 ms
 5  96.34.81.190 (96.34.81.190)  2 ms  2 ms  2 ms
 6  * * *
 7  96.34.2.12 (96.34.2.12)  11 ms  11 ms  11 ms
 8  * * *
 9  8.8.8.8 (8.8.8.8)  11 ms  11 ms  11 ms
>
```

By entering a **whois** command on a Unix device, the output shows that the route is as follows:

1. **192/8**: The local network of the IX10 device.
2. **192.168.8.1**: The local network gateway to the Internet.
3. **96/8**: Charter Communications, the network provider.
4. **216/8**: Google Inc.

Stop the traceroute process

To stop the traceroute process, enter **Ctrl-C**.

Digi IX10 regulatory and safety statements

RF exposure statement

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antenna or antennas and the user should not be less than **20 cm**.

Federal Communication (FCC) Part 15 Class B

Radio Frequency Interference (RFI) (FCC 15.105)

The Digi IX10 has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet that is on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

IX10 complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

If the FCC ID is not visible when installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module FCC ID.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Digi may void the user's authority to operate this equipment.

European Community - CE Mark Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for the IX10 concerning emissions, EMC, and safety. For more information, see www.digi.com/resources/certifications.

Important note

Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

IFETEL

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Maximum transmit power for radio frequencies

The following tables show the maximum transmit power for frequency bands.

Cellular frequency bands

Frequency bands	Maximum transmit power
Cellular LTE 700 MHz Cellular LTE 800 MHz Cellular LTE 850 MHz Cellular LTE 900 MHz Cellular LTE 1700 MHz Cellular LTE 1800 MHz Cellular LTE 1900 MHz Cellular LTE 2100 MHz	200 mW
Cellular LTE 2600 MHz Cellular LTE 2300 MHz Cellular LTE 2500 MHz	158.49 mW

Innovation, Science, and Economic Development Canada (IC) certifications

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class B prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

RoHS compliance statement

All Digi International Inc. products that are compliant with the RoHS Directive (EU Directive 2002/95/EC and subsequent amendments) are marked as **RoHS COMPLIANT**. RoHS COMPLIANT means that the substances restricted by the EU Directive 2002/95/EC and subsequent amendments of the European Parliament are not contained in a finished product above threshold limits mandated by EU Directive 2002/95/EC and subsequent amendments, unless the restrictive substance is subject of an exemption contained in the RoHS Directive. Digi International Inc., cannot guarantee that inventory held by distributors or other third parties is RoHS compliant.

Safety notices

- Read all instructions before installing and powering the router. You should keep these instructions in a safe place for future reference.
- If the power supply shows signs of damage or malfunction, stop using it immediately, turn off the power and disconnect the power supply before contacting your supplier for a repair or replacement.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Use only the accessories, attachments, and power supplies provided by the manufacturer-connecting non-approved antennas or power supplies may damage the router, cause interference or create an electric shock hazard, and will void the warranty.
- Do not attempt to repair the product. The router contains no electronic components that can be serviced or replaced by the user. Any attempt to service or repair the router by the user will void the product warranty.
- Ports that are capable of connecting to other apparatus are defined as SELV ports. To ensure conformity with IEC60950 ensure that these ports are only connected to ports of the same type on other apparatus.

Special safety notes for wireless routers

Digi International products are designed to the highest standards of safety and international standards compliance for the markets in which they are sold. However, cellular-based products contain radio devices which require specific consideration. Take the time to read and understand the following guidance. Digi International assumes no liability for an end user's failure to comply with these precautions.

Wireless routers incorporate a wireless radio module. Users should ensure that the antenna(s) is (are) positioned at least 1 meter away from themselves and other persons in normal operation.
When in a hospital or other health care facility, observe the restrictions on the use of mobile phones. Do not use the router in areas where guidelines posted in sensitive areas instruct users to switch off mobile phones. Medical equipment may be sensitive to RF energy.
The operation of cardiac pacemakers, other implanted medical equipment and hearing aids can be affected by interference from cellular terminals such as the wireless routers when places close to the device. If in doubt about potential danger, contact the physician or the manufacturer of the device to verify that the equipment is properly shielded. Pacemaker patients are advised to keep the wireless router away from the pacemaker while it is on.

Wireless routers must NOT be operated on aircraft. The operation of wireless appliances in an aircraft is forbidden to prevent interference with communications systems. Failure to observe these instructions may lead to the suspension or denial of cellular services to the offender, legal action, or both.

As with any electrical equipment, do not operate the router in the presence of flammable gases, fumes or potentially explosive atmospheres. Do not use radio devices anywhere that blasting operations occur.

Wireless routers receive and transmit radio frequency energy when power is on. Interference can occur when using the router close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always power off your router wherever forbidden or when it may cause interference or danger.

SOS IMPORTANT! Wireless routers operate using radio signals and cellular networks cannot be guaranteed to connect in all possible conditions. Therefore, never rely solely upon any wireless device for life critical communications.

Special installation instructions and warnings

IMPORTANT This information applies only to the following variants:

- IX10-00G4: Digi IX10 - LTE, CAT-4, 3G/2G,
- IX10-00N4: Digi IX10 - LTE, CAT-4, NORTH AMERICA ONLY
- IX10-00C6: Digi IX10 - LTE CAT 6 CBRS US ONLY

This equipment is open-type and intended to be installed in an enclosure suitable for the environment, such that the equipment is only accessible with the use of a tool.

This product is suitable for use in Class I, Division 2, Groups A, B, C and D hazardous locations or non-hazardous locations only.

Power supply selection - If you use your own power supply (PSU) for your IX10 router, ensure that it is certified Limited Power Source (LPS) with a supply rated at 12 VDC/1.5A or 18 VDC/1.0A minimum.

Explosion hazard. Do not disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations.

For Class I, Division 2 hazardous locations applications: Antennas intended for use with the product must be installed within the end-use enclosure. For external mounting of the antennas, routing and installation of the antennas shall be in accordance with the appropriate location regulations.

Product disposal instructions

The WEEE (Waste Electrical and Electronic Equipment: 2002/96/EC) directive has been introduced to ensure that electrical/ electronic products are recycled using the best available recovery techniques to minimize the impact on the environment.

This product contains high quality materials and components which can be recycled. At the end of its life this product MUST NOT be mixed with other commercial waste for disposal. Check with the terms and conditions of your supplier for disposal information.

Digi International Ltd WEEE Registration number: WEE/HF1515VU

Safety warnings

English

Ensure that the power cord is connected to a socket-outlet with earthing connection.

To comply with FCC/IC RF exposure limits at least 20 cm separation distance must be maintained between any antenna of the unit and any part of the user at all times.

This appliance does not contain any user-serviceable parts. Never open the equipment. For safety reasons, the equipment should be opened only by qualified personnel.

The unit must be powered off where blasting is in progress, where explosive atmospheres are present, or near medical or life support equipment. Do not power on the unit in any aircraft.

Operation of this equipment in a residential environment could cause radio interference.

For ambient temperatures above 60° C, this equipment must be installed in a Restricted Access Location only.

Explosion hazard. Do not disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations.

For Class I, Division 2 Hazardous locations applications: antennas intended for use with the product must be installed within the end enclosure. For external mounting of the antennas, routing and installation of the antennas shall be in accordance with the appropriate location regulations.

Bulgarian--български

Уверете се, че захранващият кабел е свързан към контакт със заземителна връзка.

За да се спази FCC / IC границите на излагане на радиочестота, трябва да се поддържа поне 20 cm разстояние на разделяне между която и да е антена на устройството и която и да е част от потребителя по всяко време.

Този уред не съдържа части, които обслужват потребителя. Никога не отваряйте оборудването. От съображения за безопасност оборудването трябва да се отваря само от квалифициран персонал.

Уредът трябва да се изключи там, където се извършва взривяване, където има експлозивна атмосфера или в близост до медицинско оборудване или оборудване за поддържане на живота. Не включвайте устройството в самолет.

Работата с това оборудване в жилищна среда може да причини радиосмущения.

За околни температури над 60 ° C, това оборудване трябва да се инсталира само на място с ограничен достъп.

Croatian--Hrvatski

Provjerite je li kabel za napajanje spojen na utičnicu s uzemljenjem.

Da bi se udovoljilo FCC / IC ograničenjima izlaganja RF, mora se održavati najmanje 20 cm udaljenosti odvojenosti od bilo koje antene uređaja i bilo kojeg dijela korisnika u svakom trenutku.

Ovaj uređaj ne sadrži dijelove koje korisnik može servisirati. Nikada ne otvarajte opremu. Iz sigurnosnih razloga opremu bi trebalo otvarati samo kvalificirano osoblje.

Uređaj se mora isključiti tamo gdje je u tijeku miniranje, gdje su prisutne eksplozivne atmosfere ili u blizini medicinske opreme ili opreme za održavanje života. Nemojte uključivati jedinicu ni u jednom zrakoplovu.

Rad ove opreme u stambenom okruženju mogao bi prouzročiti radio smetnje.

Za okolne temperature iznad 60 ° C, ova oprema mora biti instalirana samo na mjestu s ograničenim pristupom.

French--Français

Assurez-vous que le cordon d'alimentation est connecté à une prise de courant avec mise à la terre.

Pour se conformer aux limites d'exposition RF FCC/IC, une distance de séparation d'au moins 20 cm doit être maintenue entre toute antenne de l'unité et toute partie de l'utilisateur à tout moment.

Cet appareil ne contient aucune pièce réparable par l'utilisateur. Ne jamais ouvrir l'équipement. Pour des raisons de sécurité, l'équipement ne doit être ouvert que par du personnel qualifié.

L'unité doit être éteinte là où le dynamitage est en cours, où des atmosphères explosives sont présentes, ou à proximité d'équipements médicaux ou de survie. N'allumez pas l'appareil dans un avion.

L'utilisation de cet équipement dans un environnement résidentiel peut provoquer des interférences radio.

Pour des températures ambiantes supérieures à 60 °C, cet équipement doit être installé uniquement dans un emplacement à accès restreint.

RISQUE D'EXPLOSION - NE DÉBRANCHEZ PAS L'ÉQUIPEMENT PENDANT LE CIRCUITEST SOUS TENSION OU, À MOINS QUE L'ON SACHE QUE LA ZONE EST EXEMPTE DE CONCENTRATIONS INFLAMMABLES.

POUR LES APPLICATIONS DE CLASSE I, DIVISION 2 DANS DES ZONES DANGEREUSES : LES ANTENNES DESTINÉES À ÊTRE UTILISÉES AVEC LE PRODUIT DOIVENT ÊTRE INSTALLÉES DANS LE BOÎTIER D'UTILISATION FINALE. POUR LE MONTAGE EXTERNE DES ANTENNES,

