Digi Connect IT® 4

User Guide

User Guide

Revision history—90002355

Revision	Date	Description
C	December 2019	Added information about the LEDs.
D	March 2020	Updated for release 20.2. Added serial port status and configuration pages.
E	June 2020	Release of DigiConnect IT firmware version 20.5: ■ Support for LDAP user authentication. ■ Firmware installation from the Digi firmware server. ■ Enhanced Digi Remote Manager support: • Support for remote proxy server for Digi Remote Manager. • Watchdog support for connection to Digi Remote Manager. • **Locally authenticate CLI** option added to Digi Remote Manager configuration to control whether a user is required to provide device-level authentication when accessing the console of the device through Digi Remote Manager. • Added a randomized two minute delay window for uploading health metrics to the Digi Remote Manager to avoid situations where multiple devices are uploading metrics at the same time.
F	June 2020	Added note that for devices manufactured prior to the release of firmware version 19.11.x, the default user name may be root.
G	July 2020	Added information about the factory default network 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.

© 2020 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 (Digi Connect IT® 4 User Guide, 90002355 A) in the subject line of your email.

Contents

Digi Connect IT® 4 User Guide

Get started with Connect IT

Verify product components 13
Included equipment 13
Required additional equipment 14
Cellular ONLY: Insert the CORE module 15
Prerequisites 15
Connect the hardware to a network 15
Connect hardware and connect to a cellular network 16
Connect hardware and connect to site network using an Ethernet LAN 16

Connect equipment to the Connect IT serial ports

Serial port pinout and use 17

Configuration and management

Review Connect IT default settings 20
Local WebUI 20
Digi Remote Manager 20
Default interface configuration 20
Other default configuration settings 21
Reset default password for the default admin user 21
Configuration methods 23
Using Digi Remote Manager 24
Access Digi Remote Manager 24
Using the web interface 24
Log out of the web interface 25
Using the command line 26
Access the terminal screen from the web UI 26
Access the command line interface 27
Log in to the command line interface 27
Exit the command line interface 28

Configure Remote Power Management

Configure communication between the Connect IT, power controller, and a device 29

Create an access control to specify which users can access which outlets 29
Manage power to the power controller outlets 29
Configure the Connect IT to connect to a power controller using a serial port 30
Configure a serial port for Power Management 30
Connect a power controller to the Connect IT serial port 31
Configure the power controller and the outlets for use with a serial port on the Connect IT 31
Connect a 3rd-party device to the Connect IT serial port and the power controller 32
Configure the Connect IT to connect to a power controller using the network 33
Configure communication with a power controller using the network 33
Connect the Connect IT to your network 34
Connect a 3rd-party device to a serial port on the Connect IT and then to the power controller 34
Create an access control group for power management and assign to users 35
Manage the power to the power controller outlets from the Connect IT 36
Control the outlet power from a terminal (all users) 36
View power controller status and manage power (Administrators) 36
Control the outlet power from the Serial Status page 37

Interfaces

Wide Area Networks (WANs) 39
Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs) 40
Configure WAN/WWAN priority and default route metrics 40
WAN/WWAN failover 43
Configure SureLink active recovery to detect WAN/WWAN failures 44
Configure the device to reboot when a failure is detected 50
Disable SureLink 57
Example: Use a ping test for WAN failover from Ethernet to cellular 60
Using Ethernet devices in a WAN 62
Using cellular modems in a Wireless WAN (WWAN) 63
Configure a Wide Area Network (WAN) 77
Configure a Wireless Wide Area Network (WWAN) 83
Show WAN and WWAN status and statistics 92
Delete a WAN or WWAN. 94
Local Area Networks (LANs) 96
About Local Area Networks (LANs) 97
Configure a LAN 97
Example: Configure two LANs 103
Show LAN status and statistics 111
Delete a LAN 112
DHCP servers 114
Create a Virtual LAN (VLAN) route 128
Bridging 131
Edit the preconfigured LAN bridge 132
Configure a bridge 135

Serial port

Configure the serial port 139
Show serial status and statistics 144
Serial Status page 145

Routing

IP routing 148
Configure a static route 149
Delete a static route 152
Policy-based routing 153
Configure a routing policy 154
Routing services 162
Configure routing services 162
Show the routing table 165
Dynamic DNS 166
Configure dynamic DNS 166
Virtual Router Redundancy Protocol (VRRP) 171
Configure VRRP 171
Show VRRP status and statistics 174

Virtual Private Networks (VPN)

IPsec 177
IPsec data protection 177
IPsec modes 177
Internet Key Exchange (IKE) settings 177
Authentication 178
Configure an IPsec tunnel 178
Configure IPsec failover 200
Configure SureLink active recovery for IPsec 201
Show IPsec status and statistics 207
OpenVPN 209
Configure an OpenVPN server 210
Configure an OpenVPN Authentication Group and User 219
Configure an OpenVPN client by using an .ovpn file 223
Configure an OpenVPN client without using an .ovpn file 225
Configure active recovery for OpenVPN 230
Show OpenVPN server status and statistics 236
Show OpenVPN client status and statistics 237
Generic Routing Encapsulation (GRE) 239
Configuring a GRE tunnel 239
Show GRE tunnels 243
Example: GRE tunnel over an IPSec tunnel 244

Services

Allow remote access for web administration and SSH 261
Configure the web administration service 264
Configure SSH access 271
Use SSH with key authentication 277
Generating SSH key pairs 277
Configure telnet access 279
Configure DNS 283
Simple Network Management Protocol (SNMP) 291
SNMP Security 291
Configure Simple Network Management Protocol (SNMP) 291
Download MIBs 295
System time 297

Configure the system time 297
Network Time Protocol 299
Configure the device as an NTP server 300
Configure a multicast route 306
Enable service discovery (mDNS) 309
Use the iPerf service 312
Example performance test using Iperf3 316

User authentication

Connect IT user authentication 318
User authentication methods 318
Add a new authentication method 320
Delete an authentication method 322
Rearrange the position of authentication methods 323
Authentication groups 325
Change the access rights for a predefined group 326
Add an authentication group 328
Delete an authentication group 332
Local users 334
Change a local user's password 335
Configure a local user 336
Delete a local user 342
Terminal Access Controller Access-Control System Plus (TACACS+) 345
TACACS+ user configuration 346
TACACS+ server failover and fallback to local authentication 347
Configure your Connect IT device to use a TACACS+ server 347
Remote Authentication Dial-In User Service (RADIUS) 353
RADIUS user configuration 354
RADIUS server failover and fallback to local configuration 354
Configure your Connect IT device to use a RADIUS server 355
LDAP 360
LDAP user configuration 361
LDAP server failover and fallback to local configuration 362
Configure your Connect IT device to use an LDAP server 362
Disable shell access 367
Set the idle timeout for Connect IT users 368
Example user configuration 370
Example 1: Administrator user with local authentication 370
Example 2: RADIUS, TACACS+, and local authentication for one user 372

Firewall

Firewall configuration 383
Create a custom firewall zone 383
Configure the firewall zone for a network interface 385
Delete a custom firewall zone 386
Port forwarding rules 387
Configure port forwarding 387
Delete a port forwarding rule 392
Packet filtering 394
Configure packet filtering 394
Enable or disable a packet filtering rule 398
Delete a packet filtering rule 399

Configure custom firewall rules 401
Configure Quality of Service options 403

System administration

Review device status 416
Configure system information 417
Update system firmware 419
Manage firmware updates using Digi Remote Manager 419
Certificate management for firmware images 419
Update cellular module firmware 422
Reboot your Connect IT device 423
Reboot your device immediately 424
Schedule reboots of your device 424
Reset the device to factory defaults 425
Configuration files 429
Save configuration changes 429
Save configuration to a file 430
Restore the device configuration 431
Schedule system maintenance tasks 434

Monitoring

intelliFlow 442
Enable intelliFlow 442
Use intelliFlow to display average CPU and RAM usage 445
Use intelliFlow to display top data usage information 446
Use intelliFlow to display data usage by host over time 448
Configure NetFlow Probe 449

Central management with Digi Remote Manager

Digi Remote Manager support 455
Configure Digi Remote Manager 455
Collect device health data and set the sample interval 460
Log into Digi Remote Manager 462
Use Digi Remote Manager to view and manage your device 463
Add a device to Digi Remote Manager 464
View Digi Remote Manager connection status 464
Use the Digi Remote Manager mobile app 465
Configure multiple devices using profiles 466
Learn more 466

File system

The Connect IT local file system 468
Display directory contents 468
Create a directory 469
Display file contents 470
Copy a file or directory 470
Move or rename a file or directory 471
Delete a file or directory 472
Upload and download files 473

Upload and download files by using the WebUI 473
Upload and download files by using the Secure Copy command 474
Upload and download files using SFTP 475

Diagnostics

Generate a support report 478
View system event logs 479
View System Logs 479
View Event Logs 482
Configure syslog servers 484
Configure options for the event and system logs 486
Analyze network traffic 490
Configure packet capture for the network analyzer 491
Example filters for capturing data traffic 495
Capture packets from the command line 496
Stop capturing packets 497
Show captured traffic data 497
Save captured data traffic to a file 499
Download captured data to your PC 500
Clear captured data 501
Use the ping command to troubleshoot network connections 502
Ping to check internet connection 502
Stop ping commands 502
Use the traceroute command to diagnose IP routing problems 502

Hardware

Connect IT 4 hardware and LEDs 504
Front panel and LEDs 504
Back panel 505
Signal strength 505
Exchange power tips 506
Select SIM card 506

Troubleshooting

Cellular network fallback 508
Use the RESET button to reset your device to the factory defaults 508
Tips for improving cellular signal strength 508
Download a support report 508

Regulatory and safety information

FCC certifications 510
USA 510
INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A) 510
European Union 510
Safety warnings 510

Command line interface

Access the command line interface 514
Log in to the command line interface 514
Exit the command line interface 515
Execute a command from the web interface 515
Display help for commands and parameters 516
The help command 516
The question mark (?) command 516
Display help for individual commands 517
Use the Tab key or the space bar to display abbreviated help 518
Auto-complete commands and parameters 518
Available commands 519
Use the scp command 520
Display status and statistics using the show command 521
show config 521
show system 522
show network 522
Device configuration using the command line interface 522
Execute configuration commands at the root Admin CLI prompt 523
Display help for the config command from the root Admin CLI prompt 523
Configuration mode 525
Enable configuration mode 525
Enter configuration commands in configuration mode 525
Save changes and exit configuration mode 525
Exit configuration mode without saving changes 526
Configuration actions 526
Display command line help in configuration mode 527
Move within the configuration schema 529
Manage elements in lists 530
The revert command 532
Enter strings in configuration commands 534
Example: Create a new user by using the command line 534
Command line reference 537
analyzer 538
cp 539
help 540
ls 541
mkdir 542
modem 543
modem puk status [imei STRING] [name STRING] 546
more 548
mv 549
ping 550
reboot 551
rm 552
scp 553
show 554
system 562
traceroute 564
update 567

Digi Connect IT® 4 User Guide

This guide provides reference and usage information for the Connect IT.

The Connect IT provides out-of-band management for remote network or infrastructure devices. Cellular connectivity, available as standard in some models and as an option in other models, provides fast reliable cellular connections without additional equipment. All connections are encrypted for security.

Get started with Connect IT

This section explains what comes with each Connect IT model, how to install the necessary software, and how to connect the hardware.

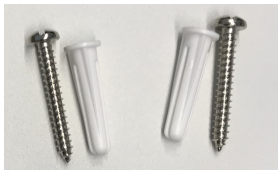
1. Verify product components.
2. Cellular ONLY: Insert the CORE module.
3. Connect the hardware to a network.
4. Using the web interface.
5. Update system firmware
6. Change a local user's password
7. Connect equipment to the Connect IT serial ports.

Verify product components

Verify that you have the following included equipment.

Included equipment

Equipment	Description
Digi Connect IT 4	For detailed information about the front and back panels, see Connect IT 4 hardware and LEDs.
Power supply kit	If you purchased the US variant (-OUS) you will receive a US plug adapter. If you purchased the global variant (-GLB) you will receive the Universal power supply kit. For instructions about exchanging power tips, see Exchange power tips.
Antennas (2)	

Equipment	Description
CORE module	 This is included with some versions of the Connect IT 4 modules. See Connect hardware and connect to a cellular network.
CORE module cover and cover screws (2)	
Mounting screws	 These are used to mount the Connect IT 4 to a wall or another surface.

Required additional equipment

Equipment	Description
Ethernet cable	CAT 5/6 Ethernet cable The cable is used to connect your PC to the Connect IT 4 for initial configuration. See Connect hardware and connect to site network using an Ethernet LAN.
SIM card	An activated SIM card provided by your cellular network operator. You can insert up to two SIM cards in the CORE module. See Cellular ONLY: Insert the CORE module. The Connect IT 4 supports the standard mini-SIM cards (2FF). **Note** This is required only if you are using a CORE module to connect to a cellular network. See Connect hardware and connect to a cellular network.

Cellular ONLY: Insert the CORE module

Note If you are connecting to a network using an Ethernet connection, you can skip this section. See Connect hardware and connect to site network using an Ethernet LAN.

This section explains how to connect the Digi CORE® module and cellular antennas to the Connect IT hardware.

Prerequisites

- Activated SIM card from your cellular network provider.
- CORE module. This may be included with your device. If it is not, you must purchase one separately.

To connect the hardware and connect to the cellular network:

1. Insert your activated SIM card into the CORE module. The notched end of SIM card should be inserted first, with the gold metal contacts facing down. You will hear a click once the SIM is completely inserted.

   Note If one SIM card is being used, insert the SIM card into the SIM 1 slot.

2. Insert the CORE module into the device.
   a. Orient the device so the front of the device is facing you.
   b. Remove the CORE module slot cover from the left side of the device.
   c. Insert the CORE module into the slot. Make sure the pin holes on the back of the module match the location of the pins in the slot.
   d. Push the module into the slot.
   e. Push the white handle down until you hear it click.
   f. Optionally, you can screw one of the CORE module cover screws into the center of the handle.
   g. Place the white CORE module cover over the end of the device. Make sure that the antenna labels are oriented correctly.
   h. Push the cover in place.
3. Attach both of the included antennas. While gripping the metal connector section with your thumb and forefinger, tighten until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.

   Note Attaching both antennas ensures maximum performance. If a single antenna solution is required, it must be attached to the antenna port labeled MAIN.

Connect the hardware to a network

These sections explain how to connect to either a cellular network using the CORE module or to a site network using an Ethernet cable.

- Connect hardware and connect to a cellular network
- Connect hardware and connect to site network using an Ethernet LAN

Connect hardware and connect to a cellular network

This section explains how to connect the Connect IT hardware and then connect to a cellular network, using a CORE module.

Note By default, the device uses a cellular network. As an alternative, you can also use an Ethernet LAN connection. See Connect hardware and connect to site network using an Ethernet LAN.

To connect the hardware and connect to the cellular network:

1. Insert a CORE module with an activated SIM card. See Cellular ONLY: Insert the CORE module.
2. Connect the power supply unit to the device.
3. Verify the cellular network signal strength indicator on the front of the Connect IT shows two or more bars for proper operation. See Signal strength.

Page break after

Connect hardware and connect to site network using an Ethernet LAN

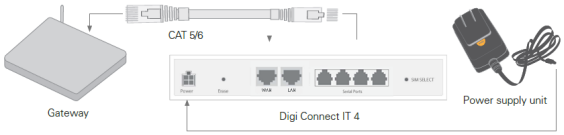
This section explains how to connect the Connect IT hardware and then connect to a site network, using an Ethernet cable.

Prerequisites

- CAT 5/6 Ethernet cable, which must be purchased separately.

To connect the hardware and connect to a site network:

1. Plug the power supply unit into an AC power outlet and connect the other end to the **Power** plug on the Connect IT.
2. Connect one end of an Ethernet cable to your site gateway.
3. Connect the other end of the Ethernet cable to the Ethernet LAN port on the Connect IT.



Connect equipment to the Connect IT serial ports

After your device is connected and powered up, you can connect equipment to the device using the serial ports.

The serial ports on the Connect IT provide console access to connected critical equipment through the cellular network or a connected Ethernet LAN. You can connect up to four network devices to the Connect IT serial ports. For pinout information, see Serial port pinout and use.

You must use a cable with an RJ45 connector to connect to the Connect IT with an RJ45, DB9F or DB9M connector, as determined by your device type, to terminate to your device. Consult the user guide for the device you are connecting to the Connect IT to determine the connector type, cable type, and pinout positions for your specific device.

The serial ports are enabled by default. The network devices connected to the serial ports may be accessed using Remote Manager, the local web user interface, TCP, telnet, or SSH connections. TCP, telnet and SSH connections to serial ports are disabled by default and must be enabled by a device-specific configuration.

Serial port pinout and use

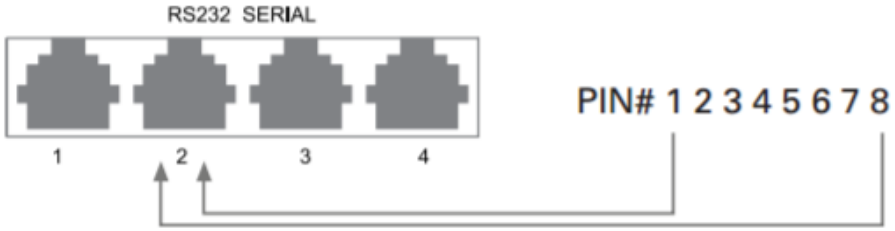
The RS232 standard requires support for baud rates up to 9600 baud on shielded multicore cable up to 50 feet (15 meters) long. For the Connect IT, the use of standard CAT 5 cables enables serial communication at all baud rates up to 50 feet. CAT5 unshielded twisted pair cable lengths much longer than 50 feet have been verified at 9600 baud but are non-standard and are not guaranteed.

The Connect IT RS232 serial ports are DTE and have the following pin configuration.

Pin		Description	Signal
Pin 1	RTS	Request to send	Output from Connect IT
Pin 2	DCD	Data carrier detect	Input to Connect IT
Pin 3	RXD	Receive data	Input to Connect IT
Pin 4/5		Ground	Signal ground
Pin 6	TXD	Transmit data	Output from Connect IT
Pin 7	DTR	Data terminal ready	Output from Connect IT
Pin 8	CTS	Clear to send	Input to Connect IT

Note Ring indicate (RI) and data set ready (DSR) are not implemented.

The serial ports use a female RJ45 jack to enable connection using UTP Ethernet cabling.