L'ACHEMINEMENT ET L'INSTALLATION DES ANTENNES DOIVENT ÊTRE CONFORMES AUX RÈGLEMENTS D'EMPLACEMENT APPROPRIÉS.

Greek--Ελληνικά

Βεβαιωθείτε ότι το καλώδιο τροφοδοσίας είναι συνδεδεμένο σε πρίζα με σύνδεση γείωσης.

Για συμμόρφωση με τα FCC / IC RF όρια έκθεσης πρέπει να διατηρείται τουλάχιστον 20 cm απόσταση διαχωρισμού μεταξύ οποιασδήποτε κεραίας της μονάδας και οποιουδήποτε μέρους του χρήστη ανά πάσα στιγμή.

Αυτή η συσκευή δεν περιέχει εξαρτήματα που μπορούν να επισκευαστούν από το χρήστη. Μην ανοίγετε ποτέ τον εξοπλισμό. Για λόγους ασφαλείας, ο εξοπλισμός πρέπει να ανοίγει μόνο από εξειδικευμένο προσωπικό.

Η μονάδα πρέπει να είναι απενεργοποιημένη όταν βρίσκεται σε εξέλιξη η έκρηξη, όπου υπάρχουν εκρηκτικές ατμόσφαιρες ή κοντά σε ιατρικό εξοπλισμό ή εξοπλισμό υποστήριξης της ζωής. Μην ενεργοποιείτε τη μονάδα σε κανένα αεροσκάφος.

Η λειτουργία αυτού του εξοπλισμού σε οικιστικό περιβάλλον μπορεί να προκαλέσει παρεμβολές ραδιοφώνου.

Για θερμοκρασίες περιβάλλοντος άνω των 60 ° C, αυτός ο εξοπλισμός πρέπει να εγκατασταθεί μόνο σε θέση περιορισμένης πρόσβασης

Hungarian--Magyar

Győződjön meg arról, hogy a tápkábel csatlakozik egy földelő csatlakozóaljzathoz.

Az FCC / IC rádiófrekvenciás expozíciós határértékeinek betartása érdekében a berendezés bármely antennája és a felhasználó bármely része között legalább 20 cm távolságot kell tartani.

Ez a készülék nem tartalmaz a felhasználó által javítható alkatrészeket. Soha ne nyissa ki a berendezést. Biztonsági okokból a berendezést csak szakképzett személyzet nyithatja meg.

Az egységet ki kell kapcsolni, ha robbantás folyik, ahol robbanásveszélyes környezet van, vagy orvosi vagy életmentő berendezések közelében. Semmilyen repülőgépen ne kapcsolja be az egységet.

A berendezés lakókörnyezetben történő működtetése rádiózavarokat okozhat.

60 ° C feletti környezeti hőmérséklet esetén ezt a berendezést csak korlátozott hozzáférésű helyre kell telepíteni.

Italian--Italiano

Assicurarsi che il cavo di alimentazione sia collegato ad una presa con messa a terra.

Per rispettare i limiti di esposizione RF FCC/IC è necessario mantenere sempre una distanza di separazione di almeno 20 cm tra qualsiasi antenna dell'unità e qualsiasi parte dell'utente.

Questo apparecchio non contiene parti riparabili dall'utente. Non aprire mai l'apparecchiatura. Per motivi di sicurezza, l'apparecchiatura deve essere aperta solo da personale qualificato.

L'unità deve essere spenta dove sono in corso esplosioni, dove sono presenti atmosfere esplosive o vicino ad apparecchiature mediche o di supporto vitale. Non accendere l'unità in nessun aereo.

Il funzionamento di questa apparecchiatura in un ambiente residenziale potrebbe causare interferenze radio.

Per temperature ambiente superiori a 60° C, questa apparecchiatura deve essere installata solo in un luogo ad accesso limitato.

Latvian--Latvietis

Pārliecinieties, ka strāvas vads ir pievienots kontaktligzdai ar zemējuma savienojumu.

Lai ievērotu FCC / IC radiofrekvenču iedarbības robežas, vienmēr jābūt vismaz 20 cm attālumam starp jebkuru ierīces antenu un jebkuru lietotāja daļu.

Šajā ierīcē nav nevienas lietotāja apkalpojamas daļas. Nekad neatveriet aprīkojumu. Drošības apsvērumu dēļ aprīkojumu drīkst atvērt tikai kvalificēts personāls.

Iekārtai jābūt izslēgtai, ja notiek spridzināšana, sprādzienbīstama vide vai medicīnas vai dzīvības uzturēšanas aprīkojuma tuvumā. Nevienā lidmašīnā neieslēdziet ierīci.

Šīs ierīces darbība dzīvojamā vidē var izraisīt radio traucējumus.

Ja apkārtējā temperatūra pārsniedz 60 ° C, šī iekārta jāuzstāda tikai ierobežotas piekļuves vietā.

Lithuanian--Lietuvis

Įsitikinkite, kad maitinimo laidas yra prijungtas prie lizdo su įžeminimu.

Kad būtų laikomasi FCC / IC radijo dažnių apšvitos ribų, tarp bet kurios įrenginio antenos ir bet kurios vartotojo dalies visada turi būti išlaikytas bent 20 cm atstumas.

Šiame prietaise nėra naudotojui prižiūrimų dalių. Niekada neatidarykite įrangos. Saugumo sumetimais įrangą turėtų atidaryti tik kvalifikuotas personalas.

Įrenginys turi būti išjungtas ten, kur vyksta sprogdinimas, sprogi aplinka arba šalia medicinos ar gyvybės palaikymo įrangos. Neįjunkite įrenginio jokiuose orlaiviuose.

Naudojant šią įrangą gyvenamojoje aplinkoje, gali kilti radijo trukdžių.

Esant aukštesnei nei 60 ° C aplinkos temperatūrai, ši įranga turi būti montuojama tik riboto patekimo vietoje.

Polish--Polskie

Upewnij się, że przewód zasilający jest podłączony do gniazdka z uziemieniem.

Aby zachować zgodność z limitami ekspozycji FCC/IC RF, między anteną urządzenia a jakąkolwiek częścią użytkownika musi być zachowana odległość co najmniej 20 cm.

To urządzenie nie zawiera żadnych części, które mogą być naprawiane przez użytkownika. Nigdy nie otwieraj urządzenia. Ze względów bezpieczeństwa urządzenie powinno być otwierane wyłącznie przez wykwalifikowany personel.

Urządzenie musi być wyłączone w miejscach, w których trwają prace wybuchowe, w atmosferze wybuchowej lub w pobliżu sprzętu medycznego lub podtrzymującego życie. Nie włączaj urządzenia w żadnym samolocie.

Praca tego sprzętu w środowisku mieszkalnym może powodować zakłócenia radiowe.

W przypadku temperatur otoczenia powyżej 60°C urządzenie to należy instalować wyłącznie w miejscach o ograniczonym dostępie.

Portuguese--Português

Certifique-se de que o cabo de alimentação esteja conectado a uma tomada com conexão de aterramento.

Para cumprir os limites de exposição à RF da FCC / IC, pelo menos 20 cm de distância de separação deve ser mantida entre qualquer antena da unidade e qualquer parte do usuário o tempo todo.

Este aparelho não contém peças cuja manutenção possa ser feita pelo usuário. Nunca abra o equipamento. Por razões de segurança, o equipamento deve ser aberto apenas por pessoal qualificado.

A unidade deve ser desligada onde houver detonações em andamento, onde houver presença de atmosferas explosivas ou próximo a equipamentos médicos ou de suporte à vida. Não ligue a unidade em nenhuma aeronave.

A operação deste equipamento em um ambiente residencial pode causar interferência de rádio.

Para temperaturas ambientes acima de 60 ° C, este equipamento deve ser instalado apenas em locais de acesso restrito.

Slovak--Slovák

Uistite sa, že je napájací kábel pripojený k zásuvke so zemniacim pripojením.

Aby boli dodržané limity vystavenia vysokofrekvenčným lúčom FCC / IC, musí byť medzi anténou jednotky a akoukoľvek časťou používateľa neustále udržiavaná vzdialenosť najmenej 20 cm.

Toto zariadenie neobsahuje žiadne diely opraviteľné používateľom. Nikdy neotvárajte zariadenie. Z bezpečnostných dôvodov by malo zariadenie otvárať iba kvalifikovaný personál.

Jednotka musí byť vypnutá tam, kde prebiehajú trhacie práce, kde je prítomné výbušné prostredie, alebo v blízkosti lekárskych prístrojov alebo zariadení na podporu života. Jednotku nezapínajte v žiadnom lietadle.

Prevádzka tohto zariadenia v obytnom prostredí by mohla spôsobiť rádiové rušenie.

Pri teplotách okolia nad 60 ° C musí byť toto zariadenie inštalované iba na mieste s obmedzeným prístupom.

Slovenian--Esloveno

Prepričajte se, da je napajalni kabel priključen v vtičnico z ozemljitvenim priključkom.

Da bi izpolnili omejitve izpostavljenosti FCC / IC RF, mora biti med katero koli anteno enote in katerim koli delom uporabnika ves čas vzdrževana najmanj 20 cm razdalja.

Ta naprava ne vsebuje nobenih delov, ki bi jih lahko uporabljal uporabnik. Nikoli ne odpirajte opreme. Iz varnostnih razlogov naj opremo odpira samo usposobljeno osebje.

Enoto je treba izklopiti tam, kjer poteka razstreljevanje, kjer so prisotne eksplozivne atmosfere ali v bližini medicinske opreme ali opreme za vzdrževanje življenja. Enote ne vklopite v nobenem letalu.

Delovanje te opreme v stanovanjskem okolju lahko povzroči radijske motnje.

Pri temperaturah okolice nad 60 ° C mora biti ta oprema nameščena samo na lokaciji z omejenim dostopom.

Spanish--Español

Asegúrese de que el cable de alimentación esté conectado a una toma de corriente con conexión a tierra.

Para cumplir con los límites de exposición a RF de la FCC / IC, se debe mantener una distancia de separación de al menos 20 cm entre cualquier antena de la unidad y cualquier parte del usuario en todo momento.

Este aparato no contiene ninguna pieza que pueda reparar el usuario. Nunca abra el equipo. Por razones de seguridad, el equipo debe ser abierto únicamente por personal calificado.

La unidad debe estar apagada donde se estén realizando explosiones, cuando haya atmósferas explosivas o cerca de equipos médicos o de soporte vital. No encienda la unidad en ningún avión.

El funcionamiento de este equipo en un entorno residencial puede provocar interferencias de radio.

Para temperaturas ambiente superiores a 60 ° C, este equipo debe instalarse únicamente en una ubicación de acceso restringido.

Digi IX10 Certifications

You can review certification information for the IX10 on the Digi Certifications page.

International EMC (Electromagnetic Compatibility) and safety standards

This product complies with the requirements of the following Electromagnetic Compatibility standards.

There are no user-serviceable parts inside the product. Contact your Digi representative for repair information.

Certification category	Standards
Electromagnetic Compatibility (EMC) compliance standards	■ EN 300 328 v1.8.1 ■ EN 301 893 v1.7.2 ■ EN 301 489 ■ FCC Part 15 Subpart B Class B
Safety compliance standards	EN 62368 UL 121201, CSA C22.2 No. 213 Hazardous Location designation: SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C AND D
E-UTRA CA, E-UTRA FDD, E-UTRA TDD, UMTS FDD	PTCRB
Cellular carriers	See the current list of carriers on the IX10 datasheet, available on the Digi IX10 Specifications page.
Electrical safety compliance	The IX10 model 50002009-01 shall be powered using a DC power source Approved in its country of use as per ES1 [IEC 62368-1:2014 (Ed.2.0)] or SELV [Safety Extra Low Voltage as per IEC 60950-1:2005(ED 2) + A1, A2.

Command line interface

This chapter contains the following topics:

Access the command line interface 943
Log in to the command line interface 943
Exit the command line interface 944
Execute a command from the web interface 944
Display help for commands and parameters 946
Auto-complete commands and parameters 948
Available commands 949
Use the scp command 950
Display status and statistics using the show command 951
Device configuration using the command line interface 953
Execute configuration commands at the root Admin CLI prompt 953
Configuration mode 955
Command line reference 967

Access the command line interface

You can access the IX10 command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

You can also access the command line interface in the WebUI by using the **Terminal**, or the Digi Remote Manager by using the **Console**.

To access the command line, your device must be configured to allow access, and you must log in as a user who has been configured for the appropriate access.

For further information about configuring access to these services, see:

- Serial: Serial port
- WebUI: Configure the web administration service
- SSH: Configure SSH access
- Telnet: Configure telnet access

Log in to the command line interface

Command line

1. Connect to the IX10 device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See Access the command line interface for more information.

   Note Telnet is not available when Primary Responder mode has been enabled for the device. For information about Primary Responder mode, see Differences between standard firmware operation and Primary Responder mode.

   - For serial connections, the default configuration is:
     - **9600** baud rate
     - **8** data bits
     - **no** parity
     - **1** stop bit
     - **no** flow control
   - For SSH and telnet connections, the Setup IP address of the device is **192.168.210.1** on the .
2. At the login prompt, enter the username and password of a user with Admin access:

   ```
   login: admin
   Password: **********
   ```

   The default username is **admin**. The default unique password for your device is printed on the device label.
3. Depending on the device configuration, you may be presented with another menu, for example:

```
Access selection menu:

   a: Admin CLI
   s: Shell
   q: Quit

Select access or quit [admin] :
```

Type **a** or **admin** to access the IX10 command line.

You will now be connected to the Admin CLI:

```
Connecting now...
 Press Tab to autocomplete commands
 Press '?' for a list of commands and details
 Type 'help' for details on navigating the CLI
 Type 'exit' to disconnect from the Admin CLI

>
```

See Command line interface for detailed instructions on using the command line interface.

Exit the command line interface

Command line

1. At the command prompt, type **exit**.

```
> exit
```

2. Depending on the device configuration, you may be presented with another menu, for example:

```
Access selection menu:

   a: Admin CLI
   s: Shell
   q: Quit

Select access or quit [admin] :
```

Type **q** or **quit** to exit.

Execute a command from the web interface

Log into the IX10 WebUI as a user with full Admin access rights.

1. At the main menu, click **Terminal**. The device console appears.

```
IX10 login:
```

2. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

The Admin CLI prompt appears.

```
>
```

Display help for commands and parameters

The help command

When executed from the root command prompt, **help** displays information about autocomplete operations, how to move the cursor on the IX10 command line, and other keyboard shortcuts:

```
> help

 Commands
 ---------------------------------------------------------------------------
 ?          Show commands help
 <Tab>      Tab completion, displays all valid commands to complete command,
            if only one command is possible, it is used
 <Space>    Like tab except shortest prefix is used if command is valid
 <Enter>    Enter an input. If quoting then a new line is created instead. If
            the input is invalid then characters will be deleted until a
            prefix for a valid command is found.
 Ctrl + A   Move cursor to start of line
 Ctrl + E   Move cursor to end of line
 Ctrl + W   Delete word under cursor until start of line or [\',", ,\,/,.]
 Ctrl + R   If the current input is invalid then characters will be deleted
            until a prefix for a valid command is found.
 Ctrl + left  Jump cursor left until start of line or [\',", ,\,/,.]
 Ctrl + right  Jump cursor right until start of line or [\',", ,\,/,.]

>
```

The question mark (?) command

When executed from the root command prompt, **?** displays available commands:

```
> ?

 Commands
 ---------------------------------------------------------------------------
 config     View and modify the configuration
 exit       Exit the CLI
 analyzer   Analyzer commands.
 cp         Copy a file or directory.
 grep       Grep a file.
 help       Show CLI editing and navigation commands.
 ls         List a directory.
 mkdir      Create a directory.
 modem      Modem commands.
 more       View a file.
 mv         Move a file or directory.
 ping       Ping a host.
 reboot     Reboot the system.
 rm         Remove a file or directory.
 scp        Copy a file or directory over SSH.
 show       Show instance statistics.
 system     System commands.
 tail       Tail a file.
 traceroute  Print the route packets trace to network host.
```

```
update     Update firmware.

>
```

Display help for individual commands

When included with a command name, both **?** and **help** provide further information about the command. For example:

1. To display further information about the **show** command, type either **show ?** or **show help**:

```
> show ?

 Commands
 ------------------------------------------------------------------------

 arp          Show ARP tables
 cloud        Show drm statistics
 config       Show config deltas.
 containers   Show container statistics.
 dhcp-lease   Show DHCP leases.
 dns          Show DNS servers.
 event        Show event list
 ipsec        Show IPsec statistics.
 l2tp         Show L2TP statistics.
 l2tppeth     Show L2TPv3 ethernet statistics.
 location     Show loction information.
 log          Show syslog.
 manufacture  Show manufacturer information.
 modbus-gateway Show modbus gateway status & statistics.
 modem        Show modem statistics.
 mqtt         Show MQTT broker information
 nemo         Show NEMO statistics.
 network      Show network interface statistics.
 ntp          Show NTP information.
 openvpn      Show OpenVPN statistics.
 route        Show IP routing information.
 scep-client  Show SCEP client statistics.
 scripts      Show scheduled scripts.
 serial       Show serial statistics.
 surelink     Show Surelink statistics.
 system       Show system statistics.
 version      Show firmware version.
 vrrp         Show VRRP statistics.
 web-filter   Show web filter information.

> show
```

Use the Tab key or the space bar to display abbreviated help

When executed from the root command prompt, pressing the **Tab** key or the space bar displays an abbreviated list of available commands:

Similar behavior is available with any command name:

```
> config network interface <space>
..          ...          setupip      setuplinklocalip lan
loopback
> config network interface
```

Auto-complete commands and parameters

When entering a command and parameter, press the **Tab** key to cause the command line interface to auto-complete as much of the command and parameter as possible. Typing the space bar has similar behavior. If multiple commands are available that will match the entered text, auto-complete is not performed and the available commands are displayed instead.

Auto-complete applies to these command elements only :

- Command names. For example, typing **net<Tab>** auto-completes the command as **network**.
- Parameter names. For example:
  - **ping *hostname* int<Tab>** auto-completes the parameter as **interface**.
  - **system b<Tab>** auto-completes the parameter as **backup**.
- Parameter values, where the value is one of an enumeration or an on|off type; for example:

  ```
  (config)> serial port1 enable t<Tab>
  ```

  auto-completes to

  ```
  (config)> serial port1 enable true
  ```

Auto-complete does not function for:

- Parameter values that are string types.
- Integer values.
- File names.
- Select parameters passed to commands that perform an action.

Available commands

The following commands are available from the Admin CLI prompt:

Command	Description
config	Used to view and modify the configuration. See Device configuration using the command line interface for more information about using the **config** command.
exit	Exits the CLI.
analyzer	Analyzer commands.
cat	View a file.
clear	Commands to clear the device's status or systems.
container	Create, delete, or interact with a container.
cp	Copies a file or directory.
grep	Grep a file.
help	Displays: ■ CLI editing and navigation commands, when executed from the root of the Admin CLI prompt. ■ Available commands, syntax diagram, and parameter information, when executed in conjunction with another command. See Display help for commands and parameters for information about the **help** command.
ls	Lists the contents of a directory.
mkdir	Creates a directory.
modem	Executes modem commands.
monitoring	Monitoring commands.
more	Displays the contents of a file.
mv	Moves a file or directory.
ping	Pings a remote host using Internet Control Message Protocol (ICMP) Echo Request messages.
poweroff	Powers off the system.
reboot	Reboots the IX10 device.
rm	Removes a file.
scp	Uses the secure copy protocol (SCP) to transfer files between the IX10 device and a

Command	Description
	remote host. See Use the scp command for information about using the **scp** command.
show	Displays information about the device and the device's configuration. See Display status and statistics using the show command for more information about the show command.
iperf	Perform a speedtest.
ssh	SSH login to a remote server.
system	Issues commands related to system functionality.
tail	Tail a file.
telnet	Telnet login to a remote server.
traceroute	Sends and tracks route packets to a destination host.

Note For commands that operate on the IX10's file system, such as the **cp**, **ls**, and **mkdir** commands, see File system for information about the file system, including how to copy, move and delete files and directories.

Use the scp command

The **scp** command uses Secure Copy Protocol (SCP) to transfer files between the IX10 device and a remote host.

Required configuration items

- The hostname or IP address of the remote host.
- The username and password of the user on the remote host.
- Whether the file is being copied to the IX10 device from a remote host, or to the remote host from the IX10 device.
  - If the file is being copied to the IX10 device from a remote host:
    - The path and filename of the file on the remote host that will be copied to the IX10 device.
    - The location on the IX10 device where the file will be copied.
  - If the file is being copied to a remote host from the IX10 device:
    - The path and filename of the file on the IX10 device that will be copied to the remote host.
    - The location on the remote host where the file will be copied.

Copy a file from a remote host to the IX10 device

To copy a file from a remote host to the IX10 device, use the scp command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX10 device.
- *local-path* is the location on the IX10 device where the copied file will be placed.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the /etc/config directory on the IX10 device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/IX10-25.2.bin local /etc/config/scripts to local
admin@192.168.4.1's password: adminpwd
IX10-25.2.bin              100%   36MB   11.1MB/s      00:03
>
```

Transfer a file from the IX10 device to a remote host

To copy a file from the IX10 device to a remote host, use the scp command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX10 device.

For example:

To copy a support report from the IX10 device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

   ```
   > system support-report path /var/log/
   Saving support report to /var/log/support-report-0040D0133536-24-01-12-12:10:00.bin
   Support report saved.
   >
   ```

2. Use the **scp** command to transfer the report to a remote host:

   ```
   > scp host 192.168.4.1 user admin remote /home/admin/temp/ local /var/log/support-report-
   00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
   admin@192.168.4.1's password: adminpwd
   support-report-0040D0133536-24-01-12-12:10:00.bin
   >
   ```

Display status and statistics using the show command

The IX10 **show** command display status and statistics for various features.

For example:

show config

The show config command displays all the configuration settings for the device that have been changed from the default settings. This is a particularly useful when troubleshooting the device.

```
> show config

auth tacacs+ service "login"
auth user admin password "$2a$05$WlJQhquI7BgsytkpobKhaeLPtWraGANBcrlEaJX/wJv63JENW/HOu"
add auth user test
add auth user test group end "admin"
add auth user test group end "serial"
auth user test password "$2a$05$RdGYz1sLKbWrqe6cZjlsd.otg03JZR6n9939XV6EYWUSP0tMAzO5W"
network interface lan ipv4 type "dhcp"
network interface lan zone "external"
network interface modem modem apn 0 apn "00000.000"
network interface modem modem apn_lock "true"
schema version "445"

>
```

show system

The show system command displays system information and statistics for the device, including CPU usage.

```
> show system

  Model               : Digi IX10
  Serial Number       : IX10xxxxxxxyyyyxx
  SKU                 : IX10
  Hostname            : IX10
  MAC Address         : DF:DD:E2:AE:21:18

  Hardware Version    : 50001947-01 1P
  Firmware Version    : 25.2
  Alt. Firmware Version   : 25.2
  Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
  Bootloader Version  : 19.7.23.0-15f936e0ed

  Current Time        : Thu, Jan 11, 2024 12:10:00 +0000
  CPU                 : 1.4%
  Uptime              : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature         : 40C
  Location            :
  Contact             :

>
```

show network

The show network command displays status and statistics for network interfaces.

```
> show network

 Interface       Proto  Status   Address
 --------------- -----  -------  --------------------------------
```

```
setupip       IPv4   up      192.168.210.1/24
setuplinklocalip  IPv4   up      169.254.100.100/16
lan           IPv4   up      192.168.2.1
lan           IPv6   up      0:0:0:0:0:ffff:c0a8:301
loopback        IPv4   up      127.0.0.1/8
wan           IPv4   up      192.168.3.1/24
wan           IPv6   up      fd00:2704::240:ffff:fe80:120/64

>
```

Device configuration using the command line interface

The **config** command allows for device configuration from the command line. All configuration tasks that can be performed by using the WebUI can also be performed by using the **config** command.

There are two ways to invoke the **config** command from the CLI:

- Execute the **config** command and parameters at the root prompt. See Execute configuration commands at the root Admin CLI prompt for more information.
- Enter configuration mode by executing the **config** command without any parameters. See Configuration mode for more information.

Execute configuration commands at the root Admin CLI prompt

You can execute the **config** command at the root Admin CLI prompt with any appropriate parameters. When the **config** command is used in this way, changes to the device's configuration are automatically saved when the command is executed.

For example, to disable the SSH service from the root prompt, enter the following command:

```
> config service ssh enable false
>
```

The IX10 device's ssh service is now disabled.

Note When the **config** command is executed at the root prompt, certain configuration actions that are available in configuration mode cannot be performed. This includes validating configuration changes, canceling and reverting configuration changes, and performing actions on elements in lists. See Configuration mode for information about using configuration mode.

Display help for the config command from the root Admin CLI prompt

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character after the **config** command.

1. For example:

   ```
   > config ?
   ```

   Will display the following help information:

   ```
   > config ?
   ```

```
Additional Configuration
--------------------------------------------------------------------------------
application          Custom scripts
auth                 Authentication
cloud                Central management
firewall             Firewall
monitoring           Monitoring
network              Network
serial               Serial
service              Services
system               System
vpn                  VPN

Run "config" with no arguments to enter the configuration editing mode.

> config
```

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command:

```
> config service ?
Services

Additional Configuration
--------------------------------------------------------------------------------
dns                  DNS
mdns                 Service Discovery (mDNS)
multicast            Multicast
ntp                  NTP
remote_control       Remote control
snmp                 SNMP
ssh                  SSH
telnet               Telnet
web_admin            Web administration

> config service
```

3. Next, display help for the **config service ssh** command:

```
> config service ssh ?

SSH: An SSH server for managing the device.

Parameters           Current Value
--------------------------------------------------------------------------------
enable               true        Enable
key                  [private]   Private key
port                 22          Port

Additional Configuration
--------------------------------------------------------------------------------
```

```
acl             Access control list
mdns

> config service ssh
```

4. Lastly, display the allowed values and other information for the **enable** parameter:

```
> config service ssh enable ?

Enable: Enable the service.
Format: true, false, yes, no, 1, 0
Default value: true
Current value: true

> config service ssh enable
```

Configuration mode

Configuration mode allows you to perform multiple configuration tasks and validate the changes prior to saving them. You can cancel all changes without saving them at any time. Configuration changes do not take effect until the configuration is saved.

Enable configuration mode

To enable configuration mode, at the root prompt, enter the **config** command without any parameters:

```
> config
(config)>
```

When the command line is in configuration mode, the prompt will change to include **(config)**, to indicate that you are currently in configuration mode.

Enter configuration commands in configuration mode

There are two ways to enter configuration commands while in configuration mode:

- Enter the full command string from the config prompt.

  For example, to disable the ssh service by entering the full command string at the config prompt:

  ```
  (config)> service ssh enable false
  (config)>
  ```

- Execute commands by moving through the configuration schema.

  For example, to disable the ssh service by moving through the configuration and then executing the **enable false** command:

  1. At the **config** prompt, enter **service** to move to the **service** node:

     ```
     (config)> service
     (config service)>
     ```

2. Enter **ssh** to move to the **ssh** node:

```
(config service)> ssh
(config service ssh)>
```

3. Enter **enable false** to disable the **ssh** service:

```
(config service ssh)> enable false
(config service ssh)>
```

See Move within the configuration schema for more information about moving within the configuration.

Save changes and exit configuration mode

To save changes that you have made to the configuration while in configuration mode, use **save**. The save command automatically validates the configuration changes; the configuration will not be saved if it is not valid. Note that you can also validate configuration changes at any time while in configuration mode by using the **validate** command.

```
(config)> save
Configuration saved.
>
```

After using **save** to save changes to the configuration, you will automatically exit configuration mode. To return to configuration mode, type **config** again.

Exit configuration mode without saving changes

You can discard any unsaved configuration changes and exit configuration mode by using the **cancel** command:

```
(config)> cancel
>
```

After using **cancel** to discard unsaved changes to the configuration, you will automatically exit configuration mode.

Configuration actions

In configuration mode, configuration actions are available to perform tasks related to saving or canceling the configuration changes, and to manage items and elements in lists. The commands can be listed by entering a question mark (**?**) at the **config** prompt.

The following actions are available:

Configuration actions	Description
cancel	Discards unsaved configuration changes and exits configuration mode.
save	Saves configuration changes and exits configuration mode.

Configuration actions	Description
validate	Validates configuration changes.
revert	Reverts the configuration to default settings. See The revert command for more information.
show	Displays configuration settings.
add	Adds a named element, or an element in a list. See Manage elements in lists for information about using the **add** command with lists.
del	Deletes a named element, or an element in a list. See Manage elements in lists for information about using the **del** command with lists.
move	Moves elements in a list. See Manage elements in lists for information about using the **move** command with lists.