Configuration and management

This chapter contains the following topics:

Review Connect IT default settings 20
Reset default password for the default admin user 21
Configuration methods 23
Using Digi Remote Manager 24
Access Digi Remote Manager 24
Using the web interface 24
Using the command line 26
Access the terminal screen from the web UI 26
Access the command line interface 27
Log in to the command line interface 27
Exit the command line interface 28

Review Connect IT default settings

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

Local WebUI

1. Log into the Connect IT WebUI as a user with Admin access. See Using the 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. Click **Device Management** to display a list of your devices.
3. Locate and select your device as described in Use Digi Remote Manager to view and manage your device.
4. Click **Configure**.

The following tables list important factory default settings for the Connect IT.

Default interface configuration

Interface type	Preconfigured interfaces	Devices	Default configuration
Wide Area Networks (WAN)	■ **WAN**	■ Ethernet: **WAN**	■ Firewall zone: External ■ WAN priority: Metric=1 ■ IP Address: DHCP client ■ Digi SureLink™ enabled for IPv4
Wireless Wide Area Networks (WWAN)	■ **Modem**	■ **Modem**	■ Firewall zone: External ■ WAN priority: Metric=3 ■ SIM failover after 5 attempts
Local Area Networks (LANs)	■ **LAN**	■ Ethernet: **LAN**	■ Firewall zone: Internal ■ IP address: 192.168.2.1/24 ■ DHCP server enabled ■ LAN priority: Metric=5
	■ **Loopback**	■ Ethernet: **Loopback**	■ Firewall zone: Loopback ■ IP address: 127.0.0.1/8

Interface type	Preconfigured interfaces	Devices	Default configuration
	■ **Default IP**	■ Ethernet: **LAN**	■ Firewall zone: Setup ■ IP address 192.168.210.1/24
	■ **Default Link-local IP**	■ Ethernet: **LAN**	■ 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: Login ■ Label: None ■ Baud rate: 9600 ■ Data bits: 8 ■ Parity: None ■ Stop bits: 1 ■ Flow control: None

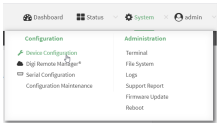
Reset default password for the default admin user

When you first log into the WebUI or the command line, or after erasing the configuration, you will be required to change the unique, factory-assigned default password for the default **admin** user prior to being able to save any changes or exit the user interface. The unique, factory-assigned default password is printed on the bottom label of the device (or the printed label included in the package).

Note If your device was manufactured prior to the release of firmware version 19.11.x, the default user name may be **root**.

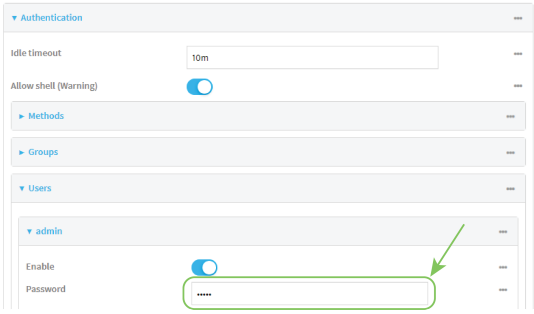
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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.



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

Command line

1. Log into the Connect IT 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:

```
(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 Connect IT 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 Connect IT device and use the configuration as a basis for a profile which can be applied to other similar devices. See Using Digi Remote Manager for more information about using the Remote Manager to manage and configure your Connect IT device.
  - The local web interface. See Using the web interface for more information about using the local web interface to manage and configure your Connect IT device.

  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 Connect IT device. See Using the command line for more information about using the command line to manage and configure your Connect IT device.

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

WebUI

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 Connect IT device is configured to use Digi Remote Manager as its central management server. No configuration changes are required to begin using the Remote Manager.

For information about configuring central management for your Connect IT device, see Central management with Digi Remote Manager.

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.

   Check your email for Digi Remote Manager login instructions.
2. Go to remotemanager.digi.com.
2. Enter your username and password.

   The Digi Remote Manager Dashboard appears.

Using the web interface

To connect to the Connect IT local WebUI:

1. Use an Ethernet cable to connect the Connect IT's **ETH2** port to a laptop or PC.
2. Open a browser and go to **192.168.2.1**.
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.

   Note If your device was manufactured prior to firmware version 19.11.x, the default user for logging into the device may be **root**, rather than **admin**.

   - The default user is **root**:
     - If the device is at a firmware level 19.8.x or older.
     - If the device has been upgraded from 19.8.x or older to 19.11.x or newer.
   - The default user is **admin**:
     - If the device is at 19.11.x or newer when manufactured.
     - If the device has been upgraded from 19.8.x or older to 19.11.x or newer and has been factory reset after the upgrade.

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

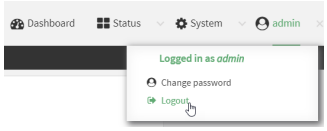
The dashboard shows the current state of the device.

Dashboard area	Description
Network activity	Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices.

Dashboard area	Description
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.
Device	Displays the Connect IT device's status, statistics, and identifying information.
Network Interfaces	Displays the status of the network interfaces configured on the device.
Modems	Provides information about the signal strength and technology of the cellular modem (s).

Log out of the web interface

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



Using the command line

The Digi Connect IT 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 terminal screen from the web UI

A user can log into a terminal screen and use CLI commands to access features.

Note You can also access the terminal screen from a port listed in the Serial Status page.

1. Log in to the web UI.
2. Click **System** > **Terminal**. The **Terminal** screen displays.
3. When prompted, enter your user name and password.
4. Enter the number of the port that you want to access.
5. Information about the port you are connected to displays, as well as commands.

```
Connecting to port5:
Settings: 9600, 8, 1, none, none
Type '~b.' to disconnect from port
Type '~b?' to list commands
```

6. Enter **~b?** to display additional commands.

   Note The **~bP**, **~bO**, and **~bN** commands are used with the remote power management feature. See Configure Remote Power Management.

Command	Description
~b.	Disconnect from the port.
~bB	Send a BREAK sequence.
~bc	Clear the history buffer.
~br	Send a DTR reset sequence.
~bP	Cycle the outlets on this port. Turn the power off, then on. If the power state for the outlet is currently off, then the power is just turned on.
~bO	Power off all the outlets on this port.
~bN	Power on all the outlets on this port.
~b?	Display a list of commands.

7. Enter **~b.** to disconnect from the port.

Access the command line interface

You can access the Connect IT 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: Configure the 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 Connect IT 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.
   - For serial connections, the default configuration is:
     - **115200** baud rate
     - **8** data bits
     - **no** parity
     - **1** stop bit
     - **no** flow control
   - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** 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
    1: Serial: port1      (9600,8,1,none,none)
    q: Quit

Select access or quit [admin] :
```

Type **a** or **admin** to access the Connect IT command line.

You will now be connected to the Admin CLI:

```
Connecting now, 'exit' to disconnect from 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
       1: Serial: port1      (9600,8,1,none,none)
       q: Quit

   Select access or quit [admin] :
   ```

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

Configure Remote Power Management

The remote power management feature allows you to control the power to the outlets on a power controller using serial or network interfaces. This means that you can turn a 3rd-party device plugged into that outlet on and off.

Configure communication between the Connect IT, power controller, and a device

Configure the Connect IT to communicate with a power controller from either a serial port or through your network. As an optional part of this configuration, you may also configure the outlets on the power controller to communicate with a specific serial port on the Connect IT.

- **Serial port**: Configure the Connect IT to connect to a power controller using a serial port
- **Network**: Configure the Connect IT to connect to a power controller using the network

You can then complete the connection between the Connect IT, power controller, and the device you want to communicate with:

- Connect the power controller to the Connect IT using a serial port or to a network port.
- Connect a 3rd-party device to a configured serial port on the Connect IT.
- Plug the 3rd-party device into the outlet on the power controller that corresponds to the serial port on the Connect IT.

Create an access control to specify which users can access which outlets

You can create an access control group that enables a set of users to control a power outlet from inside a terminal session.

Create an access control group for power management and assign to users

Manage power to the power controller outlets

You can manage the power to an individual outlet on the power controller from the web UI or a terminal.

Manage the power to the power controller outlets from the Connect IT

Configure the Connect IT to connect to a power controller using a serial port

You can configure the Connect IT to connect to a power controller from a serial port.

To use a serial port, you must configure a serial port on the Connect IT to communicate with a power controller. You can then connect the power controller to the serial port on the Connect IT using a serial cable.

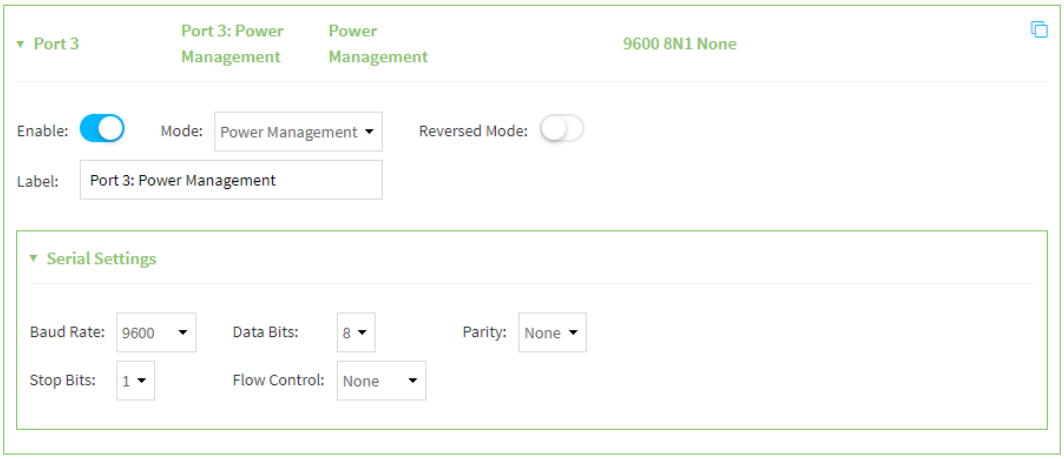
1. Review the serial settings for your power controller. You will use this information to configure the Connect IT.
2. Verify that your serial cable has the correct pinout. See Serial port pinout and use.
3. Configure a serial port for Power Management.
4. Connect a power controller to the Connect IT serial port.
5. Configure the power controller and the outlets for use with a serial port on the Connect IT.
6. Connect a 3rd-party device to the Connect IT serial port and the power controller.

Configure a serial port for Power Management

You can configure a serial port on the Connect IT to communicate with the power controller. In this example, you will configure serial port 3 as a power management port.

This is the port to which you will connect the power controller to the Connect IT using a serial cable.

1. Log in to the web UI.
2. Click **System** > **Serial Configuration**.
3. Expand the port that you want to configure for use with the power controller.
4. Select **Enable**.
5. From the **Mode** list box, select the **Power Management** option.
6. In the **Label** field, enter a descriptive name for the port.
7. Expand the **Serial Settings** section. The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries: **Baud rate**, **Data bits**, **Parity**, **Stop bits**, and **Flow control**.



8. Click **Apply**.

Connect a power controller to the Connect IT serial port

After you have configured a power management serial port on the Connect IT and configured the power controller, you should connect the Connect IT and the power controller with a serial cable.

In this example, serial port 3 was configured for use with a power controller. See Configure a serial port for Power Management.

1. Connect a serial cable to the serial port on the Connect IT that you configured for power management.
2. Connect the other end of the serial cable to the serial port on the power controller.
3. Plug the power controller into a power source.

Configure the power controller and the outlets for use with a serial port on the Connect IT

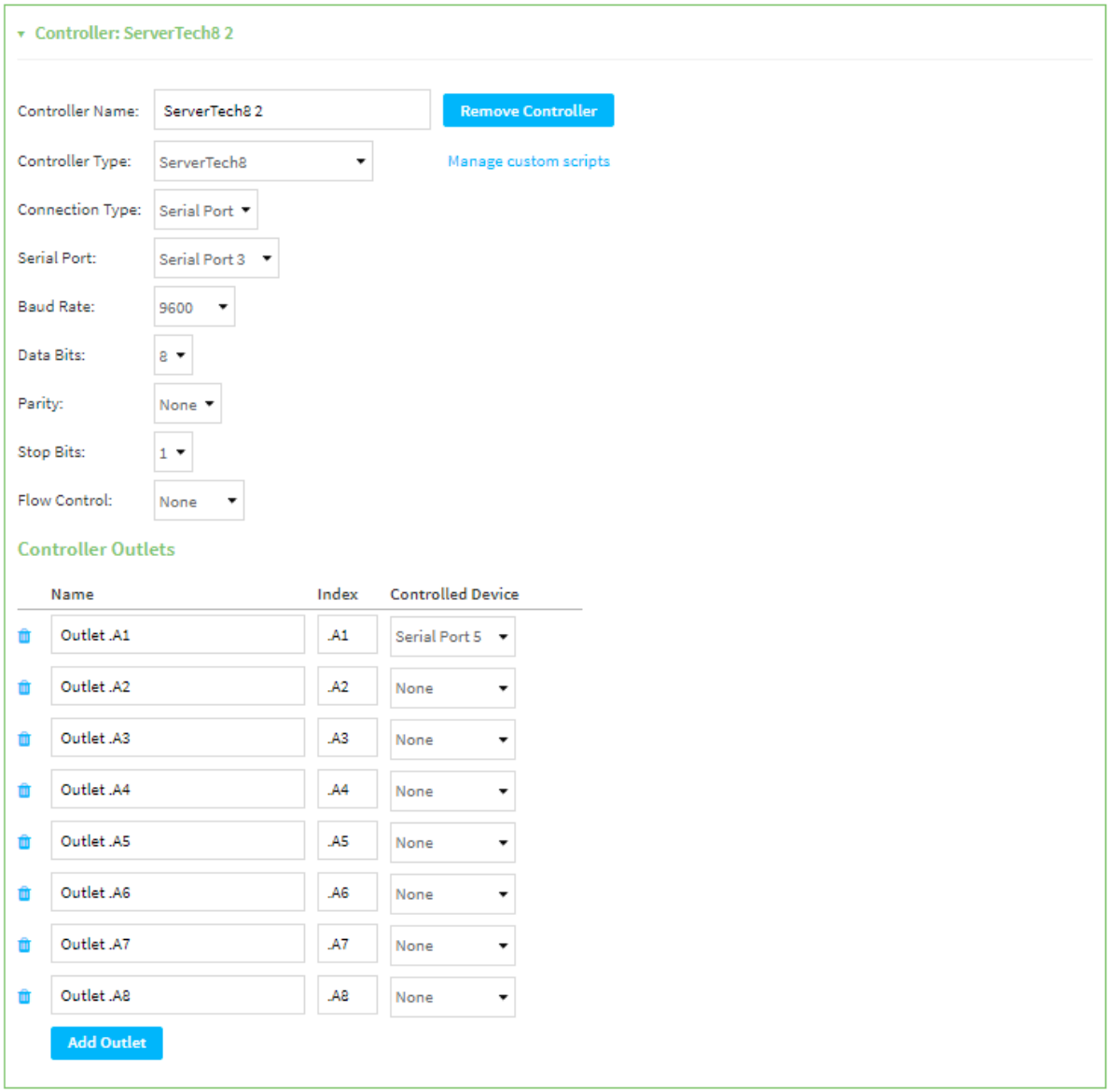
You can configure the power controller to communicate with a specific serial port on the Connect IT.

You can also configure the outlets on the power controller to work with a specific serial port on the Connect IT, into which a device will be connected.

1. Log in to the web UI.
2. Click **System** > **Power Controller Configuration**.
3. Select **Enable**.
4. In the **Monitor Interval** field, specify the number of seconds to wait between power controller status checks.
5. Click **Add Controller**.
6. In the **Controller Name** field, enter a descriptive name.
7. From the **Controller Type** list box, select the appropriate controller type.
8. From the **Connection type** list box, select **Serial Port**.
9. In the **Serial port** field, select the port number from the list box. See Configure a serial port for Power Management.
10. The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries: **Baud rate**, **Data bits**, **Parity**, **Stop bits**, and **Flow control**.
11. Configure the outlets on the power controller that can be controlled by the port.
    a. In the **Name** field, enter a descriptive name. You can type over the default name.
    b. In the **Index** field, enter the appropriate outlet index. Refer to the manual for your power controller to determine the outlet index.
    c. From the **Controlled Device** list box, select a serial port. This is the port you will use to complete the connection between the Connect IT and the 3rd-party device plugged into the outlet on the power controller. In this example, outlet 1 is configured for serial port 5.

    Note The serial port you configure for an outlet must be configured for **Remote Access** mode.

    d. Repeat the process to configure additional outlets. You can click **Add Outlet** to add another outlet.
12. Click **Apply**.



Connect a 3rd-party device to the Connect IT serial port and the power controller

The final step is to complete the connection between the power controller, the Connect IT, and the 3rd-party device that you want to manage from the Connect IT.

In this example, you configured outlet 1 for use with serial port 5 on the Connect IT.

1. Make sure the power controller is connected to the correct serial port on the Connect IT. See Connect a power controller to the Connect IT serial port.
2. Connect one end of a serial cable to the serial port on the Connect IT that is configured to communicate with a 3rd-party device plugged into the power controller. In this example, serial port 5 is configured to communicate.

3. Connect the other end of the serial cable to the 3rd-party device.
4. Connect a power cable to the 3rd-party device.
5. Plug the other end of the power cable into an outlet on the power controller that is configured to communicate with a serial port on the Connect IT. In this example, outlet 1 is configured to communicate with serial port 5.

Configure the Connect IT to connect to a power controller using the network

You can configure the Connect IT to connect to the power controller from your network.

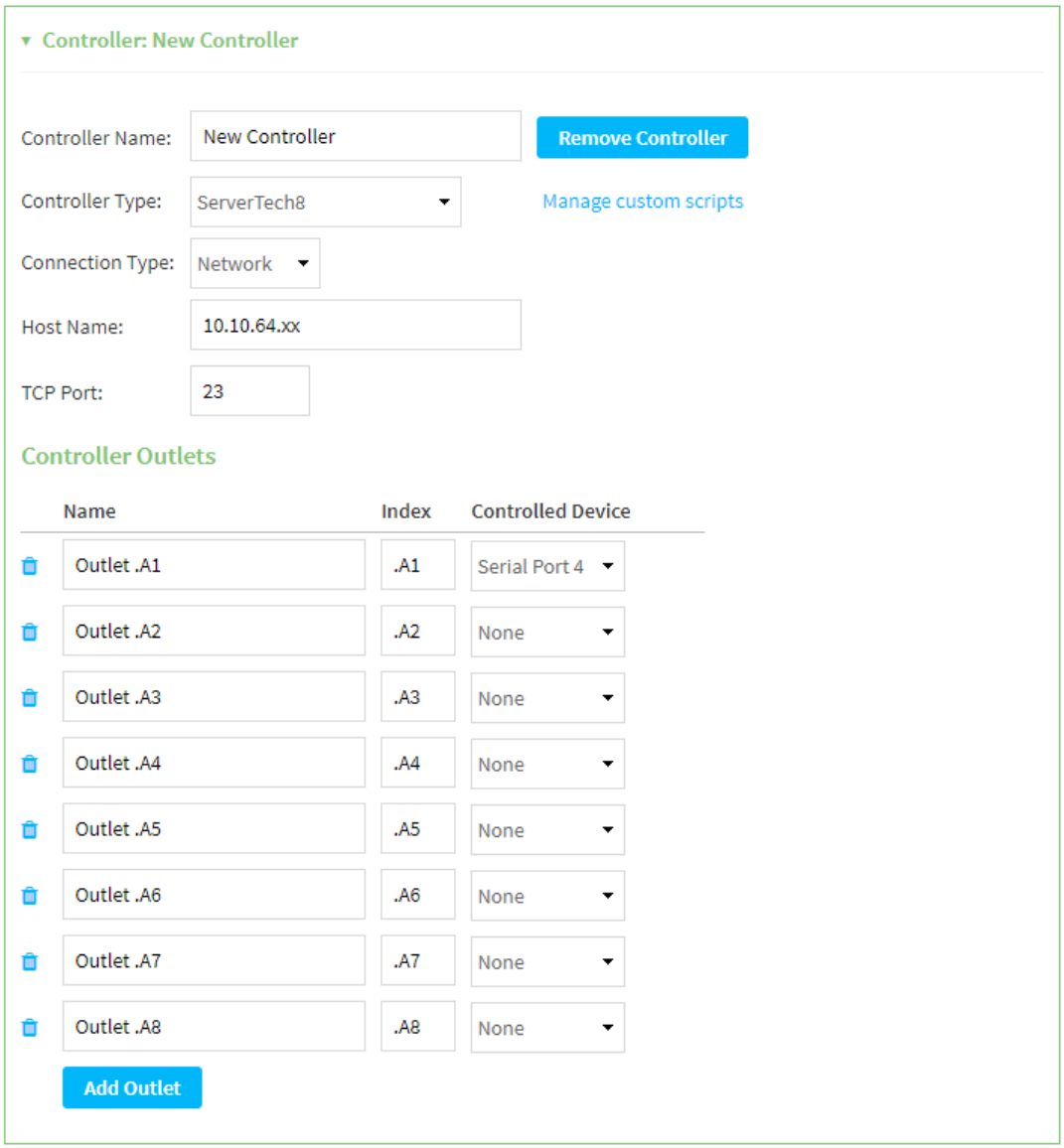
1. Configure communication with a power controller using the network.
2. Connect the Connect IT to your network.
3. Connect a 3rd-party device to a serial port on the Connect IT and then to the power controller.

Configure communication with a power controller using the network

You can configure the Connect IT to communicate with a power controller and the outlets on the power controller using the network.

You can also configure the outlets on the power controller to work with a specific serial port on the Connect IT, into which a 3rd-party device will be connected.

1. Log in to the web UI.
2. Click **System** > **Power Controller Configuration**.
3. Select **Enable**.
4. In the **Monitor Interval** field, specify the number of seconds to wait between power controller status checks.
5. Click **Add Controller**.
6. In the **Controller name** field, enter a descriptive name.
7. From the **Controller type** list box, select the appropriate controller type.
8. From the **Connection type** list box, select **Network**.
9. In the **Hostname** field, enter the name or IP address of the network host.
10. In the **TCP Port** field, enter the TCP port number that will be used for the connection. Refer to the manual for your power controller to determine the correct port.
11. Configure an outlet on the power controller to communicate with a specific serial port.
    a. In the **Name** field, enter a descriptive name.
    b. In the **Index** field, enter the appropriate outlet index. Refer to the manual for your power controller to determine the outlet index.
    c. From the **Controlled Device** list box, select a serial port. In this example, outlet 1 is configured for serial port 4.
    d. Repeat the process to configure additional outlets. You can click **Add Outlet** to add another outlet.
12. Click **Apply**.



Connect the Connect IT to your network

After you have configured the power controller to connect to the network, you should connect the Connect IT to your network with an Ethernet cable.

1. Connect an Ethernet cable to the WAN or LAN port on the Connect IT.
2. Connect the other end of the Ethernet cable to your network.
3. Plug the power controller into a power source.

Connect a 3rd-party device to a serial port on the Connect IT and then to the power controller

You can complete the connection between the power controller, the Connect IT, and the 3rd-party device that you want to manage from the Connect IT.

In this example, you configured outlet 1 for use with serial port 4 on the Connect IT.

1. Make sure the Connect IT is connected to your network using an Ethernet cable. See Connect the Connect IT to your network.
2. Connect one end of a serial cable to the serial port on the Connect IT that is configured to communicate with an outlet on the power controller. In this example, connect to serial port 4.
3. Connect the other end of the serial cable to the 3rd-party device.
4. Connect a power cable to the 3rd-party device.
5. Plug the other end of the power cable into an outlet on the power controller that is configured to communicate with a serial port on the Connect IT. In this example, plug into outlet 1, which was configured to communicate with serial port 4.

Create an access control group for power management and assign to users

You can create an access control group that enables a set of users to control a power outlet from inside a terminal session. For each access control group, you can configure a serial port and the associated outlets, and then assign the group to users that are allowed access to the outlets on that port.

Note For information about accessing and using a terminal session, see Control the outlet power from a terminal (all users).

1. Log in to the web UI.
2. Click **System** > **Device Configuration**.
3. Expand **Authentication**.
4. Expand **Groups**.
5. Add a group.
   a. In the **Add Group** field, enter a group name.
   b. Click **+**.
6. Select the **Serial access** option.
7. Configure the serial port for the group.
   a. Expand the **Serial ports** section.
   b. Click **+** next to **Add Port**.
   c. From the **Port** list box, select a port for the group. The port should have been previously configured for remote power management. See Configure a serial port for Power Management.
8. Configure the power outlets for the group.
   a. Expand the **Power outlets** section.
   b. Click **+** next to **Add Outlet**.
   c. From the **Outlet** list box, select an outlet for the group.
   d. Repeat the process to add additional outlets.
9. Click **Apply**.

Manage the power to the power controller outlets from the Connect IT

You can use any of the following methods to manage the power to an outlet on a power controller.

Control the outlet power from a terminal (all users)

A user can log into a terminal on the Connect IT and then power the device connected to an outlet on and off.

1. Log in to the web UI.
2. Click **System** > **Terminal**. The **Terminal** screen displays.
3. When prompted, enter your user name and password.
4. Enter the number of the port that you want to access.
5. Information about the port you are connected to displays, as well as commands.

```
Connecting to port3: PowerManPort3
Settings: 9600, 8, 1, none, none
Type '~b.' to disconnect from port
Type '~b?' to list commands
```

6. Enter **~b?** to display additional commands. The commands you can use to control the power to the outlets are highlighted in the table below.

Command	Description
~b.	Disconnect from the port.
~bB	Send a BREAK sequence.
~bc	Clear the history buffer.
~br	Send a DTR reset sequence.
~bP	Cycle the outlets on this port. Turn the power off, then on. If the power state for the outlet is currently off, then the power is just turned on.
~bO	Power off all the outlets on this port.
~bN	Power on all the outlets on this port.
~b?	Display a list of commands.

7. Enter **~b.** to disconnect from the port.

View power controller status and manage power (Administrators)

You can view the status of each outlet configured for a power controller and turn the power to an outlet on and off.

Note This process can only be done in the local web UI. Only admin users can access the **Power Controllers** page. Non-administrators can control the power in a Terminal screen. See Control the outlet power from a terminal (all users).

1. Log in to the web UI.
2. Click **Status** > **Power Controllers**. The **Power Controller Status** page appears.
3. You can view the power controller power status. Each outlet and power controller combination configured for remote power management appears in the page. The state of the power for each outlet is displayed in the **State** column:
   - **on**: The outlet has power.
   - **off**: The outlet does not have power.
   - **unknown**: The Connect IT cannot get a status from the power controller.
4. You can change the power state for an outlet.
   a. From the **Change State** list box, select an option from the list box.
      - **On**: Turn on the power to that outlet.
      - **Off**: Turn off the power to that outlet.
      - **Cycle**: Turn the power off, then on. If the power state for the outlet is currently off, then the power is just turned on.

   b. Click **Apply**.
5. You can view the power manager log.

   A log of all remote power management events appears in the **Log** shown at the bottom of the page. Click **Download** to download a copy of the log.

Control the outlet power from the Serial Status page

A user can access the Serial Status page in the web UI and control the power for an outlet connected to a serial port.

1. Log in to the web UI.
2. Click **Status** > **Serial**. The **Serial Status** screen displays.
3. If a serial port is configured for communication with a 3rd-party device plugged into an outlet, the power status displays in the Power column.
   - **ON**: **ON** displays in green when there is power to the outlet configured for the serial port. Click **ON** to turn power to the outlet off.
   - **OFF**: **OFF** displays in red when there is no power to the outlet configured for the serial port. Click **OFF** to turn power to the outlet on.

Interfaces

Connect IT 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:

Wide Area Networks (WANs) 39
Local Area Networks (LANs) 96
Bridging 131

Wide Area Networks (WANs)

The Connect IT device is preconfigured with one Wide Area Network (WAN), named **WAN**, and one Wireless Wide Area Network (WWAN), named **Modem**.

You can modify configuration settings for the existing WAN and WWANs, and you can create new WANs and WWANs.

This section contains the following topics:

Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs) 40
Configure WAN/WWAN priority and default route metrics 40
WAN/WWAN failover 43
Configure SureLink active recovery to detect WAN/WWAN failures 44
Configure the device to reboot when a failure is detected 50
Disable SureLink 57
Example: Use a ping test for WAN failover from Ethernet to cellular 60
Using Ethernet devices in a WAN 62
Using cellular modems in a Wireless WAN (WWAN) 63
Configure a Wide Area Network (WAN) 77
Configure a Wireless Wide Area Network (WWAN) 83
Show WAN and WWAN status and statistics 92
Delete a WAN or WWAN. 94

Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs)

A Wide Area Network (WAN) provides connectivity to the internet or a remote network. A WAN configuration consists of the following:

- A physical device, such as an Ethernet device or a cellular modem.
- Several networking parameters for the WAN, such as firewall configuration and IPv4 and IPv6 support.
- Several parameters controlling failover.

Configure WAN/WWAN priority and default route metrics

The Connect IT device is preconfigured with one Wide Area Network (WAN), named **WAN**, and one Wireless Wide Area Network (WWAN), named **Modem**. You can also create additional WANs and WWANs.

When a WAN is initialized, the Connect IT device automatically adds a default IP route for the WAN. The priority of the WAN is based on the metric of the default route, as configured in the WAN's IPv4 and IPv6 metric settings.

Assigning priority to WANs

By default, the Connect IT device's WAN (**WAN**) is configured with the lowest metric (**1**), and is therefor the highest priority WAN. By default, the Wireless WAN (**Modem**) is configured with a metric of **3**, which means it has a lower priority than **WAN**. You can assign priority to WANs based on the behavior you want to implement for primary and backup WAN interfaces. For example, if you want a cellular connection to be your primary WAN, with an Ethernet interface as backup, configure the metric of the WWAN to be lower than the metric of the WAN.

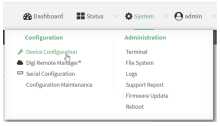
Example: Configure cellular connection as the primary WAN, and the Ethernet connection as backup

Required configuration items

- Configured WAN and WWAN interfaces. This example uses the preconfigured **WAN** and **Modem** interfaces.
- The metric for each WAN.

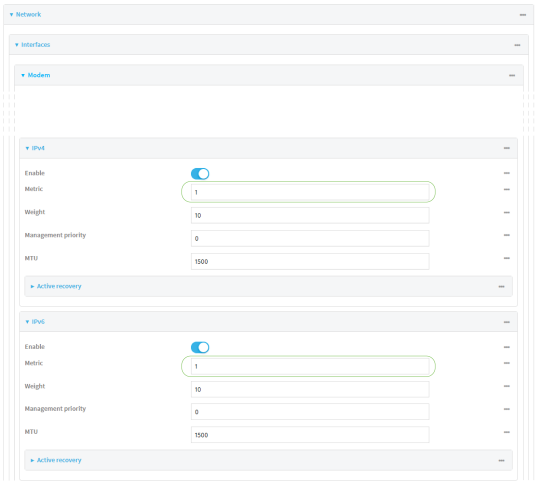
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

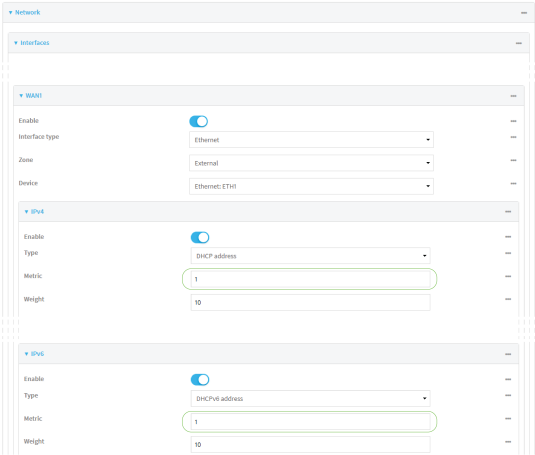


   The **Configuration** window is displayed.

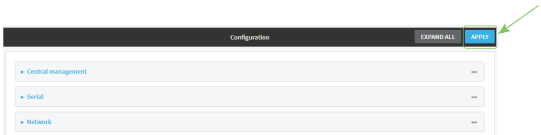
3. Set the metrics for **Modem**:
   a. Click **Network** > **Interfaces** > **Modem** > **IPv4**.
   b. For **Metric**, type **1**.
   c. Click **IPv6**.
   d. For **Metric**, type **1**.



4. Set the metrics for **WAN**:
   a. Click **Network** > **Interfaces** > **WAN** > **IPv4**.
   b. For **Metric**, type **2**.
   c. Click **IPv6**.
   d. For **Metric**, type **2**.



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



The Connect IT device is now configured to use the cellular modem WWAN, **Modem**, as its highest priority WAN, and its Ethernet WAN, **WAN**, as its secondary WAN.

Command line

1. Log into the Connect IT 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 metrics for **Modem**:

   a. Set the IPv4 metric for **Modem** to **1**. For example:

```
(config)> network interface modem ipv4 metric 1
(config)>
```

   b. Set the IPv6 metric for **Modem** to **1**:

```
(config)> network interface modem ipv6 metric 1
(config)>
```

4. Set the metrics for **WAN**:
   a. Set the IPv4 metric for **WAN** to **2**:

```
(config)> network interface wan ipv4 metric 2
(config)>
```

   b. Set the IPv6 metric for **WAN** to **1**:

```
(config)> network interface wan ipv6 metric 2
(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.

The Connect IT device is now configured to use the cellular modem WWAN, **Modem**, as its highest priority WAN, and its Ethernet WAN, **WAN**, as its secondary WAN.

WAN/WWAN failover

If a connection to a WAN interface is lost for any reason, the Connect IT device will immediately fail over to the next WAN or WWAN interface, based on WAN priority. See Configure WAN/WWAN priority and default route metrics for more information about WAN priority.

Active vs. passive failure detection

There are two ways to detect WAN or WWAN failure: active detection and passive detection.

- Active detection uses Digi SureLink™ technology to send probe tests to a target host or to test the status of the interface. The WAN/WWAN is considered to be down if there are no responses for a configured amount of time. See Configure SureLink active recovery to detect WAN/WWAN failures for more information about active failure detection.
- Passive detection involves detecting the WAN going down by monitoring its link status by some means other than active detection. For example, if an Ethernet cable is disconnected or the state of a cellular interface changes from **on** to **off**, the WAN is down.

Default Digi SureLink configuration

Beginning with firmware version 20.2.*x*, Surelink is enabled by default for IPv4 on all WAN and WWAN interfaces, and is configured to perform two tests on these interfaces:

- Interface connectivity.
- DNS query to the DNS servers for interface's the network connection.

  DNS servers are typically received as part of the interface's DHCP client connection, although you can manually configure the DNS servers that will be used by SureLink.

Note If your device is operating on a private APN or on wired network with firewall restrictions, ensure that the DNS servers on your private network allow DNS lookups for my.devicecloud.com; otherwise, the SureLink DNS query test will fail and the Connect IT device will determine that the interface is down.

By default, these tests will be performed every 15 minutes, with a response timeout of 15 seconds. If the tests fail three consecutive times, the device will reset the network interface to attempt to recover the connection.

Configure SureLink active recovery to detect WAN/WWAN failures

Problems can occur beyond the immediate WAN/WWAN connection that prevent some IP traffic from reaching its destination. Normally this kind of problem does not cause the Connect IT device to detect that the WAN 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 Connect IT device to regularly probe connections through the WAN to determine if the WAN has failed.

Required configuration items

- Enable SureLink.

  SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**WAN**) and WWAN (**Modem**). It is disabled for IPv6.
- The type of probe test to be performed, either:
  - Ping: Requires the hostname or IP address of the host to be pinged.
  - DNS query: You can perform a DNS query to a named DNS server, or to the DNS servers configured for the WAN.
  - HTTP or HTTPS test: Requires the URL of the host to be tested.
  - Interface status: Determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

  The preconfigured WAN is configured by default to use SureLink to both test the interface status and perform a test DNS query.

Additional configuration items

- The behavior of the Connect IT device upon test failure:
  - The default behavior, which is to fail over to the next priority WAN/WWAN.
  - Restart the WAN interface.
  - Reboot the device.
- The interval between connectivity tests.
- The number of probe attempts before the WAN 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.

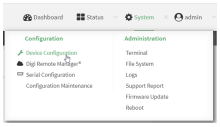
- Additional test targets.
- If more than one test target is configured, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.

To configure the Connect IT device to regularly probe connections through the WAN:

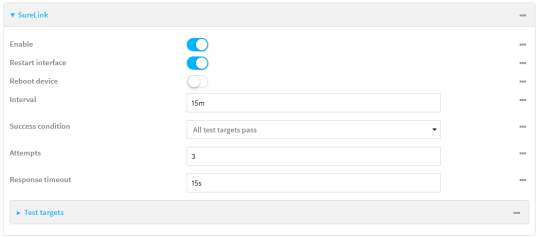
WebUI

SureLink can be configured for both IPv4 and IPv6.

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

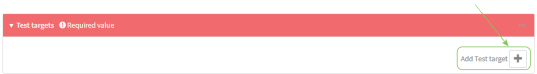


   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Create a new WAN or WWAN or select an existing one:
   - To create a new WAN or WWAN, see Configure a Wide Area Network (WAN) or Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WAN or WWAN, click to expand the appropriate WAN or WWAN.
5. After creating or selecting the WAN or WWAN, click **IPv4** (or **IPv6**) > **SureLink**.



6. **Enable** SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**WAN**) and WWAN (**Modem**). It is disabled for IPv6.
7. Click to expand **Test targets**.
8. For **Add Test Target**, click ♑



9. Select the **Test type**:
   - **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.

- **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
- **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
- **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

    The default is 60 seconds.
  - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

    The default is 60 seconds.

10. Optional active recovery configuration parameters:
    a. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
    b. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.
    c. Change the **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.
    d. If more than one test target is configured, for **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
    e. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.
    f. For **Response timeout**, type the amount of time that the device should wait for a response to a probe attempt 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. (Optional) Repeat this procedure for IPv6.

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

Command line

Active recovery can be configured for both IPv4 and IPv6. These instructions are for IPv4; to configure IPv6 active recovery, replace **ipv4** in the command line with **ipv6**.

1. Log into the Connect IT 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 WAN or WWAN, or edit an existing one:
   - To create a new WAN or WWAN, see Configure a Wide Area Network (WAN) or Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WAN or WWAN, change to the WAN or WWAN's node in the configuration schema. For example, for a WAN or WWAN named **my_wan**, change to the **my_wan** node in the configuration schema:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Enable SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (wan) and WWAN (modemwwan2). It is disabled for IPv6.