Display command line help in configuration mode

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character at the **config** prompt. For example:

1. Enter **?** at the **config** prompt:

```
(config)> ?
```

This will display the following help information:

```
(config)> ?

 Additional Configuration
 ------------------------------------------------------------------------------
application          Custom scripts
auth               Authentication
cloud               Central management
firewall            Firewall
monitoring             Monitoring
network              Network
serial             Serial
service              Services
system               System
vpn                VPN

(config)>
```

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command, use one of the following methods:

- At the **config** prompt, enter **service ?**:

```
(config)> service ?
```

- At the **config** prompt:
  a. Enter **service** to move to the **service** node:

```
(config)> service
(config service)>
```

  b. Enter **?** to display help for the **service** node:

```
(config service)> ?
```

Either of these methods will display the following information:

```
config> service ?

Services

 Additional Configuration
 ------------------------------------------------------------------------------
dns                DNS
mdns               Service Discovery (mDNS)
multicast          Multicast
ntp                NTP
remote_control     Remote control
snmp               SNMP
ssh                SSH
telnet             Telnet
web_admin          Web administration

(config)> service
```

3. Next, to display help for the **service ssh** command, use one of the following methods:
   - At the **config** prompt, enter **service ssh ?**:

```
(config)> service ssh ?
```

   - At the **config** prompt:
     a. Enter **service** to move to the **service** node:

```
(config)> service
(config service)>
```

     b. Enter **ssh** to move to the **ssh** node:

```
(config service)> ssh
(config service ssh)>
```

     c. Enter **?** to display help for the **ssh** node:

```
(config service ssh)> ?
```

Either of these methods will display the following information:

```
(config)> service ssh ?

SSH: An SSH server for managing the device.

 Parameters            Current Value
 ------------------------------------------------------------------------------
 enable                  true        Enable
 key                   [private]     Private key
 port                  22            Port

 Additional Configuration
 ------------------------------------------------------------------------------
 acl                   Access control list
 mdns

(config)> service ssh
```

4. Lastly, to display allowed values and other information for the **enable** parameter, use one of the following methods:
   - At the **config** prompt, enter **service ssh enable ?**:

     ```
     (config)> service ssh enable ?
     ```

   - At the **config** prompt:
     a. Enter **service** to move to the **service** node:

        ```
        (config)> service
        (config service)>
        ```

     b. Enter **ssh** to move to the **ssh** node:

        ```
        (config service)> ssh
        (config service ssh)>
        ```

     c. Enter **enable ?** to display help for the **enable** parameter:

        ```
        (config service ssh)> enable ?
        (config service ssh)>
        ```

Either of these methods will display the following information:

```
(config)> service ssh enable ?

Enable: Enable the service.
Format: true, false, yes, no, 1, 0
Default value: true
Current value: true

(config)> service ssh enable
```

Move within the configuration schema

You can perform configuration tasks at the CLI by moving within the configuration.

- Move forward one node in the configuration by entering the name of an Additional Configuration option:
  1. At the **config** prompt, type **service** to move to the **service** node:

     ```
     (config)> service
     (config service)>
     ```

  2. Type **ssh** to move to the **ssh** node:

     ```
     (config service)> ssh
     (config service ssh)>
     ```

  3. Type **acl** to move to the **acl** node:

     ```
     (config service ssh)> acl
     (config service ssh acl)>
     ```

  4. Type **zone** to move to the **zone** node:

     ```
     (config service ssh acl)> zone
     (config service ssh acl zone)>
     ```

  You can also enter multiple nodes at once to move multiple steps in the configuration:

  ```
  (config)> service ssh acl zone
  (config service ssh acl zone)>
  ```

- Move backward one node in the configuration by entering two periods (**..**):

  ```
  (config service ssh acl zone)> ..
  (config service ssh acl)>
  ```

  You can also move back multiples nodes in the configuration by typing multiple sets of two periods:

  ```
  (config service ssh acl zone)> .. .. ..
  (config service)>
  ```

- Move to the root of the config prompt from anywhere within the configuration by entering three periods (**...**):

  ```
  (config service ssh acl zone)> ...
  (config)>
  ```

Manage elements in lists

While in configuration mode, you can use the **add**, **del**, and **move** action commands to manage elements in a list. When working with lists, these actions require an index number to identify the list item that will be acted on.

Add elements to a list

When used with parameters that contains lists of elements, the **add** command is used to add an element to the list.

For example, to add an authentication method:

1. Display current authentication method by using the **show** command:

```
(config)> show auth method
0 local
(config)>
```

2. Add an authentication method by using the **add** ***index_item*** command. For example:
   - To add the TACACS+ authentication method to the beginning of the list, use the index number **0**:

```
(config)> add auth method 0 tacacs+
(config)> show auth method
0 tacacs+
1 local
(config)>
```

   - To add the TACACS+ authentication method to the end of the list, use the **end** keyword:

```
(config)> add auth method end tacacs+
(config)> show auth method
0 local
1 tacacs+
(config)>
```

The end keyword

As demonstrated above, the **end** keyword is used to add an element to the end of a list. Additionally, the **end** keyword is used to add an element to a list that does not have any elements.

For example, to add an authentication group to a user that has just been created:

1. Use the **show** command to verify that the user is not currently a member of any groups:

```
(config)> show auth user new-user group
(config)>
```

2. Use the **end** keyword to add the admin group to the user's configuration:

```
(config)> add auth user new-user group end admin
(config)>
```

3. Use the **show** command again to verify that the admin group has been added to the user's configuration:

```
(config)> show auth user new-user group
0 admin
(config)>
```

Delete elements from a list

When used with parameters that contains lists of elements, the **del** command is used to delete an element in the list.

For example, to delete an authentication method:

1. Use the **show** command to display current authentication method configuration:

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

2. Delete one of the authentication methods by using the **del *index_number*** command. For example:
   a. To delete the local authentication method, use the index number **0**:

```
(config)> del auth method 0
(config)>
```

   b. Use the **show** command to verify that the local authentication method was removed:

```
(config)> show auth method
0 tacacs+
1 radius
(config)>
```

Move elements within a list

Use the **move** command to reorder elements in a list.

For example, to reorder the authentication methods:

1. Use the **show** command to display current authentication method configuration:

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

2. To configure the device to use TACACS+ authentication first to authenticate a user, use the **move *index_number_1 index_number_2*** command:

```
(config)> move auth method 1 0
(config)>
```

3. Use the **show** command again to verify the change:

```
(config)> show auth method
0 tacacs+
1 local
2 radius
(config)>
```

The revert command

The **revert** command is used to revert changes to the IX10 device's configuration and restore default configuration settings. The behavior of the revert command varies depending on where in the configuration hierarchy the command is executed, and whether the optional **path** parameter is used. After executing the revert command, you must save the configuration changes by using the **save** command. You can also discard the configuration changes by using the **cancel** command.

CAUTION! The **revert** command reverts all changes to the default configuration, not only unsaved changes.

Revert all configuration changes to default settings

To discard all configuration changes and revert to default settings, use the **revert** command at the config prompt without the optional **path** parameter:

1. At the config prompt, enter **revert**:

```
(config)> revert
(config)>
```

2. Set the password for the admin user prior to saving the changes:

```
(config)> auth user admin password pwd
(config)>
```

3. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

4. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Revert a subset of configuration changes to the default settings

There are two methods to revert a subset of configuration changes to the default settings.

- Enter the **revert** command with the **path** parameter. For example, to revert all changes to the authentication methods configuration:
  1. Enter the **revert** command with the **path** set to **auth method**:

```
(config)> revert auth method
(config)>
```

  2. Save the configuration and apply the change.

```
(config)> save
Configuration saved.
>
```

3. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

- Move to the location in the configuration and enter the **revert** command without the **path** parameter. For example:
  1. Change to the auth method node:

     ```
     (config)> auth method
     (config auth method)>
     ```

  2. Enter the **revert** command:

     ```
     (config auth method)> revert
     (config auth method)>
     ```

  3. Save the configuration and apply the change.

     ```
     (config auth method)> save
     Configuration saved.
     >
     ```

  4. Type **exit** to exit the Admin CLI.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

- You can also use a combination of both of these methods:
  1. Change to the **auth** node:

     ```
     (config)> auth
     (config auth)>
     ```

  2. Enter the **revert** command with the **path** set to **method**:

     ```
     (config auth)> revert method
     (config auth)>
     ```

  3. Save the configuration and apply the change.

     ```
     (config auth)> save
     Configuration saved.
     >
     ```

  4. Type **exit** to exit the Admin CLI.

     Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enter strings in configuration commands

For string parameters, if the string value contains a space, the value must be enclosed in quotation marks. For example, to assign a descriptive name for the device using the **system** command, enter:

```
(config)> system description "Digi IX10"
```

Example: Create a new user by using the command line

In this example, you will use the IX10 command line to create a new user, provide a password for the user, and assign the user to authentication groups.