```
(config network interface my_wan> ipv4 surelink enable true
(config network interface my_wan)>
```

5. Add a test target:

```
(config network interface my_wan)> add ipv4 surelink target end
(config network interface my_wan ipv4 surelink target 0)>
```

6. Set the test type:

```
(config network interface my_wan ipv4 surelink target 0)> test value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> ping_host host
(config network interface my_wanipv4 surelink target 0)>
```

- (Optional) Set the size, in bytes, of the ping packet:

```
(config network interface my_wan ipv4 surelink target 0)> ping_size [num]
(config network interface my_wan 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 my_wan ipv4 surelinktarget 0)> dns_server ip_address
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> http_url value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_down_time value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_down_time 600s
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_timeout value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_timeout 600s
(config network interface my_wan ipv4 surelink target 0)>
```

The default is 60 seconds.

(Optional) Repeat to add additional test targets.

7. Optional active recovery configuration parameters:
   a. Move back two levels in the configuration by typing **.. ..**:

```
(config network interface my_wan ipv4 surelink target 0)> .. ..
(config network interface my_wan ipv4 surelink>
```

   b. To configure the device to restart the interface when its connection is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> restart enable
(config network interface my_wan ipv4 surelink>
```

   This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

   c. To configure the device to reboot when the interface is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> reboot enable
(config network interface my_wan ipv4 surelink>
```

   d. Set the **Interval** between connectivity tests:

```
(config network interface my_wan ipv4 surelink)> interval value
(config network interface my_wan ipv4 surelink>
```

   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 ipv4 surelink)> interval 600s
(config network interface my_wan ipv4 surelink)>
```

   The default is 15 minutes.

   e. 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:

```
(config network interface my_wan ipv4 surelink)> success_condition value
(config network interface my_wan ipv4 surelink>
```

   Where *value* is either **one** or **all**.

f. Set the number of probe attempts before the WAN is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> attempts num
(config network interface my_wan ipv4 surelink>
```

The default is **3**.

g. Set the amount of time that the device should wait for a response to a probe attempt before considering it to have failed:

```
(config network interface my_wan ipv4 surelink)> timeout value
(config network interface my_wan ipv4 surelink>
```

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 ipv4 surelink)> timeout 600s
(config network interface my_wan ipv4 surelink)>
```

The default is 15 seconds.

8. (Optional) Repeat this procedure for IPv6.
9. Save the configuration and apply the change:

```
(config network interface my_wan ipv4 surelink)> 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 reboot when a failure is detected

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

Required configuration items

- Enable SureLink.

  SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**WAN**) and WWAN (**Modem**). It is disabled for IPv6.
- Enable device reboot upon interface failure.
- The type of probe test to be performed, either:
  - Ping: Requires the hostname or IP address of the host to be pinged.
  - DNS query: You can perform a DNS query to a named DNS server, or to the DNS servers configured for the WAN.
  - HTTP or HTTPS test: Requires the URL of the host to be tested.
  - Interface status: Determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

Additional configuration items

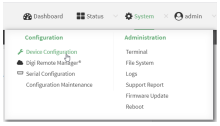
- See Configure SureLink active recovery to detect WAN/WWAN failures for optional SureLink configuration parameters.

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

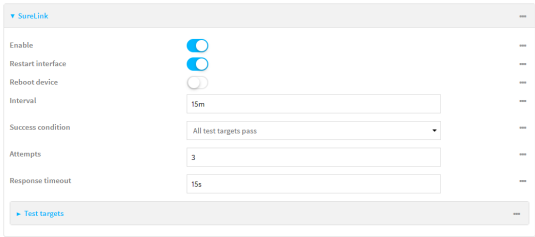
WebUI

SureLink can be configured for both IPv4 and IPv6.

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 LAN, Configure a Wide Area Network (WAN), or 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 **IPv4** (or **IPv6**) > **SureLink**.



6. **Enable** SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**WAN**) and WWAN (**Modem**). It is disabled for IPv6.
7. Enable **Reboot device**.
8. Click to expand **Test targets**.
9. For **Add Test Target**, click ♑

10. Select the **Test type**:
    - **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
    - **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
    - **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.

- **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

    The default is 60 seconds.
  - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

    The default is 60 seconds.

11. Optional active recovery configuration parameters:
    a. Change the **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.
    b. If more than one test target is configured, for **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
    c. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.
    d. For **Response timeout**, type the amount of time that the device should wait for a response to a probe attempt 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.
12. (Optional) Repeat this procedure for IPv6.
13. Click **Apply** to save the configuration and apply the change.

Command line

Active recovery can be configured for both IPv4 and IPv6. These instructions are for IPv4; to configure IPv6 active recovery, replace **ipv4** in the command line with **ipv6**.

1. Log into the Connect IT 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 LAN, Configure a Wide Area Network (WAN), or Configure a Wide Area Network (WAN) or 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_wan**, change to the **my_wan** node in the configuration schema:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Enable SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (wan) and WWAN (modemwwan2). It is disabled for IPv6.

```
(config network interface my_wan> ipv4 surelink enable true
(config network interface my_wan)>
```

5. Set the device to reboot when the interface is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> reboot true
(config network interface my_wan ipv4 surelink>
```

6. Add a test target:

```
(config network interface my_wan)> add ipv4 surelink target end
(config network interface my_wan ipv4 surelink target 0)>
```

7. Set the test type:

```
(config network interface my_wan ipv4 surelink target 0)> test value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> ping_host host
(config network interface my_wanipv4 surelink target 0)>
```

- (Optional) Set the size, in bytes, of the ping packet:

```
(config network interface my_wan ipv4 surelink target 0)> ping_size [num]
(config network interface my_wan 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 my_wan ipv4 surelinktarget 0)> dns_server ip_address
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> http_url value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_down_time value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_down_time 600s
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_timeout value
(config network interface my_wan 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 my_wan ipv4 surelink target 0)> interface_timeout 600s
(config network interface my_wan ipv4 surelink target 0)>
```

The default is 60 seconds.

(Optional) Repeat to add additional test targets.

8. Optional active recovery configuration parameters:
   a. Move back two levels in the configuration by typing **.. ..**:

```
(config network interface my_wan ipv4 surelink target 0)> .. ..
(config network interface my_wan ipv4 surelink>
```

   b. Set the **Interval** between connectivity tests:

```
(config network interface my_wan ipv4 surelink)> interval value
(config network interface my_wan ipv4 surelink>
```

   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 ipv4 surelink)> interval 600s
(config network interface my_wan ipv4 surelink)>
```

   The default is 15 minutes.

   c. 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:

```
(config network interface my_wan ipv4 surelink)> success_condition value
(config network interface my_wan ipv4 surelink>
```

   Where *value* is either **one** or **all**.

   d. Set the number of probe attempts before the WAN is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> attempts num
(config network interface my_wan ipv4 surelink>
```

   The default is **3**.

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

```
(config network interface my_wan ipv4 surelink)> timeout value
(config network interface my_wan ipv4 surelink>
```

   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 ipv4 surelink)> timeout 600s
(config network interface my_wan ipv4 surelink)>
```

   The default is 15 seconds.

9. (Optional) Repeat this procedure for IPv6.
10. Save the configuration and apply the change:

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

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

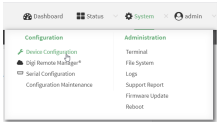
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable SureLink

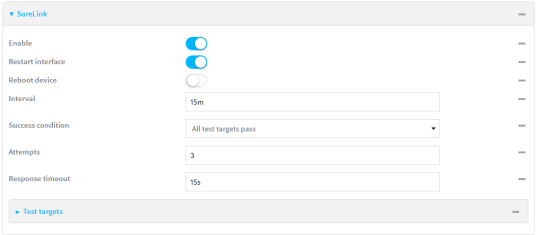
If your device uses a private APN with no Internet access, or your device has a restricted wired WAN connection that doesn't allow DNS resolution, follow this procedure to disable the default SureLink connectivity tests. You can also disable DNS lookup or other internet activity, while retaining the SureLink interface test.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 **IPv4** > **SureLink**.



6. Toggle off **Enable** to disable SureLink.
7. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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> ipv4 surelink enable false
(config network interface modem)>
```

5. Save the configuration and apply the change:

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

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

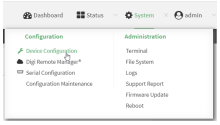
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable DNS lookup

Alternatively, you can disable DNS lookup or other internet activity for device that use a private APN with no Internet access, or that have restricted wired WAN connections that do not allow DNS resolution, while retaining the SureLink interface test. The SureLink interface test determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

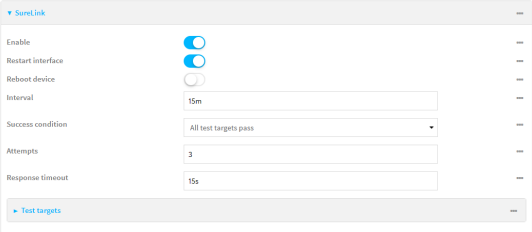
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

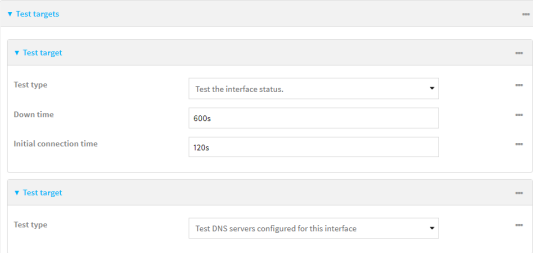


   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Select the appropriate WAN or WWAN on which SureLink should be disabled..

5. After selecting the WAN or WWAN, click **IPv4** > **SureLink**.



6. Click to expand **Test targets**.
7. Click to expand the second test target. This test target has its **Test type** set to **Test DNS servers configured for this interface**.



8. Click the menu icon **(...)** next to the target and select **Delete**.

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

Command line

1. Log into the Connect IT 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. Determine the index number of the target:

```
(config network interface modem)> show ipv4 surelink target
0
    interface_down_time 600s
    interface_timeout 120s
    test interface_up
1
    test dns_configured
(config network interface modem)>
```

5. Delete the target:

```
(config network interface modem> del ipv4 surelink target 1
(config network interface modem)>
```

6. Save the configuration and apply the change:

```
(config network interface my_wwan 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.

Example: Use a ping test for WAN failover from Ethernet to cellular

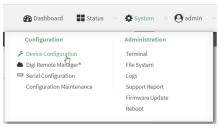
In this example configuration, the **WAN** interface serves as the primary WAN, while the cellular **Modem** interface serves as the backup WAN.

In this example configuration, SureLink is used over for the **WAN** interface to send a probe packet of size **256** bytes to the IP host **43.66.93.111** every **10** seconds. If there are three consecutive failed responses, the Connect IT device brings the **WAN** interface down and starts using the **Modem** interface. It continues to regularly test the connection to **WAN**, and when tests on **WAN** succeed, the device falls back to **ETH1**.

To achieve this WAN failover from the **WAN** to the **Modem** interface, the WAN failover configuration is:

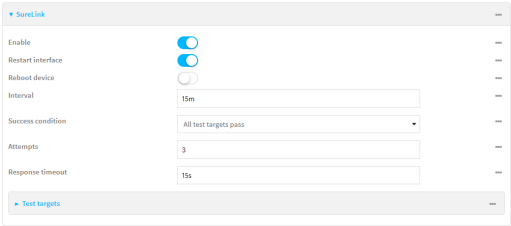
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

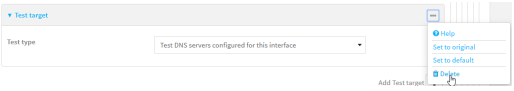


   The **Configuration** window is displayed.

3. Configure active recovery on **WAN**:
   a. Click **Network** > **Interface** > **WAN** > **IPv4** > **SureLink**.

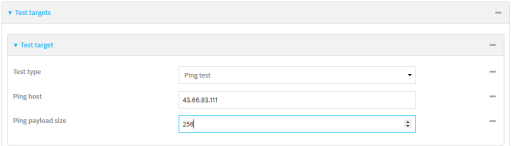


   b. For **Interval**, type **10s**.
   c. Click to expand **Test targets**.
   d. Delete the existing test targets:
      Click the menu icon **(...)** next to each target and select **Delete**.



   e. For **Add Test Target**, click ♑

   f. For **Test type**, select **Ping test**.
   g. For **Ping host**, type **43.66.93.111**.
   h. For **Ping payload size**, type **256**.



4. Repeat the above step for **Modem** to enable SureLink on that interface.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 SureLink on **WAN**:
   a. Set the interval to ten seconds:

```
(config)> network interface wan ipv4 surelink interval 10s
(config)>
```

   b. Delete the existing test targets:

```
(config network interface wan> del ipv4 surelink target 0
(config network interface wan> del ipv4 surelink target 1
(config network interface wan)>
```

   c. Add a test target:

```
(config)> add network interface wan ipv4 surelink target end
(config network interface wan ipv4 surelink target 0)>
```

   d. Set the probe type to ping:

```
(config network interface wan ipv4 surelink target 0)> test ping
(config network interface wan ipv4 surelink target 0)>
```

   e. Set the packet size to 256 bytes:

```
(config network interface wan ipv4 surelink target 0)> ping_size 256
(config network interface wan ipv4 surelink target 0)>
```

   f. Set the host to ping:

```
(config network interface wan ipv4 surelink target 0)> ping_host 43.66.93.111
(config network interface wan ipv4 surelink target 0)>
```

3. Repeat the above step for the cellular **Modem** (modem) interface to enable SureLink on that interface.
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.

Using Ethernet devices in a WAN

The Connect IT device has two Ethernet devices, named **WAN** and **LAN**. You can use these Ethernet interfaces as a WAN when connecting to the Internet, through a device such as a cable modem:

By default, the **WAN** Ethernet device is configured as a WAN, named **WAN**, with both DHCP and NAT enabled and using the **External** firewall zone. This means you should be able to connect to the Internet by connecting the **WAN** Ethernet port to another device that already has an internet connection.

The **ETH2** device is configured either as a LAN interface, named **LAN**, or for wireless-enabled Connect ITW devices, part of a bridge named **LAN1** that is used by the **LAN** interface, which uses the **Internal** firewall zone. If desired, you can assign these Ethernet devices to a WAN.

Using cellular modems in a Wireless WAN (WWAN)

The Connect IT 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 interface 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 Connect IT device cannot connect to the network using SIM1, it automatically fails over to SIM2. Connect IT devices automatically use the correct cellular module firmware for each carrier when switching SIMs.

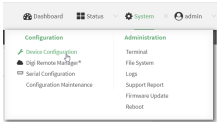
Configure cellular modem APNs

The Connect IT device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. However, you can configure the system to use a specified APN.

To configure the APN:

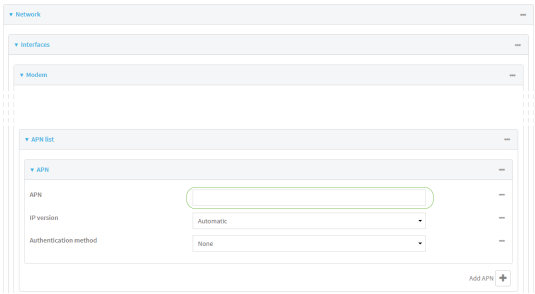
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.

3. Click **Network** > **Interfaces** > **Modem** > **APN list** > **APN**.



4. For **APN**, type the Access Point Name (APN) to be used when connecting to the cellular carrier.

5. (Optional) **IP version**:

   For **IP version**, select one of the following:

   - **Automatic**: Requests both IPv4 and IPv6 address.
   - **IPv4**: Requests only an IPv4 address.
   - **IPv6**: Requests only an IPv6 address.

   The default is **Automatic**.

6. (Optional) **Authentication method**:

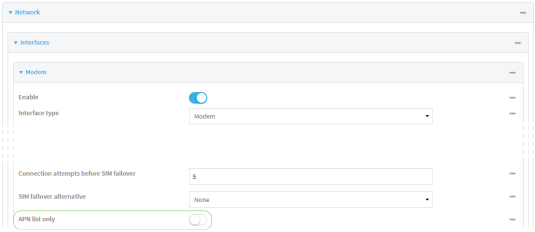
   For **Authentication method**, select one of the following:

   - **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**.

7. To add additional APNs, for **Add APN**, click ♑and repeat the preceding instructions.
8. (Optional) To configure the device to bypass its preconfigured APN list and only use the configured APNs, enable **APN list only**.



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

Command line

1. Log into the Connect IT 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 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**.

7. (Optional) To configure the device to bypass its preconfigured APN list and only use the configured APNs:

```
(config)> network interface modem modem apn_lock true
```

```
(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 cellular status and statistics

You can view a summary status for all cellular modems, or view detailed status and statistics for a specific modem.

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **Status**.
3. Under **Connections**, click **Modems**.

   The modem status window is displayed

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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
Manufacturer            : Telit
Model                : LM940
FW Version            : 24.01.541_ATT
```

```
Revision            : 24.01.541

Status
------
State               : connected
APN                 : 1234
Signal Strength     : Good (-85 dBm)
Bars                : 2/5
Access Mode         : 4G
Temperature         : 34C
IP address (IPv4)   : 10.200.1.2
Gateway (IPv4)      : 10.200.1.1

SIM
---
SIM Slot            : 1
SIM Status          : ready
IMSI                : 21685216482134
ICCID               : 26587956542156312312
SIM Provider        : AT&T

>
```

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 Connect IT device cannot make a cellular connection.

Command line

To unlock a SIM card:

1. Log into the Connect IT command line as a user with Admin access.

   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 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 Connect IT device to another location.
- Try connecting a different set of antennas, if available.
- Purchase a Digi Antenna Extender Kit:
  - Antenna Extender Kit, 1m
  - Antenna Extender Kit, 3m

AT command access

To run AT commands from the Connect IT command line:

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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 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.

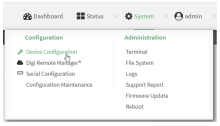
In the following example configuration, all traffic on LAN1 is routed through the public APN to the internet, and all traffic on LAN2 is routed through the private APN to the customer's data center:

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.

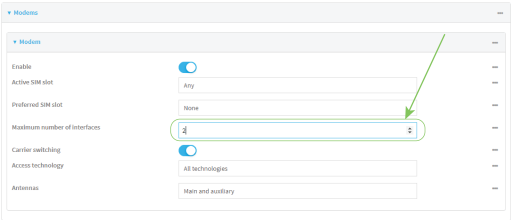
Note Dual-APN connections with the Telit LE910-NAv2 module when using a Verizon SIM are not supported. Using an AT&T SIM with the Telit LE910-NAv2 module is supported. The Telit LE910-NAv2 module is used in the 1002-CM04 CORE modem.

WebUI

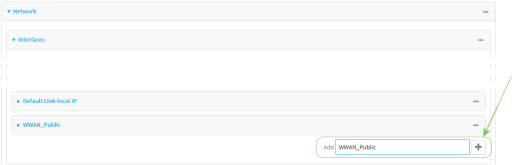
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



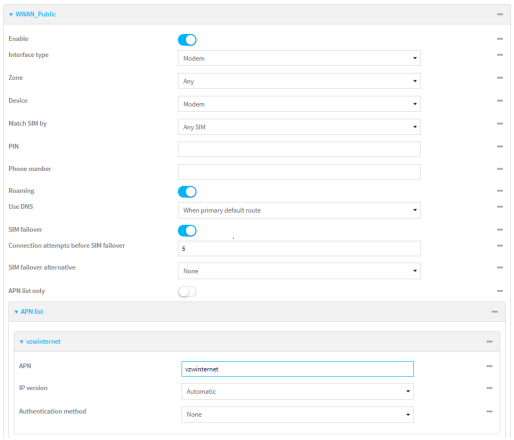
   The **Configuration** window is displayed.
3. Increase the maximum number of interfaces allowed for the modem:
   a. Click **Network** > **Modems** > **Modem**.
   b. For **Maximum number of interfaces**, type **2**.



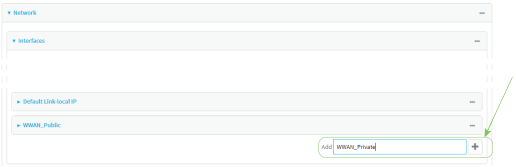
4. Create the WWAN interfaces:
   In this example, we will create two interfaces named **WWAN_Public** and **WWAN_Private**.
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface**, type **WWAN_Public** and click ♑



   c. For **Interface type**, select **Modem**.
   d. For **Zone**, select **External**.
   e. For **Device**, select **Modem** .
   f. (Optional): Configure the public APN. If the public APN is not configured, the Connect IT will attempt to determine the APN.
      i. Click to expand **APN list** > **APN**.
      ii. For **APN**, type the public APN for your cellular carrier.



g. For **Add Interface**, type **WWAN_Private** and click ♑



h. For **Interface type**, select **Modem**.

i. For **Zone**, select **External**.

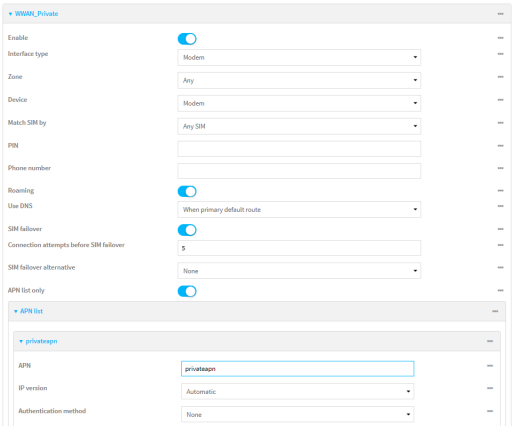
j. For **Device**, select **Modem** .

This should be the same modem selected for the **WWAN_Public** WWAN.

k. Enable **APN list only**.

l. Click to expand **APN list** > **APN**.

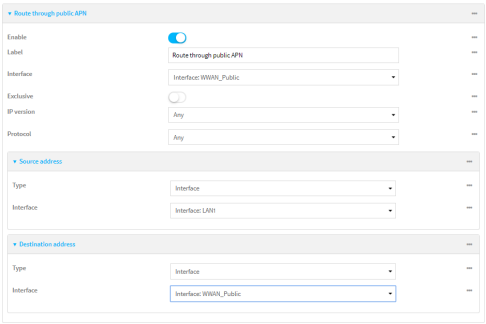
m. For **APN**, type the private APN provided to you by your cellular carrier.



5. Create the routing policies. For example, to route all traffic from LAN1 through the public APN, and LAN2 through the private APN:

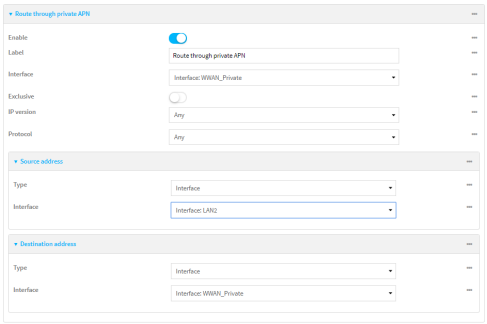
a. Click **Network** > **Routes** > **Policy-based routing**.
b. Click the ♑ to add a new route policy.

c. For **Label**, enter **Route through public APN**.
d. For **Interface**, select **Interface: WWAN_Public**.
e. Configure the source address:
   i. Click to expand **Source address**.
   ii. For **Type**, select **Interface**.
   iii. For **Interface**, select **LAN1**.
f. Configure the destination address:
   i. Click to expand **Destination address**.
   ii. For **Type**, select **Interface**.
   iii. For **Interface**, select **Interface: WWAN_Public**.



g. Click the ♑ to add another route policy.
h. For **Label**, enter **Route through private APN**.
i. For **Interface**, select **Interface: WWAN_Private**.
j. Configure the source address:
   i. Click to expand **Source address**.
   ii. For **Type**, select **Interface**.
   iii. For **Interface**, select **LAN2**.
k. 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. Log into the Connect IT 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. (Optional): Set the public APN. If the public APN is not configured, the Connect IT will attempt to determine the APN.

```
(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)> apn_lock true
(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 LAN1 through the public APN, and LAN2 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 public apn"
(config network route policy 0)>
```

c. Set the interface:

```
(config network route policy 0)> interface /network/interface/WWANPublic
(config network route policy 0)>
```

d. Configure the source address:

   i. Set the source type to **interface**:

```
(config network route policy 0)> src type interface
(config network route policy 0)>
```

   ii. Set the interface to **LAN1**:

```
(config network route policy 0)> src interface LAN1
(config network route policy 0)>
```

e. Configure the destination address:

   i. Set the type to **interface**:

```
(config network route policy 0)> dst type interface
(config network route policy 0)>
```

   ii. Set the interface to **WWANPublic** :

```
(config network route policy 0)> interface /network/interface/WWANPublic
(config network route policy 0)>
```

f. Use to periods (**..**) to move back one level in the configuration:

```
(config nnetwork route policy 0)> ..
(config nnetwork route policy)>
```

g. Add a new routing policy:

```
(config network route policy )> add end
(config network route policy 1)>
```

h. Set the label that will be used to identify this route policy:

```
(config network route policy 1)> label "Route through private apn"
(config network route policy 1)>
```

i. Set the interface:

```
(config network route policy 1)> interface /network/interface/WWANPrivate
(config network route policy 1)>
```

j. Configure the source address:

   i. Set the source type to **interface**:

```
(config network route policy 1)> src type interface
(config network route policy 1)>
```

   ii. Set the interface to **LAN2**:

```
(config network route policy 1)> src interface LAN2
(config network route policy 1)>
```

k. 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 Wide Area Network (WAN)

Configuring a Wide Area Network (WAN) involves configuring the following items:

Required configuration items

- The interface type: **Ethernet**.
- The firewall zone: **External**.
- The network device or bridge that is used by the WAN.
- Configure the WAN as a DHCP client.

Additional configuration items

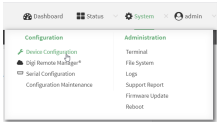
- Additional IPv4 configuration:
  - The metric for IPv4 routes associated with the WAN.
  - The relative weight for IPv4 routes associated with the WAN.
  - The IPv4 management priority of the WAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
  - The IPv4 Maximum Transmission Unit (MTU) of the WAN.
  - When to use DNS servers for this interface.
  - Whether to include the Connect IT device's hostname in DHCP requests.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- IPv6 configuration:
  - 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.
  - When to use DNS servers for this interface.
  - Whether to include the Connect IT device's hostname in DHCP requests.
  - Active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- MAC address blacklist and whitelist.

To create a new WAN or edit an existing WAN:

WebUI

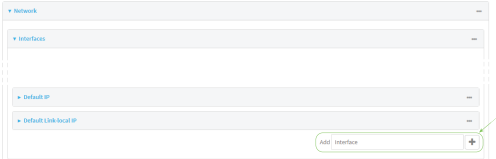
1. Log into the Connect IT WebUI as a user with full Admin access rights.

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



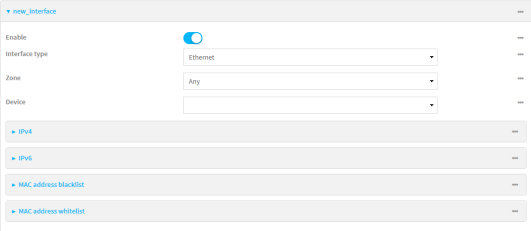
The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Create the WAN or select an existing WAN:
   - To create a new WAN, for **Add interface**, type a name for the WAN and click ♑



   - To edit an existing WAN, click to expand the WAN.

The Interface configuration window is displayed.



New WANs are enabled by default. To disable, click **Enable**.

5. For **Interface type**, leave at the default setting of **Ethernet**.
6. For **Zone**, select **External**.
7. For **Device**, select an Ethernet device or a bridge. See Bridging for more information about bridging.
8. Configure IPv4 settings:
   a. Click to expand **IPv4**.

      IPv4 support is enabled by default.

   b. For **Type**, select **DHCP address**.
   c. Optional IPv4 configuration items:
      i. Set the **Metric**.

         See Configure WAN/WWAN priority and default route metrics for further information about metrics.

      ii. 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.
      iii. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

iv. Set the **MTU**.

v. 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.

vi. Enable **DHCP Hostname** to instruct the Connect IT device to include the device's system name with DHCP requests as the Client FQDN option. The DHCP server can then be configured to register the device's hostname and IP address with an associated DNS server.

- See RFC4702 for further information about DHCP server support for the Client FQDN option.
- See Configure system information for information about setting the Connect IT device's system name.

d. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring **Active recovery**.

9. (Optional) Configure IPv6 settings:

a. Click to expand **IPv6**.

b. **Enable** IPv6 support.

c. For **Type**, select **DHCPv6 address**.

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 **Metric**.

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

g. 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.

h. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

i. Set the **MTU**.

j. For **Use DNS**:

- **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.

k. Enable **DHCP Hostname** to instruct the Connect IT device to include the device's system name with DHCP requests as the Client FQDN option. The DHCP server can then be configured to register the device's hostname and IP address with an associated DNS server.
   - See RFC4702 for further information about DHCP server support for the Client FQDN option.
   - See Configure system information for information about setting the Connect IT device's system name.

10. (Optional) Click to expand **MAC address blacklist**.

    Incoming packets will be dropped from any devices whose MAC addresses is included in the **MAC address blacklist**.

    a. Click to expand **MAC address blacklist**.
    b. For **Add MAC address**, click ♑
    c. Type the **MAC address**.

11. (Optional) Click to expand **MAC address whitelist**.

    If there whitelist entries are specified, incoming packets will only be accepted from the listed MAC addresses.

    a. Click to expand **MAC address whitelist**.
    b. For **Add MAC address**, click ♑
    c. Type the **MAC address**.

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

Command line

1. Log into the Connect IT 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 WAN or edit an existing one:
   - To create a new WAN named **my_wan**:

```
(config)> add network interface my_wan
(config network interface my_wan)>
```

   - To edit an existing WAN named **my_wan**, change to the **my_wan** node in the configuration schema:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Set the appropriate firewall zone:

```
(config network interface my_wan)> zone zone
(config network interface my_wan)>
```

See Firewall configuration for further information.

5. Select an Ethernet device or a bridge. See Bridging for more information about bridging.
   a. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface my_wan)> device ?

Current value:

(config network interface my_wan)> device
```

   b. Set the device for the LAN:

```
(config network interface my_wan)> device device
(config network interface my_wan)>
```

6. Configure IPv4 settings:
   - IPv4 support is enabled by default. To disable:

```
(config network interface my_wan)> ipv4 enable false
(config network interface my_wan)>
```

   - Configure the WAN to be a DHCP client:

```
(config network interface my_wan)> ipv4 type dhcp
(config network interface my_wan)>
```

   a. Optional IPv4 configuration items:
      i. Set the IP metric:

```
(config network interface my_wan)> ipv4 metric num
(config network interface my_wan)>
```

      See Configure WAN/WWAN priority and default route metrics for further information about metrics.

      ii. 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 my_wan)> ipv4 weight num
(config network interface my_wan)>
```

      iii. 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 my_wan)> ipv4 mgmt num
(config network interface my_wan)>
```

iv. Set the MTU:

```
(config network interface my_wan)> ipv4 mtu num
(config network interface my_wan)>
```

v. Configure how to use DNS:

```
(config network interface my_wan)> ipv4 use_dns value
(config network interface my_wan)>
```

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.

vi. Enable DHCP Hostname to instruct the Connect IT device to include the device's system name with DHCP requests as the Client FQDN option. The DHCP server can then be configured to register the device's hostname and IP address with an associated DNS server.

```
(config network interface my_wan)> ipv4 dhcp_hostname true
(config network interface my_wan)>
```

- See RFC4702 for further information about DHCP server support for the Client FQDN option.
- See Configure system information for information about setting the Connect IT device's system name.

b. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring active recovery.

7. (Optional) Configure IPv6 settings:

a. Enable IPv6 support:

```
(config network interface my_wan)> ipv6 enable true
(config network interface my_wan)>
```

b. Set the IPv6 type to DHCP:

```
(config network interface my_wan)> ipv6 type dhcpv6
(config network interface my_wan)>
```

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_wan)> ipv6 ?

IPv6

 Parameters            Current Value
 ---------------------------------------------------------------------------------
 dhcp_hostname         false          DHCP Hostname
 enable                true           Enable
 metric                0              Metric
 mgmt                  0              Management priority
 mtu                   1500           MTU
 type                  dhcpv6         Type
 use_dns               always         Use DNS
 weight                10             Weight

 Additional Configuration
 ---------------------------------------------------------------------------------
 connection_monitor    Active recovery

(config network interface my_wan)>
```

d. Modify any of the remaining default settings as appropriate. For example, to change the metric:

```
(config network interface my_wan)> ipv6 metric 1
(config network interface my_wan)>
```

If the minimum length is not available, then a longer prefix will be used.

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

8. Save the configuration and apply the change:

```
(config network interface my_wan)> 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 a Wireless Wide Area Network (WWAN)

Configuring a Wireless Wide Area Network (WWAN) involves configuring the following items:

Required configuration items

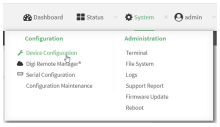
- The interface type: **Modem**.
- The firewall zone: **External**.
- The cellular modem that is used by the WWAN.

Additional configuration items

- SIM selection for this WWAN.
- The SIM PIN.
- The SIM phone number for SMS connections.
- Enable or disable roaming.
- DNS options.
- SIM failover configuration.
- APN configuration.
- The custom gateway/netmask.
- IPv4 configuration:
  - 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.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- IPv6 configuration:
  - 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.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.

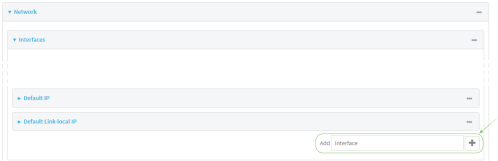
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



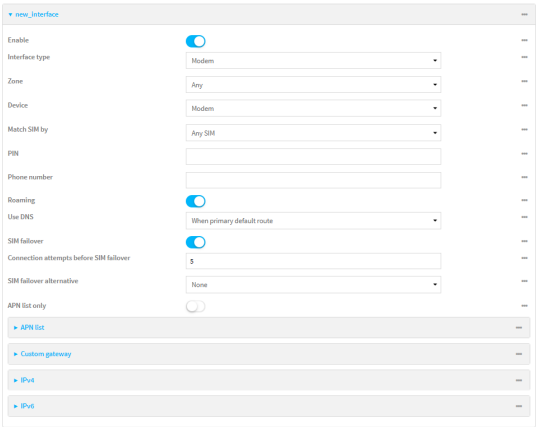
   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.

4. Create the WWAN or select an existing WWAN:
   - To create a new WWAN, for **Add interface**, type a name for the WWAN and click ♑



   - To edit an existing WWAN, click to expand the WWAN.

     New WWANs are enabled by default. To disable, click **Enable**.
5. For **Interface type**, select **Modem**.



6. For **Zone**, select **External**.
7. For **Device**, select a cellular modem.
8. Optional WWAN configuration items:
   a. 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.
   b. Type the **PIN** for the SIM. Leave blank if no PIN is required.
   c. 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.
   d. **Roaming** is enabled by default. Click to disable.

e. 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**.

f. **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:
   i. 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.
   ii. 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.

9. For **APN list** and **APN list only**, the Connect IT device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. See Configure cellular modem APNs for further information and instructions for setting an APN.
10. (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.
11. Optional IPv4 configuration items:
    a. Click **IPv4** to expand.
    b. IPv4 support is **Enabled** by default. Click to disable.
    c. Set the **Metric**.

       See Configure WAN/WWAN priority and default route metrics for further information about metrics.
    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. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring **Active recovery**.

12. Optional IPv6 configuration items:

a. Click **IPv6** to expand.

b. IPv6 support is **Enabled** by default. Click to disable.

c. Set the **Metric**.