1. Select the device in Remote Manager and click **Actions** > **Open Console**, or log into the IX10 local command line as a user with full Admin access rights.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, create a new user with the username **user1**:
   - Method one: Create a user at the root of the config prompt:

```
(config)> add auth user user1
(config auth user user1)>
```

   - Method two: Create a user by moving through the configuration:
     a. At the config prompt, enter **auth** to move to the **auth** node:

```
(config)> auth
(config auth)>
```

     b. Enter **user** to move to the **user** node:

```
(config auth)> user
(config auth user)>
```

     c. Create a new user with the username **user1**:

```
(config auth user)> add user1
(config auth user user1)>
```

4. Configure a password for the user:

```
(config auth user user1)> password pwd1
(config auth user user1)>
```

5. List available authentication groups:

```
(config auth user user1)> show .. .. group

admin
  acl
    admin
      enable true
    nagios
      enable false
    openvpn
      enable false
```

```
        no tunnels
      portal
        enable false
        no portals
      serial
        enable false
        no ports
      shell
        enable false

  serial
    acl
      admin
        enable true
      nagios
        enable false
      openvpn
        enable false
        no tunnels
      portal
        enable false
        no portals
      serial
        enable true
          ports
            0 port1
      shell
        enable false
(config auth user user1)>
```

6. Add the user to the admin group:

```
(config auth user user1)> add group end admin
(config auth user user1)>
```

7. Save the configuration and apply the change.

```
(config auth user user1)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Command line reference

ain calibrate

Measure current value of analog input, and set it as zero offset.

Syntax

```
ain calibrate <name> <type> <setpoint>
```

Parameters

name: Name of the analog input.

type: Calibrate low or high-end of analog input range.

setpoint: Reference voltage/current connected on the analog input (in mV/uA). (Minimum: 0)

ain calibration-reset

Reset both voltage and current calibration of analog input.

Syntax

```
ain calibration-reset <name>
```

Parameters

name: Name of the analog input.

analyzer clear

Clears the traffic captured by the analyzer.

Syntax

```
analyzer clear <name>
```

Parameters

name: Name of the capture filter to use.

analyzer save

Saves the current captured traffic to a file.

Syntax

```
analyzer save <name> <path>
```

Parameters

name: Name of the capture filter to use.

path: The path and filename to save captured traffic to. If a relative path is provided, /etc/config/analyzer will be used as the root directory for the path and file.

analyzer start

Start a capture session of packets on this devices interfaces.

Syntax

```
analyzer start <name>
```

Parameters

name: Name of the capture filter to use.

analyzer stop

Stops the traffic capture session.

Syntax

```
analyzer stop <name>
```

Parameters

name: Name of the capture filter to use.

cat

View the contents of a file.

Syntax

```
cat <path>
```

Parameters

path: The file to view.

clear dhcp-lease ip-address

Clear the DHCP lease for the specified IP address.

Syntax

```
clear dhcp-lease ip-address <address>
```

Parameters

address: An IPv4 or IPv6 address.

clear dhcp-lease mac

Clear the DHCP lease for the specified MAC address.

Syntax

```
clear dhcp-lease mac ADDRESS
```

Parameters

address: 12-digit, colon-delimited MAC address [00:11:22:AA:BB:CC]

container create

Create a LXC container from a given image. This process creates a copy of the image, so the orginal image may be deleted after creating the container without breaking the container.

Syntax

```
container create <path>
```

Parameters

path: Filepath for container image to be created. .

container delete

Delete a LXC container. This will remove the LXC container configuration and the container image.

Syntax

```
container delete <container>
```

Parameters

container: Filepath for container image to be deleted. This process also removes any associated configuration.

cp

Copy a file or directory.

Syntax

```
cp <source> <destination> [force]
```

Parameters

source: The source file or directory to copy.

destination: The destination path to copy the source file or directory to.

force: Do not ask to overwrite the destination file if it exists.

dio state

Set digital I/O.

Syntax

```
dio state <name> <state>
```

Parameters

name: Name of the digital I/O.

state: State of the digital I/O.

grep

Grep the contents of a file.

Syntax

```
grep <match> <path>
```

Parameters

match: Output all lines in file matching string.
path: The file to grep.

help

Show CLI editing and navigation commands.

Syntax

```
help
```

Parameters

None

ls

List a directory.

Syntax

ls <path> [*show-hidden*]

Parameters

path: List files and directories under this path.

show-hidden: Show hidden files and directories. Hidden filenames begin with '.'.

mkdir

Create a directory. Parent directories are created as needed.

Syntax

```
mkdir <path>
```

Parameters

path: The directory path to create.

modem at

Send an AT command to the modem and display the response.

Syntax

```
modem at <cmd> [name STRING] [imei STRING]
```

Parameters

cmd: The AT command string.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem at-interactive

Start an AT command session on the modem's AT serial port.

Syntax

```
modem at-interactive [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem firmware bundle ota check

Query the Digi firmware server for the latest remote modem firmware version.

Syntax

```
modem firmware bundle ota check [name STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

modem firmware bundle ota download

Downloads modem firmware from the server. The firmware will be downloaded on the device but the modem won't be updated.

Syntax

modem firmware bundle ota download [*name* STRING] [*version* STRING] [*binary* STRING]

Parameters

name: The configured name of the modem to execute this CLI command on.

version: Firmware version name.

binary: Firmware binary position.

modem firmware bundle ota list

Query the Digi firmware server for a list of modem firmware versions.

Syntax

modem firmware bundle ota list [*name* STRING]

Parameters

name: The configured name of the modem to execute this CLI command on.

modem firmware bundle ota update

Perform FOTA (firmware-over-the-air) update. The modem will be updated to the latest modem firmware image unless a specific firmware version is specified.

Syntax

modem firmware bundle ota update [*name* STRING] [*version* STRING]

Parameters

name: The configured name of the modem to execute this CLI command on.

version: Firmware version name.

modem firmware check

Inspect /opt/[MODEM_MODEL]/Custom_Firmware/ directory for new modem firmware file.

Syntax

modem firmware check [*name* STRING] [*imei* STRING]

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem firmware list

List modem firmware files found in the /opt/[MODEM_MODEL]/ directory.

Syntax

```
modem firmware list [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem firmware ota check

Query the Digi firmware server for the latest remote modem firmware version.

Syntax

```
modem firmware ota check [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem firmware ota download

Downloads modem firmware from the server. The firmware will be downloaded on the device but the modem won't be updated.

Syntax

```
modem firmware ota download [name STRING] [imei STRING] [version STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

version: Firmware version name.

modem firmware ota list

Query the Digi firmware server for a list of modem firmware versions.

Syntax

```
modem firmware ota list [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem firmware ota update

Perform FOTA (firmware-over-the-air) update. The modem will be updated to the latest modem firmware image unless a specific firmware version is specified.

Syntax

```
modem firmware ota update [name STRING] [imei STRING] [version STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

version: Firmware version name.

modem firmware update

Update modem firmware using local firmware file. The modem will be updated to the firmware specified in the /opt/[MODEM_MODEL]/Custom_Firmware/ directory unless a specific firmware version is specified.

Syntax

```
modem firmware update [name STRING] [imei STRING] [version STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

version: Firmware version name.

modem pin change

Change the SIM's PIN code.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin change <old-pin> <new-pin> [name STRING] [imei STRING]
```

Parameters

old-pin: The SIM's PIN code.

new-pin: The PIN code to change to.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem pin disable

Disable the PIN lock on the SIM card that is active in the modem.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin disable <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem pin enable

Enable the PIN lock on the SIM card that is active in the modem. The SIM card will need to be unlocked before each use.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin enable <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem pin status

Print the PIN lock status and the number of PIN enable/disable/unlock attempts remaining. The SIM will be PUK locked when there are no remaining retries.

Syntax

```
modem pin status [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem pin unlock

Temporarily unlock the SIM card with a PIN code. Set the PIN field in the modem interface's configuration to unlock the SIM card automatically before use.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin unlock <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem puk status

Print the PUK status and the number of PUK unlock attempts remaining.

Syntax

```
modem puk status [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem puk unlock

Unlock the SIM with a PUK code from the SIM provider.

Syntax

```
modem puk unlock <puk> <new-pin> [name STRING] [imei STRING]
```

Parameters

puk: The SIM's PUK code.

new-pin: The PIN code to change to.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem reset

Reset the modem hardware (reboot it). This can be useful if the modem has stopped responding to the network or is behaving inconsistently.

Syntax

```
modem reset [name STRING] [imei STRING]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

modem scan

List of carriers present in the network.

Syntax

```
modem scan [name STRING] [imei STRING] [timeout INTEGER]
```

Parameters

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

timeout: The amount of time in seconds to wait for modem scan to complete. (Default: 300)

modem sim-slot

Show or change the modem's active SIM slot. This applies only to modems with multiple SIM slots.

Syntax

```
modem sim-slot <slot> [name STRING] [imei STRING]
```

Parameters

slot: The SIM slot to change to.
name: The configured name of the modem to execute this CLI command on.
imei: The IMEI of the modem to execute this CLI command on.

modem sms send

Send an SMS message to the provided phone number (MSISDN).

Syntax

```
modem sms send <msisdn> <message> [name STRING] [imei STRING]
```

Parameters

msisdn: Destination phone number (MSISDN).
message: Message to send.
name: The configured name of the modem to execute this CLI command on.
imei: The IMEI of the modem to execute this CLI command on.

modem sms send-binary

Send a binary SMS message to the provided phone number (MSISDN).

Syntax

```
modem sms send-binary <msisdn> <message> [name STRING] [imei STRING]
```

Parameters

msisdn: Destination phone number (MSISDN).
message: Message to send.
name: The configured name of the modem to execute this CLI command on.
imei: The IMEI of the modem to execute this CLI command on.

monitoring metrics upload

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

Syntax

```
monitoring metrics upload
```

Parameters

None

monitoring

Commands to clear the device's status or systems.

monitoring metrics

Device metrics commands.

uplaod

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

Parameters

None

monitoring metrics upload

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

Syntax

```
monitoring metrics upload
```

Parameters

None

more

View a file.

Syntax

```
more <path>
```

Parameters

path: The file to view.

mv

Move a file or directory.

Syntax

```
mv <source> <destination> [force]
```

Parameters

source: The source file or directory to move.
destination: The destination path to move the source file or directory to.
force: Do not ask to overwrite the destination file if it exists.

ping

Ping a host using ICMP echo.

Syntax

```
ping <host> [interface STRING] [source STRING] [ipv6] [size INTEGER] [count INTEGER] [broadcast]
```

Parameters

host: The name or address of the remote host to send ICMP ping requests to. If broadcast is enabled, can be the broadcast address.

interface: The network interface to send ping packets from when the host is reachable over a default route. If not specified, the system's primary default route will be used.

source: The ping command will send a packet with the source address set to the IP address of this interface, rather than the address of the interface the packet is sent from.

ipv6: If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

size: The number of bytes sent in the ICMP ping request. (Minimum: 0, Default: 56)

count: The number of ICMP ping requests to send before terminating. (Minimum: 1, Default: 100)

broadcast: Enable broadcast ping functionality.

poweroff

Power off the system.

Syntax