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

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. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring **Active recovery**.

Command line

1. Log into the Connect IT 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. Optional WWAN configuration items:
   a. Set theSIM 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:

     i. 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)>
```

ii. 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**.

b. 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)>
```

c. 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.

d. Roaming is enabled by default. To disable:

```
(config network interface my_wwan)> modem roaming false
(config network interface my_wwan)>
```

e. Configure when the WWAN's DNS servers will be used:

```
(config network interface my_wwan)> modem 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**.

f. 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:

i. 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**.

ii. 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.

7. The Connect IT device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. See Configure cellular modem APNs for further information and instructions for setting an APN.

8. (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.

9. 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 metric:

```
(config network interface my_wwan)> ipv4 metric num
(config network interface my_wwan)>
```

   See Configure WAN/WWAN priority and default route metrics for further information about metrics.

   c. 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 my_wwan)> ipv4 weight num
(config network interface my_wwan)>
```

   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.

```
(config network interface my_wwan)> ipv4 mgmt num
(config network interface my_wwan)>
```

   e. Set the MTU:

```
(config network interface my_wwan)> ipv4 mtu num
(config network interface my_wwan)>
```

   f. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring active recovery.

10. Optional IPv6 configuration items:
   a. Click **IPv6** to expand.

b. IPv6 support is enabled by default. To disable:

```
(config network interface my_wwan)> ipv6 enable false
(config network interface my_wwan)>
```

c. Set the metric.

```
(config network interface my_wwan)> ipv6 metric num
(config network interface my_wwan)>
```

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

d. 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 my_wwan)> ipv6 weight num
(config network interface my_wwan)>
```

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.

```
(config network interface my_wwan)> ipv6 mgmt num
(config network interface my_wwan)>
```

f. Set the **MTU**.

```
(config network interface my_wwan)> ipv6 mtu num
(config network interface my_wwan)>
```

g. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring active recovery.

Show WAN and WWAN status and statistics

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. From the menu, click **Status**.
3. Under **Networking**, click **Interfaces**.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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
---------------- -----  -------  -------------------------------
defaultip        IPv4   up       192.168.210.1/24
defaultlinklocal IPv4   up       169.254.100.100/16
lan              IPv4   up       192.168.2.1/24
lan              IPv6   up       fd00:2704::1/48
loopback         IPv4   up       127.0.0.1/8
wan              IPv4   up       10.10.10.10/24
wan              IPv6   up       fe00:2404::240:f4ff:fe80:120/64
modem            IPv4   up       10.200.1.101/30
modem            IPv6   down

>
```

3. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific WAN. For example, to display information about WAN, enter **show network interface *wan***:

```
> show network interface wan

wan1 Interface Status
---------------------
Device            : wan
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

>
```

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

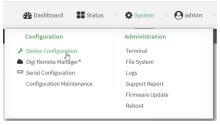
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a WAN or WWAN.

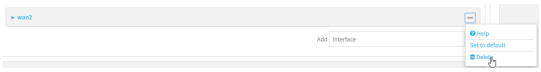
Follow this procedure to delete any WANs and WWANs that have been added to the system. You cannot delete the preconfigured WAN, **WAN**, or the preconfigured WWAN, **Modem**.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT device is preconfigured with the following Local Area Networks (LANs):

You can modify configuration settings for **LAN**, and you can create new LANs.

This section contains the following topics:

About Local Area Networks (LANs) 97
Configure a LAN 97
Example: Configure two LANs 103
Show LAN status and statistics 111
Delete a LAN 112
DHCP servers 114
Create a Virtual LAN (VLAN) route 128

About Local Area Networks (LANs)

A Local Area Network (LAN) connects network devices together, such as Ethernet or Wi-Fi, in a logical Layer-2 network.

The following diagram shows a LAN connected to the **ETH2** 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

- The interface type: either **Ethernet**, **IP Passthrough**, or **PPPoE**.
- The firewall zone: **Internal**.
- The network device or bridge 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, **LAN** 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** Ethernet device is being used by a WAN with the same IP subnet, you should change the default IP address and subnet of LAN1.

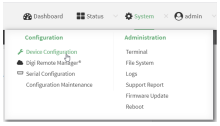
Additional configuration items

- Additional IPv4 configuration:
  - 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.
  - IPv4 DHCP server configuration. See DHCP servers for more information.
- IPv6 configuration:
  - 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.
  - The IPv6 prefix length and ID.
  - IPv6 DHCP server configuration. See DHCP servers for more information.
- MAC address blacklist and whitelist.

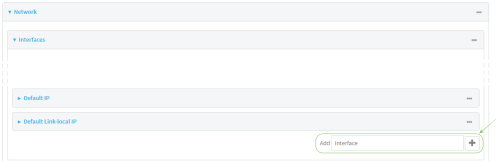
To create a new LAN or edit an existing LAN:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

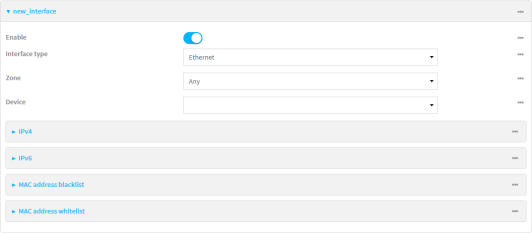


   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces**.
4. Create the LAN or select an existing LAN:
   - To create a new LAN, for **Add interface**, type a name for the LAN and click ♑



   - To edit an existing LAN, click to expand the LAN.

   The Interface configuration window is displayed.



   New LANs are enabled by default. To disable, click **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 or a bridge. See Bridging for more information about bridging.
8. 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 **Metric**.

ii. 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.

iii. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

iv. 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.

9. See Configure DHCP relay for information about configuring **DHCP relay**.

10. (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 **Metric**.

g. 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.

h. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

i. Set the **MTU**.

11. (Optional) Click to expand **MAC address blacklist**.

Incoming packets will be dropped from any devices whose MAC addresses is included in the **MAC address blacklist**.

a. Click to expand **MAC address blacklist**.

b. For **Add MAC address**, click ♑

c. Type the **MAC address**.

12. (Optional) Click to expand **MAC address whitelist**.

If there whitelist entries are specified, incoming packets will only be accepted from the listed MAC addresses.

a. Click to expand **MAC address whitelist**.

b. For **Add MAC address**, click ♑

c. Type the **MAC address**.

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

Command line

1. Log into the Connect IT 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 or a bridge. See Bridging for more information about bridging.
   a. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface my_lan)> device ?

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 IP metric:

         ```
         (config network interface my_lan)> ipv4 metric num
         (config network interface my_lan)>
         ```

      ii. 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 my_lan)> ipv4 weight num
         (config network interface my_lan)>
         ```

      iii. 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 my_lan)> ipv4 mgmt num
         (config network interface my_lan)>
         ```

      iv. 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.

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. For example, to change the minimum length of the prefix:

```
(config network interface my_lan)> ipv6 prefix_length 60
(config network interface my_lan)>
```

If the minimum length is not available, then a longer prefix will be used.

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

8. Save the configuration and apply the change:

```
(config network interface my_lan)> 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: Configure two LANs

The default configuration of the Connect IT consists of one WAN (named **ETH1**), one WWAN (**Modem**), and one LAN (**ETH2**). For Connect ITW Wi-Fi enabled devices, the default configuration of the **ETH2** uses a bridge that consists of two devices, the **ETH2** Ethernet device and the **Digi AP** Wi-Fi access point.

In this example, we will:

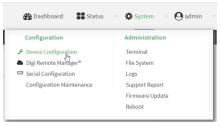
1. Create a new Wi-Fi access point (Connect ITW models only).
2. Create a new bridge that consists of the new access point and the **ETH1** device.

   In this configuration, the **ETH1** device will no longer be part of a WAN. Internet access will be provided by the cellular modem.
3. Create two new LANs:
   - **LAN1** will be configured to use the new bridge.
   - **LAN2** will be configured to use the **ETH2** device.

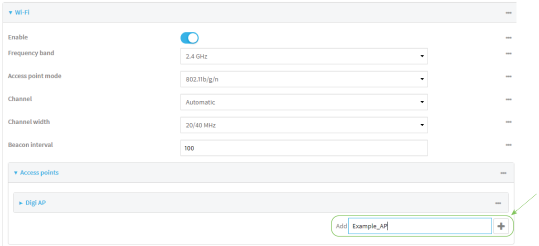
Task one: Create a new access point (Connect ITW models only)

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

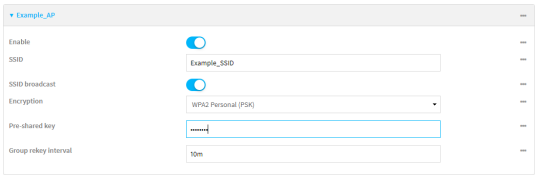


   The **Configuration** window is displayed.
3. Click **Network** > **Wi-Fi** > **Access points**.
4. For **Add Wi-Fi access point**, type **Example_AP** for the name of the new access point and click ♑



The Wi-Fi access point configuration window is displayed.

5. For **SSID**, type **Example_SSID**.
6. Type a **Pre-shared key** that clients will use to access the AP.



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

Command line

1. Log into the Connect IT 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 access point:

```
(config)> add network wifi ap Example_AP
(config network wifi ap Example_AP)>
```

   New access points are enabled by default.
4. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap Example_AP)> ssid Example_SSID
(config network wifi ap Example_AP)>
```

   SSID broadcasting is enabled by default for new access points.

5. Set the security for the access point to WPA2:

```
(config network wifi ap Example_AP)> encryption type wpa2
(config network wifi ap Example_AP)>
```

6. Set the password that clients will use when connecting to the access point:

```
(config network wifi ap Example_AP)> encryption key_psk2 password
(config network wifi ap Example_AP)>
```

7. Save the configuration and apply the change:

```
(config network wireless ap Example_AP)> save
Configuration saved.
>
```

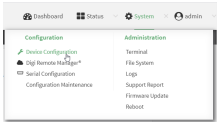
8. Type **exit** to exit the Admin CLI.

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

Task two: Create a new bridge (Connect ITW models only)

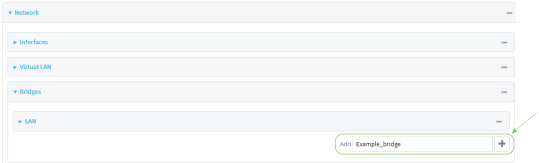
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.

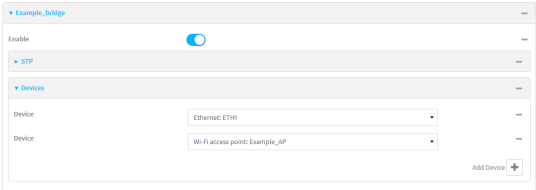
3. Click **Network** > **Bridges**.
4. For **Add Bridge**, type **Example_bridge** and click ♑



   The new bridge configuration window is displayed.

5. Click to expand **Devices**.
6. For **Add Device**, click ♑
7. For Device, select **Ethernet: ETH1**.

8. Click ♑again to add another device.
9. For Device, select **Wi-Fi access point: Example_AP**.



10. (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.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 bridge:

```
(config)> add network bridge Example_bridge
(config network bridge Example_bridge)>
```

   New access points are enabled by default.
4. Use the Tab key (twice) to determine available devices:

```
(config network bridge Example_bridge)> add device end [TAB][TAB]
/network/device/eth1          /network/device/eth2
/network/device/loopback      /network/bridge/lan
/network/wifi/ap/digi_ap      /network/wifi/ap/Example_AP
(config network bridge Example_bridge)> add device end /network/
```

5. Add the **eth1** Ethernet device:

```
(config network bridge Example_bridge)> add device end /network/device/eth1
(config network bridge Example_bridge)>
```

6. Add the **Example_AP** Wi-Fi access point:

```
(config network bridge Example_bridge)> add device end /network/wireless/ap/Example_AP
(config network bridge Example_bridge)>
```

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. Enable STP:

   ```
   (config network bridge Example_bridge)> stp enable true
   ```

   b. Set the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data:

   ```
   (config network bridge Example_bridge)> stp forward_delay num
   (config)>
   ```

   The default is **2** seconds.

8. Save the configuration and apply the change:

```
(config network bridge Example_bridge)> save
Configuration saved.
>
```

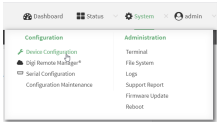
9. Type **exit** to exit the Admin CLI.

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

Task three: Create the LANs

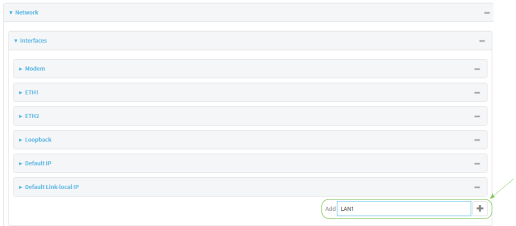
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

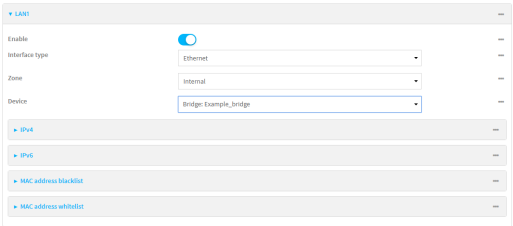


   The **Configuration** window is displayed.

3. Create **LAN1**:
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface:**, type **LAN1** and click ♑



   c. For **Zone**, select **Internal**.
   d. For **Device**:
      - If you are configuring a Wi-Fi enabled Connect ITW, select **Bridge: Example_bridge**.
      - If you are configuring a non-Wi-Fi Connect IT, select **Ethernet: ETH1**.



   e. Click to expand **IPv4**.
   f. For **Address**, type **192.168.3.1/24**.
   g. Click to expand **DHCP server**.
   h. Click **Enable**.
4. Create LAN2:
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface:**, type **LAN2** and click ♑
   c. For **Zone**, select **Internal**.
   d. For **Device**, select **Ethernet: ETH2**.
   e. Click to expand **IPv4**.
   f. For **Address**, type **192.168.4.1/24**.
   g. Click to expand **DHCP server**.
   h. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 LAN1 interface:
   a. Add the interface:

```
(config)> add network interface LAN1
(config network interface LAN1)>
```

   b. Configure the LAN1 interface:
      i. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface LAN1)> device ?

Device: The network device used by this network interface.
Format:
  /network/device/eth1
  /network/device/eth2
  /network/bridge/LAN
  /network/bridge/Example_bridge
  /network/wireless/ap/digi_ap
  /network/wireless/ap/Example_AP
Current value:

(config network interface LAN1)> device
```

      ii. Set the device for the LAN1 interface:
         - If you are configuring a Wi-Fi enabled Connect ITW, set the device to **/network/bridge/Example_bridge**.

```
(config network interface LAN1)> device /network/bridge/Example_bridge
(config network interface LAN1)>
```

         - If you are configuring a non-Wi-Fi Connect IT, set the device to **/network/device/eth1** .

```
(config network interface LAN1)> device /network/device/eth1
(config network interface LAN1)>
```

   c. Configure the firewall zone for the LAN1 interface to **internal**:

```
(config network interface LAN1)> zone internal
(config network interface LAN1)>
```

d. Configure the IPv4 address for the LAN1 interface:

```
(config network interface LAN1)> ipv4 address 192.168.3.1/24
(config network interface LAN1)>
```

e. Enable the DHCP server for the LAN1 interface:

```
(config network interface LAN1)> ipv4 dhcp_server enable true
(config network interface LAN1)>
```

4. Create the LAN2 interface:

a. Add the interface:

```
(config)> add network interface LAN2
(config network interface LAN2)>
```

b. Configure the LAN2 interface:

i. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface LAN2)> device ?

Device: The network device used by this network interface.
Format:
  /network/device/eth1
  /network/device/eth2
  /network/bridge/LAN
  /network/bridge/Example_bridge
  /network/wireless/ap/digi_ap
  /network/wireless/ap/Example_AP
Current value:

(config network interface LAN2)> device
```

ii. Set the device for the LAN2 interface:

```
(config network interface LAN2)> device /network/device/eth1
(config network interface LAN2)>
```

c. Configure the firewall zone for the LAN2 interface to **internal**:

```
(config network interface LAN2)> zone internal
(config network interface LAN2)>
```

d. Configure the IPv4 address for the LAN2 interface:

```
(config network interface LAN2)> ipv4 address 192.168.4.1/24
(config network interface LAN2)>
```

e. Enable the DHCP server for the LAN2 interface:

```
(config network interface LAN2)> ipv4 dhcp_server enable true
(config network interface LAN2)>
```

5. Save the configuration and apply the change:

```
(config network interface LAN2)> 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.

Task four: Verify the new configuration

The final step in this example is to verify the new configuration.

1. Verify that LAN1 is operating correctly:
   a. Connect a device to LAN1 through the **ETH1** Ethernet port, or by connecting to the Example_AP Wi-Fi1 access point.
   b. Verify that the device has been provided an IP address from the LAN DHCP server in the 192.168.3.* subnet.
2. Verify that LAN2 is operating correctly:
   a. Connect a device to LAN2 through the **ETH2** Ethernet port.
   b. Verify that the device has been provided an IP address from the LAN2 DHCP server in the 192.168.4.* subnet.

Show LAN status and statistics

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. From the menu, click **Status**.
3. Under **Networking**, click **Interfaces**.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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
----------------  -----  -------  -------------------------------
defaultip        IPv4   up       192.168.210.1/24
defaultlinklocal  IPv4   up       169.254.100.100/16
lan              IPv4   up       192.168.2.1/24
lan              IPv6   up       fd00:2704::1/48
loopback         IPv4   up       127.0.0.1/8
```

```
wan          IPv4   up      10.10.10.10/24
wan          IPv6   up      fe00:2404::240:f4ff:fe80:120/64
modem          IPv4   up      10.200.1.101/30
modem          IPv6   down

>
```

3. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific LAN. For example, to display information about LAN, enter **show network interface *lan***:

```
> show network interface lan

lan1 Interface Status
---------------------
Device            : lan
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)  :

>
```

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

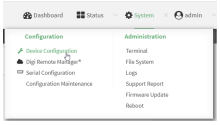
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a LAN

Follow this procedure to delete any LANs that have been added to the system. You cannot delete the preconfigured LAN, **LAN1**.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

DHCP servers

You can enable DHCP on your Connect IT 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.

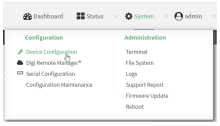
Additional configuration items

- 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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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.
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**.
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 Connect IT 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 Connect IT device's server.
   - **Custom**: Allows you to identify the IP address of the server.

f. For **Bootfile name**, type the relative path and file name of the bootfile on the TFTP server.

g. For **TFTP server** name, type the IP address or host name of the TFTP server.