```
poweroff
```

Parameters

None

pyinstall

Pyinstall commands.

Syntax

```
pyinstall <package>
```

Parameters

package: Path and filename of the package to install (.zip, .whl).

reboot

Reboot the system.

Parameters

None

rm

Remove a file or directory.

Syntax

```
rm <path> [force]
```

Parameters

path: The path to remove.

force: Force the file to be removed without asking.

scp

Copy a file or directory over SSH.

Syntax

```
scp <local> <remote> <host> <user> <to> [port INTEGER]
```

Parameters

local: The path and name of the file on the local device to copy to or from.

remote: The path and name of the file on the remote host to copy to or from.

host: The hostname or IP address of the remote host.

user: The username to use when connecting to the remote host.

to: Determine whether to copy the file from the local device to the remote host, or from the remote host to the local device.

port: The SSH port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 22)

config directory: show command

Show a summary of changes made to the default configuration in a format that can be copied and pasted.

Note This same information can be displayed using the show config command, but the display is not suitable for copying and pasting.

Syntax

```
> config
(config)> show
```

Parameters

None

show ain

Show analog input status.

Syntax

```
show ain [name STRING]
```

Parameters

name: Name of the analog input.

show analyzer

Show packets from a specified analyzer capture.

Syntax

```
show analyzer <name>
```

Parameters

name: Name of the capture filter to use.

show arp

Show ARP tables. If no IP version is specified IPv4 & IPV6 will be displayed.

Syntax

```
show arp [ipv4] [ipv6] [verbose]
```

Parameters

ipv4: Display IPv4 routes. If no IP version is specified IPv4 & IPV6 will be displayed.

ipv6: Display IPv6 routes. If no IP version is specified IPv4 & IPV6 will be displayed.

verbose: Display more information (less concise, more detail).

show bluetooth-scanner log

Show the Bluetooth scanner output log.

Syntax

```
show bluetooth-scanner log
```

Parameters

None

show bluetooth-scanner nearby

Show Bluetooth devices detected during the most recent update interval.

Syntax

```
show bluetooth-scanner nearby
```

Parameters

None

show bluetooth-scanner static-candidate

Show Bluetooth devices detected during the most recent observation period but not evaluated as static.

Syntax

```
show bluetooth-scanner static-candidate
```

Parameters

None

show bluetooth-scanner static-confirmed

Show Bluetooth devices that have been evaluated as static.

Syntax

```
show bluetooth-scanner static-confirmed
```

Parameters

None

show cloud

Show drm status & statistics.

Syntax

```
show cloud
```

Parameters

None

show config

Show a summary of changes made to the default configuration. The changes shown are not suitable for pasting into a CLI session.

Syntax

```
show config [cli_format]
```

Parameters

cli_format: Show the exact CLI commands required to configure the device from a default configuration. The changes shown are suitable for pasting into a CLI session, although individual output lines maybe context sensitive and unable to be entered in isolation.

show containers

Show container status & statistics.

Syntax

```
show containers [container STRING]
```

Parameters

container: Display more details and config data for a specific container.

show dhcp-lease

Show DHCP leases.

Syntax

```
show dhcp-lease [all] [verbose]
```

Parameters
all: Show all leases (active and inactive (not in etc/config/dhcp.*lease)).
verbose: Display more information (less concise, more detail).

show dio

Show digital I/O status.

Syntax

show dio [*name* STRING]

Parameters
name: Name of the digital I/O.

show dns

Show DNS servers and associated domains.

Syntax

show dns

Parameters
None

show eth

Show ethernet status & statistics.

Syntax

show eth [*name* STRING]

Parameters
name: Display more details and configuration data for a specific ethernet instance.

show event

Show event list (high level).

Syntax

show event [*table* <status|error|info>] [*number* INTEGER]

Parameters
table: Type of event log to be displayed (status, error, info).
number: Number of lines to retrieve from log. (Minimum: 1, Default: 20)

show hotspot

Show hotspot statistics.

Syntax

show hotspot [*name* STRING] [*ip* STRING]

Parameters
name: The configured instance name of the hotspot.
ip: IP address of a specific client, to limit the status display to only this client.

show ipsec

Show IPsec status & statistics.

Syntax

show ipsec [*tunnel* STRING] [*all*] [*verbose*]

Parameters
tunnel: Display more details and config data for a specific IPsec tunnel.
all: Display all tunnels including disabled tunnels.
verbose: Display status of one or all tunnels in plain text.

show l2tp lac

Show L2TP access concentrator status & statistics.

Syntax

show l2tp lac [*name* STRING]

Parameters
name: Display more details for a specific L2TP access concentrator.

show l2tp lns

Show L2TP network server status & statistics.

Syntax

show l2tp lns [*name* STRING]

Parameters
name: Display more details for a specific L2TP network server.

show l2tpeth

Show L2TPv3 ethernet tunnel session status and statistics.

Syntax

```
show l2tpeth [name STRING]
```

Parameters

name: Display more details for a specific L2TPv3 ethernet tunnel session.

show location

Show location information.

Syntax

```
show location [geofence]
```

Parameters

geofence: Show geofence information.

show log

Show system log (low level).

Syntax

```
show log [number INTEGER] [filter <critical|warning|debug|info>]
```

Parameters

number: Number of lines to retrieve from log. (Minimum: 1, Default: 20)

filter: Filters for type of log message displayed (critical, warning, info, debug). Note, filters from the number of messages retrieved not the whole log (this can be very time consuming). If you require more messages of the filtered type, increase the number of messages retrieved using 'number'.

show manufacture

Show manufacturer information.

Syntax

```
show manufacture [verbose]
```

Parameters

verbose: Display more information (less concise, more detail).

show modbus-gateway

Show modbus gateway status & statistics.

Syntax

```
show modbus-gateway [verbose]
```

Parameters
verbose: Display more information (less concise, more detail).

show modem

Show modem status & statistics.

Syntax

show modem [*name* STRING] [*imei* STRING] [*verbose*]

Parameters
name: The configured name of the modem to execute this CLI command on.
imei: The IMEI of the modem to execute this CLI command on.
verbose: Display more information (less concise, more detail).

show mqtt

Show MQTT broker information.

Syntax

show mqtt [*verbose*]

Parameters
verbose: Display more information (less concise, more detail).

show nemo

Show NEMO status and statistics.

Syntax

show nemo [*name* STRING]

Parameters
name: Display more details and configuration data for a specific NEMO instance.

show network

Show network interface status & statistics.

Syntax

show network [*interface* STRING] [*all*] [*verbose*]

Parameters
interface: Display more details and config data for a specific network interface.
all: Display all interfaces including disabled interfaces.
verbose: Display more information (less concise, more detail).

show ntp

Show NTP status & statistics.

Syntax

```
show ntp
```

Parameters

None

show openvpn client

Show OpenVPN client status & statistics.

Syntax

```
show openvpn client [name STRING] [all]
```

Parameters

name: Display more details and config data for a specific OpenVPN client.
all: Display all clients including disabled clients.

show openvpn server

Show OpenVPN server status & statistics.

Syntax

```
show openvpn server [name STRING] [all]
```

Parameters

name: Display more details and config data for a specific OpenVPN server.
all: Display all servers including disabled servers.

show route

Show IP routing information.

Syntax

```
show route [ipv4] [ipv6] [verbose]
```

Parameters

ipv4: Display IPv4 routes.
ipv6: Display IPv6 routes.
verbose: Display more information (less concise, more detail).

show scep-client

Show SCEP client status and statistics.

Syntax

```
show scep-client [name STRING]
```

Parameters

name: Display more details and configuration data for a specific SCEP client instance.

show scripts

Show scheduled system scripts.

Syntax

```
show scripts
```

Parameters

None

show serial

Show serial status and statistics.
If the

Syntax

```
show serial [port STRING]
```

Parameters

port: Display more details and configuration data for a specific serial port.

show surelink interface

Show SureLink status & statistics for network interfaces.

Syntax

```
show surelink interface [name STRING] [all]
```

Parameters

name: The name of a specific network interface.
all: Show all network interfaces.

show surelink ipsec

Show SureLink status & statistics for IPsec tunnels.

Syntax

```
show surelink ipsec [tunnel STRING] [all]
```

Parameters
tunnel: The name of a specific IPsec tunnel.
all: Show all IPsec tunnels.

show surelink openvpn

Show SureLink status & statistics for OpenVPN clients.

Syntax

show surelink openvpn [*client* STRING] [*all*]

Parameters
client: The name of the OpenVPN client.
all: Show all OpenVPN clients.

show surelink state

Show SureLink state & fail counts for each network interfaces.

Syntax

show surelink state

Parameters
None

show system

Show system status & statistics.

Syntax

show system [*verbose*]

Parameters
verbose: Display more information (disk usage, etc).

show version

Show firmware version.

Syntax

show version [*verbose*]

Parameters
verbose: Display more information (build date).

show vrrp

Show VRRP status & statistics.

Syntax

show vrrp [*name* STRING] [*all*] [*verbose*]

Parameters

name: Display more details and config data for a specific VRRP instance.

all: Display all VRRP instances including disabled instances.

verbose: Display all VRRP status and statistics including disabled instances.

show web-filter

Show web filter status & statistics.

Syntax

show web-filter

Parameters

None

iperf

Perform a speedtest to a remote host using nuttcp or iPerf. The system's primary default route will be used. The speed test will take approximately 30 seconds to complete.

Syntax

iperf <host> [*size* INTEGER] [*mode* <nuttcp|iperf>] [*output* <text|json>]

Parameters

host: The name or address of the remote speed test host/server.

size: The number of kilobytes sent in the speed test packets. (Minimum: 0, Default: 1000)

mode: The type of speed test protocol to run. (Default: nuttcp)

output: The format of output to display the speed test results as. (Default: text)

ssh

Use SSH protocol to log into a remote server.

Syntax

ssh <host> <user> [*port* INTEGER] [*command* STRING]

Parameters

host: The hostname or IP address of the remote host.

user: The username to use when connecting to the remote host.

port: The SSH port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 22)

command: The command that will be automatically executed once the SSH session to the remote host is established.

system backup

CAUTION! This CLI command is obsolete in DAL OS firmware 24.12.x and newer versions. Use the **system custom-default-config** command.

Save the device's configuration to a file. Archives are full backups including generated SSH keys and dynamic DHCP lease information. Command backups are a list of CLI commands required to build the device's configuration.

Syntax