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. Log into the Connect IT 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)>
```

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. 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 Connect IT 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 Connect IT 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)>
```

8. See Configure DHCP options for information about custom DHCP options.
9. See Map static IP addresses to hosts for information about static leases.
10. Save the configuration and apply the change:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease 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.

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.

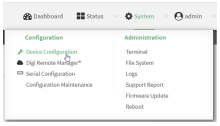
Additional configuration items

- A label for this instance of the static lease.

To map static IP addresses:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Networking**, click **DHCP Leases**.

Command line

1. Log into the Connect IT 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.

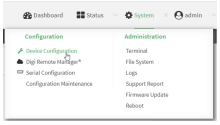
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete static IP mapping entries

To delete a static IP entry:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT 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

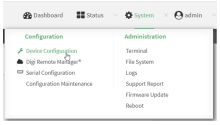
- DHCP option number.
- Value for the DHCP option.

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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, uncheck **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. Log into the Connect IT 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 Connect IT 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

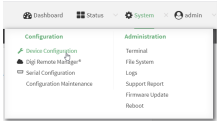
- Disable the DHCP server, if it is enabled.
- IP address of the primary DHCP relay server, to define the relay server that will respond to DHCP requests.

Additional configuration items

- IP address of additional DHCP relay servers.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.
2. 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 Connect IT device and to diagnose DHCP issues.

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Networking**, click **DHCP Leases**.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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. 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 Virtual LAN (VLAN) route

Virtual LANs (VLANs) allow splitting a single physical LAN into separate Virtual LANs. This is useful for security reasons, and also helps to reduce broadcast traffic on the LAN.

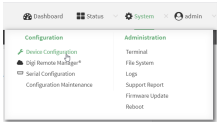
Required configuration items

- 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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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/wan
  /network/device/lan
  /network/device/loopback
  /network/vlan/vlan1
  /network/bridge/lan
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.

Bridging

Bridging is a mechanism to create a single network consisting of multiple devices, such as Ethernet devices and wireless access points.

By default, the Connect IT has the following preconfigured bridges:

You can modify configuration settings for the existing bridge, and you can create new bridges.

This section contains the following topics:

Edit the preconfigured LAN bridge 132
Configure a bridge 135

Edit the preconfigured LAN bridge

Required configuration items

- Enable or disable the bridge.
- Modify the devices included in the bridge.

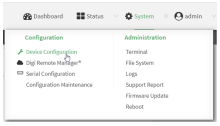
Additional configuration items

- Enable Spanning Tree Protocol (STP).

To edit the preconfigured **LAN1** bridge:

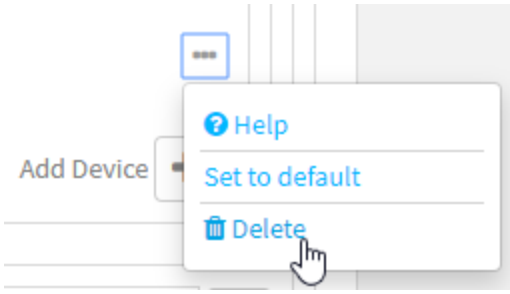
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **Bridges** > **LAN1**.
4. The **LAN1** bridge is enabled by default. To disable, uncheck **Enable**.
5. Modify the list of devices that are a part of the bridge. By default, the **LAN1** bridge includes the following devices:
   - Ethernet: LAN
   - Wi-Fi access point: Digi AP (Wi-Fi1)

   a. To delete a device from the bridge, click the down arrow (⊲) next to the field label and select **Delete**.



   b. To add a device, for **Add device**, click ♑and select the **Device**.
6. (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.

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

Command line

1. Log into the Connect IT 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 **LAN1** bridge is enabled by default.
   - To disable:

```
(config)> network bridge lan enable false
(config)>
```

   - To enable if it has been disabled:

```
(config)> network bridge lan enable true
(config)>
```

4. Modify the list of devices that are a part of the bridge. By default, the **LAN1** bridge includes the following devices:
   - Ethernet: LAN
   - Wi-Fi access point: Digi AP (Wi-Fi1)

   a. To delete a device from the bridge:
      i. Determine the index numbers of the devices included with the bridge:

```
(config)> show network bridge lan device
0 /network/device/eth2
1 /network/wireless/ap/digi_ap
(config)>
```

      ii. Use the index number to delete the appropriate device. For example, to delete the **Digi AP (Wi-Fi1)** Wi-Fi access point from the bridge:

```
(config)> del network bridge lan device
(config)>
```

Note If you are deleting multiple devices from the bridge, the device index may be reordered after each deletion. As a result, best practice is to perform a **show network bridge lan1 device** command after each device is deleted to determine the new index numbering.

b. Add devices to the bridge:

i. Determine available devices:

```
(config network bridge my_bridge)> .. .. interface lan device ?


Default value: /network/bridge/lan
Current value: /network/bridge/lan

(config network bridge my_bridge)>
```

ii. Add the appropriate device. For example, to add the **Digi AP (Wi-Fi1)** Wi-Fi access point:

```
(config network bridge my_bridge)> add device end /network/wireless/ap/digi_ap
(config)>
```

5. (Optional) Enable Spanning Tree Protocol (STP).

   STP is used when multiple LANs are configured on the same device, to prevent bridge loops and other routing conflicts.

   a. Enable STP:

```
(config)> network bridge lan stp enable true
```

   b. Set the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data:

```
(config)> network bridge lan stp forward_delay num
(config)>
```

   The default is **2** seconds.

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 a bridge

Required configuration items

- A name for the bridge.
  Bridges are enabled by default.
- Devices to be included in the bridge.

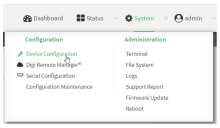
Additional configuration items

- Enable Spanning Tree Protocol (STP).

To create a bridge:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, uncheck **Enable**.
6. Add devices to the bridge:
   a. Click to expand **Devices**.
   b. For **Add device**, click ♑
   c. Select the **Device**.
   d. Repeat to add additional devices.
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. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 bridge:

```
(config)> add network bridge my_bridge
(config network bridge my_bridge)>
```

4. Bridges are enabled by default.
   - To disable:

```
(config network bridge my_bridge)> enable false
(config network bridge my_bridge)>
```

   - To enable if it has been disabled:

```
(config network bridge my_bridge)> enable true
(config network bridge my_bridge)>
```

5. Add devices to the bridge:
   a. Determine available devices:

```
(config network bridge my_bridge)> .. .. interface lan device ?


Default value: /network/bridge/lan
Current value: /network/bridge/lan

(config network bridge my_bridge)>
```

   b. Add the appropriate device. For example, to add the **Digi AP (Wi-Fi1)** Wi-Fi access point:

```
(config network bridge my_bridge)> add device end /network/wireless/ap/digi_ap
(config)>
```

6. (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. Enable STP:

```
(config network bridge my_bridge)> stp enable true
```

   b. Set the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data:

```
(config network bridge my_bridge)> stp forward_delay num
(config)>
```

The default is **2** seconds.

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.

Serial port

Connect IT devices have a single serial port that provides access to the command-line interface.

Use an RS-232 serial cable to establish a serial connection from your Connect IT to your local laptop or PC. Use a terminal emulator program to establish the serial connection. The terminal emulator's serial connection must be configured to match the configuration of the Connect IT device's serial port. The default serial port configuration for the Connect IT is:

- Enabled: **enabled**
- Serial mode: **Remote access**
- Label: **None**
- Baud rate: **9600**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**
- Flow control: **None**
- Escape sequence: **~b**
- History size: **4000**
- Exclusive access: **enabled**
- Idle timeout: **15m**

Configure the serial port

By default, the Connect IT numbered serial ports are configured as follows:

- **Enabled**
- **Serial mode**: Login
- **Label**: None
- **Baud rate**: 9600
- **Data bits**: 8
- **Parity**: None
- **Stop bits**: 1
- **Flow control**: None
- **Escape sequence**: ~
- **History size**: 4000

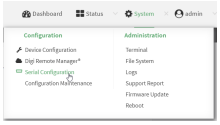
- **Exclusive access**: enabled
- **Idle timeout**: 15m

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.

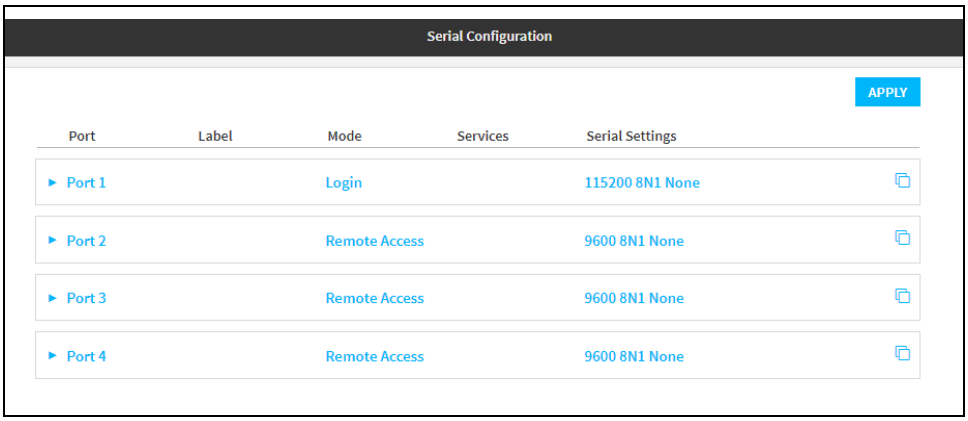
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



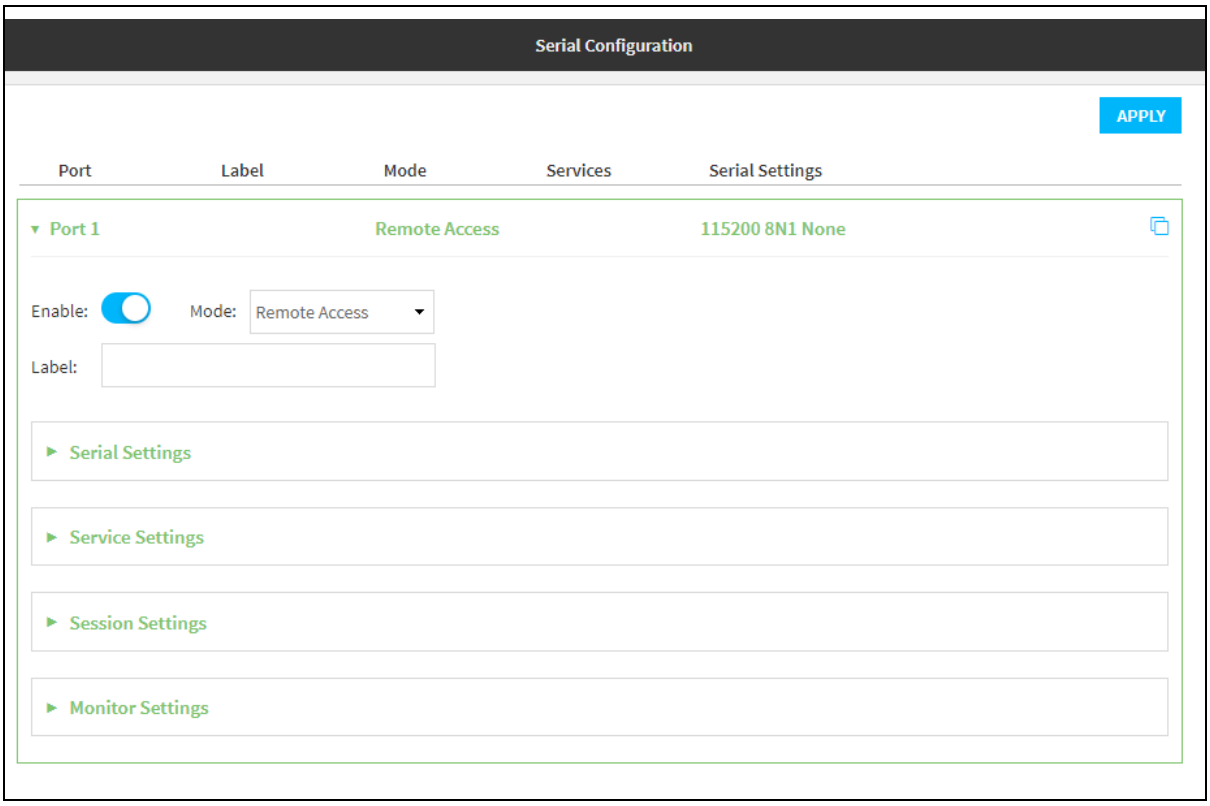
The **Serial Configuration** page is displayed.



3. Click on the port name to expand the port you want to configure.

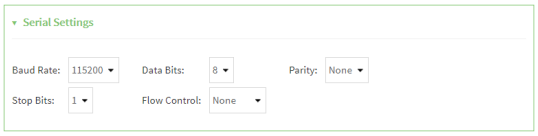
   The **Settings** section that display depend on the mode selected for the port. If **Remote Access** is selected, all sections display. If **Login** or **Power Management** are selected, only the **Serial Settings** section displays.

   Note The serial port is enabled by default. To disable the serial port, toggle off **Enable**.



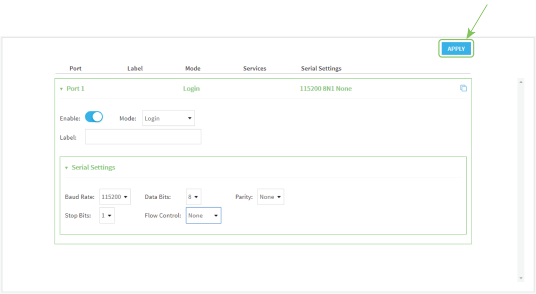
4. For **Mode**, select one of the following:
   - **Login**: Allows the user to log into the device through the serial port.
   - **Remote access**: Allows for remote access to another device that is connected to the serial port.
   - **Power Management**: Allows you to configure the port for use with a power controller. See Configure Remote Power Management.

   The default is **Remote Access**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. Click to expand **Serial Settings**.



   - For **Baud rate**, select the baud rate used by the device to which you want to connect.
   - For **Data bits**, select the number of data bits used by the device to which you want to connect.
   - For **Parity**, select the type of parity used by the device to which you want to connect.
   - For **Stop bits**, select the number of stop bits used by the device to which you want to connect.
   - For **Flow control**, select the type of flow control used by the device to which you want to connect.

7. Click to expand **Service Settings**. Within this section you can enable SSH, TCP, or Telnet. This section is available only if the **Remote Access** mode is selected.
   - **SSH**: Allow the serial port to be directly accessed using an SSH connection.
     a. Click **Enable SSH**.
     b. In the **IP Port** field, enter the IP port number on which the device will listen for SSH connections. The range is 1-65535.
     c. Click **Enable mDNS** to enable mDNS reporting for the SSH service.
   - **TCP**: Allow the serial port to be directly accessed using a TCP connection.
     a. Click **Enable TCP**.
     b. In the **IP Port** field, enter the IP port number on which the device will listen for TCP connections. The range is 1-65535.
     c. Click **Enable mDNS** to enable mDNS reporting for the TCP service.
   - **Telnet**: Allow the serial port to be directly accessed using a Telnet connection.
     a. Click **Enable Telnet**.
     b. In the **IP Port** field, enter the IP port number on which the device will listen for Telnet connections. The range is 1-65535.
     c. Click **Enable mDNS** to enable mDNS reporting for the Telnet service.
8. Click to expand **Session Settings**. Within this section you can configure the session parameters. This section is available only if the **Remote Access** mode is selected.
   - Click **Exclusive Access** if access should be limited to a single active session.
   - For **Escape Sequence**, enter the characters that can be used to start an escape sequence.
   - For **History Size**, enter the number of bytes of output from the serial port to buffer.
   - For **Idle Timeout**, enter the amount of time that the active session can be idle before the user is automatically logged out. Enter **0s** to disable the idle timeout feature.
9. Click to expand **Monitor Settings**. This section is available only if the **Remote Access** mode is selected.
   - Click **CTS Changes** to monitor CTS (Clear To Send) changes on this port.
   - Click **DCD Changes** to monitor DCD (Data Carrier Detect) changes on this port.
10. Click **Apply** to save the configuration and apply the change.



Command line

1. Log into the Connect IT 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
```

4. Set the mode:

```
(config)> serial port1 mode mode
```

   where *mode* is either:
   - **login**: Allows the user to log into the device through the serial port.
   - **remote**: Allows for remote access to another device that is connected to the serial port.
   - **powerman**: Allows you to configure the port for use with a power controller. See Configure Remote Power Management.

   The default is **login**.
5. (Optional) Set a label that will be used when referring to this port.

```
(config)> serial port1 label label
```

6. Set the baud rate used by the device to which you want to connect:

```
(config)> serial port1 baudrate rate
```

7. Set the number of data bits used by the device to which you want to connect:

```
(config)> serial port1 databits bits
```

8. Set the type of parity used by the device to which you want to connect:

```
(config)> serial port1 parity parity
```

   Allowed values are:
   - **even**
   - **odd**
   - **none**

   The default is **none**.
9. Set the stop bits used by the device to which you want to connect:

```
(config)> serial port1 stopbits bits
```

10. Set the type of flow control used by the device to which you want to connect:

```
(config)> serial port1 flow type
```

Allowed values are:

- **none**
- **rts/cts**
- **xon/xoff**

The default is **none**.

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 serial status and statistics

To show the status and statistics for the serial port:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Connections**, click **Serial**. The **Serial Status** page displays. See Serial Status page for information about the features in this page.

Command line

1. Log into the Connect IT command line as a user with Admin access.

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.

Item	Description
✸ configuration icon	Click the ✸ (configuration) icon in the upper right corner of the page to access the **Serial Configuration** page. See Configure the serial port for more information.
Status	Displays the connection status. ■ CONNECTED: A terminal, SSH, TCP, or telnet session is active. ■ 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.
Power	Displays the power status of the outlet on a power controller for which this serial port is configured as a controlled device. You can click the **ON** or **OFF** status button to turn the power to that outlet on or off. See Configure Remote Power Management and Control the outlet power from the Serial Status page.
User	When the port is connected to a terminal, SSH, TCP, or Telnet connection the name of the user logged into the device displays. See the description for Port (above) for more information.
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

Routing

This chapter contains the following topics:

IP routing 148
Show the routing table 165
Dynamic DNS 166
Virtual Router Redundancy Protocol (VRRP) 171

IP routing

The Connect IT 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 149
Delete a static route 152
Policy-based routing 153
Configure a routing policy 154
Routing services 162
Configure routing services 162

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.

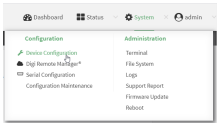
Additional configuration items

- 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:

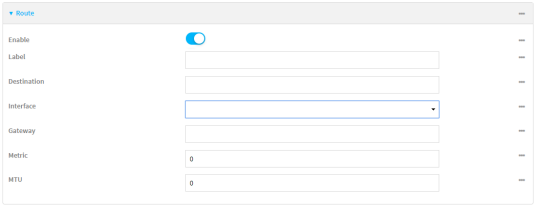
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, click to toggle **Enable** to off.
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 Connect IT 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. Log into the Connect IT 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 Connect IT device that will be used with this static route:
   a. Use the **?** to determine available interfaces:

```
(config network route static 0)> interface ?