```
system backup [type <custom-defaults|cli-config|archive>] [path STRING] [passphrase STRING] [remove <custom-defaults>]
```

Parameters

type: The type of backup file to create. Archives are full backups including generated SSH keys and dynamic DHCP lease information. CLI configuration backups are a list of CLI commands used to build the device's configuration. (Default: archive)

path: The file path to save the backup to. (Default: /var/log/)

passphrase: Encrypt the archive with a passphrase.

remove: Remove a backup file.

system cloud register

Register with Digi Remote Manager account.

Syntax

```
system cloud register <username> <password> [group STRING]
```

Parameters

username: Digi Remote Manager username.

password: Digi Remote Manager password.

group: Group to add device in Digi Remote Manager.

system custom-default-config current

Install the current configuration as a custom-default-config.bin file and generates the SHA file.

Syntax

```
system custom-default-config current
```

Parameters

None

system custom-default-config file

Sets up a backup file as a custom-default-config.bin file and generates the SHA file.

Syntax

```
system custom-default-config file <path>
```

Parameters

path: Backup file to set up as a custom-default-config.bin file.

system custom-default-config remove

Removes the current custom-default-config.bin and SHA file.

Syntax

```
system custom-default-config remove
```

Parameters

None

system disable-cryptography

Erase the device's configuration and reboot into a limited mode with no cryptography available. The device's shell will be accessible over Telnet (port 23) at IP address 192.168.210.1. To return the device to normal operation, perform the configuration erase procedure with the device's ERASE button twice consecutively.

Syntax

```
system disable-cryptography
```

Parameters

None

system duplicate-firmware

Duplicate the running firmware to the alternate partition so that the device will always boot the same firmware version.

Syntax

```
system duplicate-firmware
```

Parameters

None

system factory-erase

Erase the device to restore to factory defaults. All configuration and automatically generated keys will be erased.

Syntax

```
system factory-erase
```

Parameters

None

system find-me

Find Me function to flash LEDs on this device to help users locate the unit.

Syntax

```
system find-me <state>
```

Parameters

state: Find Me control to flash cellular-related LEDs.

system firmware ota check

Query the Digi firmware server for the latest device firmware version.

Syntax

```
system firmware ota check
```

Parameters

None

system firmware ota list

Query the Digi firmware server for a list of device firmware versions.

Syntax

```
system firmware ota list
```

Parameters

None

system firmware ota update

Perform FOTA (firmware-over-the-air) update. The device will be updated to the latest firmware version unless the version argument is used to specify the firmware version.

Syntax

```
system firmware ota update [version STRING]
```

Parameters

version: Firmware version name.

system firmware update

Update the current firmware image. Upon reboot the new firmware will be run.

Syntax

```
system firmware update <file>
```

Parameters

file: Firmware filename and path.

system power ignition off_delay

Update the current ignition off delay without changing the configuration.

Syntax

```
system power ignition off_delay <off_delay>
```

Parameters

off_delay: Ignition power off delay. Format: number{h|m|s}, Max: 18h. (Minimum: 0s, Maximum: 18h)

system restore

Restore the device's configuration from a backup archive or CLI commands file.

Syntax

```
system restore <path> [passphrase STRING]
```

Parameters

path: The path to the backup file.

passphrase: Decrypt the archive with a passphrase.

system script start

Run a manual script. Scripts that are disabled, not a manual script, or already running can not be run.

Syntax

```
system script start <script>
```

Parameters

script: Script to start.

system script stop

Stop an active running script. Scripts scheduled to run again will still run again (disable a script to prevent it from running again).

Syntax

```
system script stop <script>
```

Parameters

script: Script to stop.

system serial clear

Clears the serial log.

Syntax

```
system serial clear <port>
```

Parameters

port: Serial port.

system serial copy

Copy serial settings from a port to a list of ports.

Syntax

```
system serial copy <source> <destination> [all] [label] [base] [serial] [session] [monitor] [service] [hangup]
[autoconnect] [framing] [modem] [ppp_dialin] [udp] [logging]
```

Parameters

source: The serial port to copy settings from.
destination: A list of serial ports to copy settings to. Example: 1-4,8-10 or all.
all: Copy all serial port settings.
label: Copy label setting.
base: Copy enable, mode, sharing, and signal settings.
serial: Copy baudrate, data bits, parity, stop bits, and flow control settings.
session: Copy escape, history, exclusive, and idle timeout settings.
monitor: Copy signal change monitoring settings.
service: Copy SSH, TCP, and Telnet service settings.
hangup: Copy hangup on signal loss settings.
autoconnect: Copy autoconnect settings.
framing: Copy data framing settings.
modem: Copy modem emulator settings.
ppp_dialin: Copy PPP dial-in settings.
udp: Copy UDP serial settings.
logging: Copy logging settings.

system serial ipport

Set sequential IP port numbers for a service on a list of ports.

Syntax

```
system serial ipport <destination> <service> <base>
```

Parameters

destination: A list of serial ports to set IP port numbers. Example: 1-4,8-10 or all.

service: The service type to set IP port numbers.

base: Set service IP port numbers to base port + serial port number. (Minimum: 1, Maximum: 65535)

system serial restart

Delete and restart the serial log.

Syntax

```
system serial restart <port>
```

Parameters

port: Serial port.

system serial save

Saves the current serial log to a file.

Syntax

```
system serial save <port> <path>
```

Parameters

port: Serial port.

path: The path and filename to save captured traffic to. If a relative path is provided, /etc/config/serial will be used as the root directory for the path and file.

system serial show

Displays the serial log on the screen.

Syntax

```
system serial show <port>
```

Parameters

port: Serial port.

system storage format

Format a device to the selected filesystem type.

Syntax

```
system storage format <device> <fstype>
```

Parameters
device: Storage device type.
fstype: Format to this filesystem type.

system storage mount

Mount a partition on the device.

Syntax

```
system storage mount <device> [partition INTEGER]
```

Parameters
device: Storage device type.
partition: The partition number to mount. (Minimum: 1, Default: 1)

system storage show

Display information about external devices.

Syntax

```
system storage show
```

Parameters
None

system storage unmount

Unmount the device.

Syntax

```
system storage unmount <device>
```

Parameters
device: Storage device type.

system support-report

Save a support report to a file and include with support requests.

Syntax

```
system support-report [path STRING]
```

Parameters
path: The file path to save the support report to. (Default: /var/log/)

system time set

Set the local date and time using the timezone set in the system.time.timezone config setting.

Syntax

```
system time set <datetime>
```

Parameters
datetime: The date in year-month-day hour:minute:second format (e.g "2021-09-26 12:24:48").

system time sync

Set the local time to the first enabled time source that returns valid time information.

Syntax

```
system time sync
```

Parameters
None

system time test

Test each enabled time source. This test will not affect the device's current local date and time.

Syntax

```
system time test
```

Parameters
None

tail

Tail a file to see its contents.

Syntax

```
tail <path> [timeout INTEGER] [filter STRING] [match STRING]
```

Parameters
path: The file to tail.
timeout: The amount of time in seconds to tail the file. (Default: 10)
filter: Only see output that contains this string.
match: Stop tail when this string is detected in output.

telnet

Use Telnet protocol to log into a remote server.

Syntax

telnet <host> [*port* INTEGER]

Parameters

host: The hostname or IP address of the remote host.

port: The telnet port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 23)

traceroute

Print the route packets trace to network host.

Syntax

traceroute <host> [*ipv6*] [*gateway* STRING] [*interface* STRING] [*first_ttl* INTEGER] [*max_ttl* INTEGER] [*port* INTEGER] [*nqueries* INTEGER] [*src_addr* STRING] [*tos* INTEGER] [*waittime* INTEGER] [*pausemsecs* INTEGER] [*packetlen* INTEGER] [*debug*] [*dontfragment*] [*icmp*] [*nomap*] [*bypass*]

Parameters

host: The host that we wish to trace the route packets for.

ipv6: If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

gateway: Tells traceroute to add an IP source routing option to the outgoing packet that tells the network to route the packet through the specified gateway.

interface: Specifies the interface through which traceroute should send packets. By default, the interface is selected according to the routing table.

first_ttl: Specifies with what TTL to start. (Minimum: 1, Default: 1)

max_ttl: Specifies the maximum number of hops (max time-to-live value) traceroute will probe. (Minimum: 1, Default: 30)

port: Specifies the destination port base traceroute will use (the destination port number will be incremented by each probe). A value of -1 specifies that no specific port will be used. (Minimum: -1, Default: -1)

nqueries: Sets the number of probe packets per hop. A value of -1 indicated. (Minimum: 1, Default: 3)

src_addr: Chooses an alternative source address. Note that you must select the address of one of the interfaces. By default, the address of the outgoing interface is used.

tos: For IPv4, set the Type of Service (ToS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput). Note that in order to use some TOS precedence values, you have to be super user. For IPv6, set the Traffic Control value. A value of -1 specifies that no value will be used. (Minimum: -1, Default: -1)

waittime: Determines how long to wait for a response to a probe. (Minimum: 1, Default: 5)

pausemsecs: Minimal time interval between probes. (Minimum: 0, Default: 0)

packetlen: Total size of the probing packet. Default 60 bytes for IPv4 and 80 for Ipv6. A value of -1 specifies that the default value will be used. (Minimum: -1, Default: -1)

debug: Enable socket level debugging.

dontfragment: Do not fragment probe packets.

icmp: Use ICMP ECHO for probes.

nomap: Do not try to map IP addresses to host names when displaying them.

bypass: Bypass the normal routing tables and send directly to a host on an attached network.

vtysh

Opens the integrated shell for FRRouting (FRR), for more information on FRRouting and VTYSH, visit the FRRouting documentation at https://docs.frrouting.org/projects/dev-guide/en/latest/vtysh.html.

Syntax

```
vtysh
```

Parameters

None