Interface: The network interface to use to reach the destination.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config network route static 0)> interface
```

   b. Set the interface. For example:

```
(config network route static 0)> interface /network/interface/wan
(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.
>
```

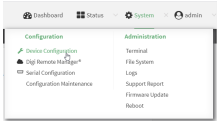
11. Type **exit** to exit the Admin CLI.

    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

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT 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 Connect IT 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.

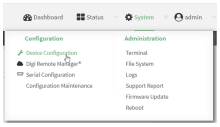
Additional configuration items

- 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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, click to toggle **Enable** to off.
5. (Optional) For **Label**, type a label that will be used to identify this route policy.

6. For **Interface**, select the interface on the Connect IT 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. 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.
11. 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.

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

Command line

1. Log into the Connect IT 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 Connect IT device that will be used with this route policy:
   a. Use the **?** to determine available interfaces:

```
(config network route policy 0)> interface ?

Interface: The network interface used to reach the destination. Packets that satisfy the
matching criteria will be routed through this interface. If the interface has a gateway then it will
be used as the next hop.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config network route policy 0)> interface
```

b. Set the interface. For example:

```
(config network route policy 0)> interface /network/interface/wan
(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:

```
(config network route policy 0)> src interface ?

Interface: The network interface.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config network route policy 0)> src interface
```

b. Set the interface. For example:

```
(config network route policy 0)> src interface /network/interface/wan
(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:

```
(config network route policy 0)> dst interface ?

Interface: The network interface.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config network route policy 0)> dst interface
```

  b. Set the interface. For example:

```
(config network route policy 0)> dst interface /network/interface/wan
(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.

Routing services

Your Connect IT includes support for dynamic routing services and protocols. The following routing services are supported:

Service or protocol	Information
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).
OSPFv2	The IPv4 Open Shortest Path First (OSPF) service supports OSPFv2 (RFC2328).
OSPFv3	The IPv6 Open Shortest Path First (OSPF) service supports OSPFv3 (RFC2740).
BGP	The Border Gateway Protocol (BGP) service supports BGP-4 (RFC1771).
Babel	The IPv4 and IPv6 Babel service.
IS-IS	The IPv4 and IPv6 Intermediate System to Intermediate System (IS-IS) service.

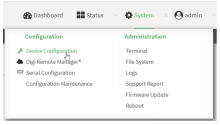
Configure routing services

Required configuration items

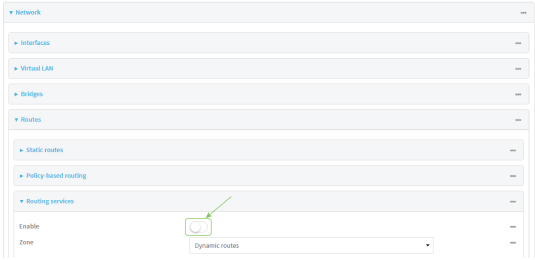
- Enable routing services.
- Enable and configure the types of routing services that will be used.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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
-------------------------------------------------------------------------------
babel                 Babel
bgp                   BGP
isis                  IS-IS
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.

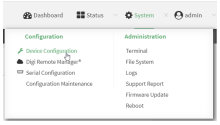
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show the routing table

To display the routing table:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT command line as a user with Admin access.

   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

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 Connect IT 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 Connect IT 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 Connect IT device.

Required configuration items

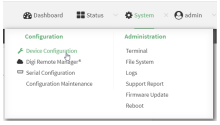
- Add a new Dynamic DNS service.
- The interface that has its IP address registered with the Dynamic DNS provider.
- The name of a Dynamic DNS provider.
- The domain name that is linked to the interface's IP address.
- The username and password to authenticate with the Dynamic DNS provider.

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.

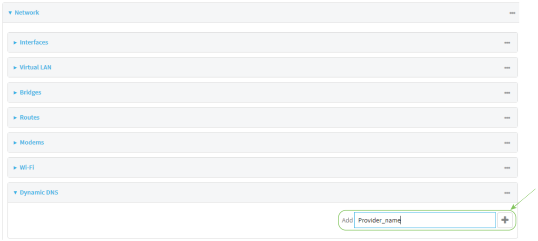
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

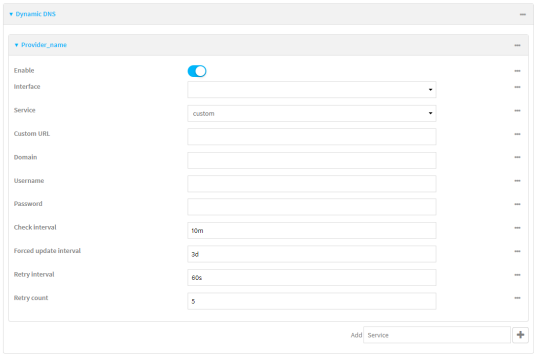


The **Configuration** window is displayed.

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, click to toggle **Enable** to off.

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. Log into the Connect IT 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:

```
(config network ddns new_ddns_instance)> interface ?

Interface: The network interface from which to obtain the IP address to register with the
dynamic DNS service.
```

```
Format:
  defaultip
  defaultlinklocal
  eth1
  eth2
  loopback
Current value:

(config network ddns new_ddns_instance)> interface
```

b. Set the interface. For example:

```
(config network ddns new_ddns_instance)> interface wan
(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 Connect IT 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.

Configure VRRP

This section describes how to configure VRRP on a Connect IT device.

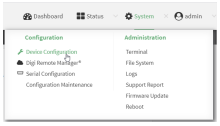
Required configuration items

- 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 that devices connected to the LAN will use as their default gateway.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.

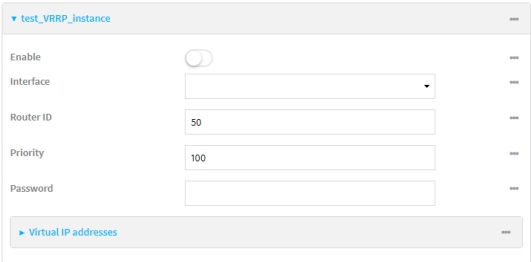
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

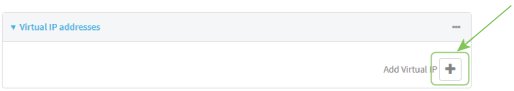
3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click ♋

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

Command line

1. Log into the Connect IT 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 new_vrrp_instance
(config network vrrp new_vrrp_instance)>
```

4. Enable the VRRP instance:

```
(config network vrrp new_vrrp_instance)> enable true
(config network vrrp new_vrrp_instance)>
```

5. Set the interface on which this VRRP instance should run:
   a. Use the **?** to determine available interfaces:

```
(config network vrrp new_vrrp_instance)> interface ?

Interface: The network interface to communicate with VRRP peers on and listen for traffic to
virtual IP addresses.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:
```

```
(config network vrrp new_vrrp_instance)> interface
```

b. Set the interface. For example:

```
(config network vrrp new_vrrp_instance)> interface /network/interface/wan
(config network vrrp new_vrrp_instance)>
```

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 new_vrrp_instance)> router_id int
(config network vrrp new_vrrp_instance)>
```

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 new_vrrp_instance)> priority int
(config network vrrp new_vrrp_instance)>
```

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 new_vrrp_instance)> password pwd
(config network vrrp new_vrrp_instance)>
```

9. Add a virtual IP address associated with this VRRP instance. This can be an IPv4 or IPv6 address.

```
(config network vrrp new_vrrp_instance)> add virtual_address end ip_address
(config network vrrp new_vrrp_instance)>
```

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.

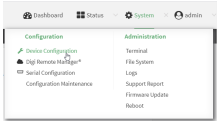
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show VRRP status and statistics

This section describes how to display VRRP status and statistics for a Connect IT device. VRRP status is available from the Web UI only.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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.

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 177
OpenVPN 209
Generic Routing Encapsulation (GRE) 239

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 modes

IPsec can run in two different modes: **Tunnel** and **Transport**.

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 Connect IT device can be configured to authenticate with the remote peer as an XAUTH client.

RSA Signatures

With RSA signatures authentication, the Connect IT 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 Connect IT 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:**
  - 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 authentication type and pre-shared key or other applicable keys and certificates.
  - 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.

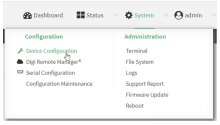
Additional configuration items

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.
- **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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

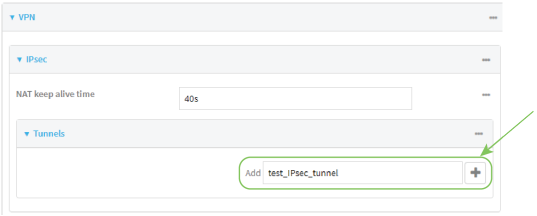


   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec**.
4. (Optional) Change the **NAT keep alive time**.

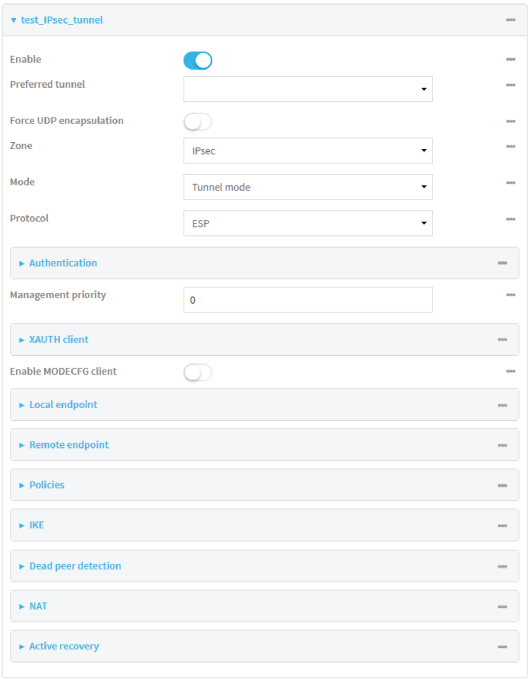
   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

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

   The default is 40 seconds.
5. Click to expand **Tunnels**.
6. For **Add IPsec tunnel**, type a name for the tunnel and click ♑



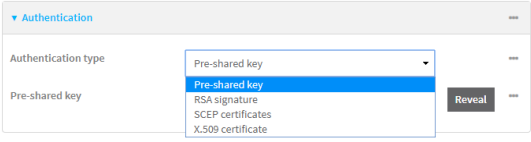
   The new IPsec tunnel configuration is displayed.



7. The IPsec tunnel is enabled by default. To disable, click **Enable**.
8. (Optional) The **Preferred tunnel** option allows you to configure IPsec failover behavior. When configuring a backup IPsec tunnel, for **Preferred tunnel**, select the primary IPsec tunnel. This instructs the backup tunnel to only start when the primary tunnel is determined to have failed. It will continue to operate until the preferred tunnel returns to full operational status.

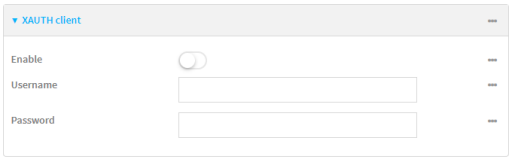
   When configuring the primary tunnel, and when configuring tunnels that will not fail over to a backup tunnel, leave this option blank.
9. (Optional) Enable **Force UDP encapsulation** to force the tunnel to use UDP encapsulation even when it does not detect that NAT is being used.
10. For **Zone**, select the firewall zone for the IPsec tunnel. Generally this should be left at the default of **IPsec**.
11. Select the Mode, 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.
12. Select the **Protocol**, either:
    - **ESP** (Encapsulating Security Payload): Provides encryption as well as authentication and integrity.
    - **AH** (Authentication Header): Provides authentication and integrity only.

13. 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**.
      - **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.
      - **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.

14. (Optional) For **Management Priority**, set the priority for this IPsec tunnel.
15. (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.
16. (Optional) Click **Enable MODECFG client** to receive configuration information, such as the private IP address, from the remote peer.

17. 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.
18. Click to expand **Remote endpoint**.
    a. For **Hostname**, select either a hostname or IP 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.
    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 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.

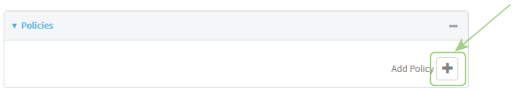
  For **FQDN ID value**, type the ID as an FQDN.
- **KeyID**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  For **KEYID ID value**, type the key ID.

19. Click to expand **Policies**.

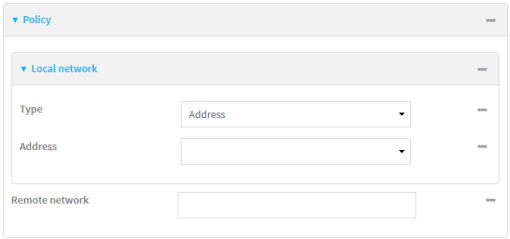
    Policies define the network traffic that will be encapsulated by this tunnel.

    a. Click to create a new policy.

    The new policy configuration is displayed.

    b. Click to expand **Local network**.

    c. For **Type**, select one of the following:
    - **Address**: The address of a local network interface.

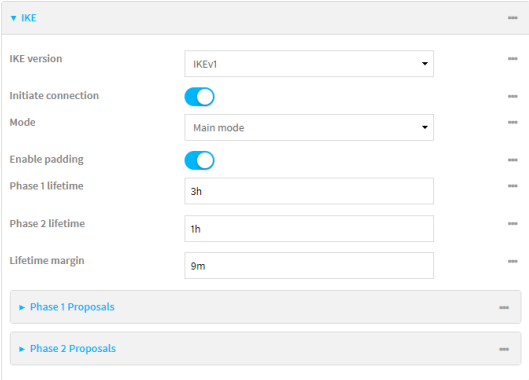
      For **Address**, select the appropriate interface.
    - **Network**: The subnet of a local network interface.

      For **Address**, select the appropriate interface.
    - **Custom network**: A user-defined network.

      For **Custom network**, enter the IPv4 address and optional netmask. The keyword **any** can also be used.
    - **Request a network**: Requests a network from the remote peer.

    d. For **Remote network**, enter the IP address and optional netmask of the remote network. The keyword **any** can also be used. .

20. 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 **Enable padding**, click to disable the padding of IKE packets. This should normally not be disabled except for compatibility purposes.
e. 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**.
f. 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**.
g. 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**.
h. 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**.

i. 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**.

21. (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.
22. (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.
23. See Configure SureLink active recovery for IPsec for information about IPsec **Active recovery**.
24. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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) Configure the device to serve as a backup IPsec tunnel.

   When configuring a backup IPsec tunnel the **ipsec_failover** parameter instructs the backup tunnel to only start when the primary tunnel is determined to have failed. It will continue to operate until the preferred tunnel returns to full operational status.

   When configuring the primary tunnel, and when configuring tunnels that will not fail over to a backup tunnel, do not set this parameter.

   a. Use the **?** to view a list of available tunnels:

```
(config vpn ipsec tunnel ipsec_example)> 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
Optional: yes
Current value:

(config vpn ipsec tunnel ipsec_example)> ipsec_failover
```

   b. Set the primary IPsec tunnel:

```
(config vpn ipsec tunnel ipsec_example)> ipsec_failover primary_ipsec_tunnel
(config vpn ipsec tunnel ipsec_example)>
```

5. (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)>
```

6. 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)>
```

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)>
```

- **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 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 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 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 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.

  Set the ID as an FQDN:

  ```
  (config vpn ipsec tunnel ipsec_example)> local id rfc822_id id
  (config vpn ipsec tunnel ipsec_example)>
  ```

- **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 keyid_id id
(config vpn ipsec tunnel ipsec_example)>
```

14. Configure the remote endpoint:
    a. Set the hostname or IP address of the remote endpoint:

```
(config vpn ipsec tunnel ipsec_example)> remote hostname value
(config vpn ipsec tunnel ipsec_example)>
```

    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.

    b. 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 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 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 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 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.

  Set the ID as an FQDN:

```
(config vpn ipsec tunnel ipsec_example)> remote id rfc822_id id
(config vpn ipsec tunnel ipsec_example)>
```

- **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 keyid_id id
(config vpn ipsec tunnel ipsec_example)>
```

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. 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)>
```

    e. 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.

f. 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.

g. 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.

h. 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**, **aes192**, **aes256**, or **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**, or **sha512**. The default is **sha1**.

iv. Set the type of Diffie-Hellman group to use for key exchange during phase 1:

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> dh_group value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

where *value* is one of **ecp384**, **modp768**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144**, or **modp8192**, . The default is **modp1024**.

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.

i. 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**, **aes192**, **aes256**, or **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**, or **sha512**. The default is **sha1**.

v. Set the type of Diffie-Hellman group to use for key exchange during phase 2:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> dh_group value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

where *value* is one of **ecp384**, **modp768**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144**, or **modp8192**, . The default is **modp1024**.

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 network policy:

```
(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:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local address ?

Address: The local network interface to use the address of. This field must be set
when 'Type' is set to 'Address'.
Format:
  defaultip
  defaultlinklocal
  eth1
  eth2
  loopback
Current value:

(config vpn ipsec tunnel ipsec_example policy 0)> local address
```

  ii. Set the interface. For example:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local address wan
(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:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local network ?

Interface: The network interface.
Format:
  defaultip
  defaultlinklocal
  eth1
  eth2
  loopback
Current value:

(config vpn ipsec tunnel ipsec_example policy 0)> local network
```

  ii. Set the interface. For example:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local network wan
(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.

d. Set the IP address and optional netmask of the remote network. The keyword **any** can also be used.

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote network value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

19. (Optional) Change the NAT keep alive time:

a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example policy 0)> ...
(config)>
```

b.

```
(config)> vpn ipsec advanced keep_alive 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 **keep_alive** to ten minutes, enter either **10m** or **600s**:

```
(config)> vpn ipsec advanced keep_alive 600s
(config)>
```

The default is 40 seconds.

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 Connect IT device to fail over from a primary IPsec tunnel to a backup tunnel.

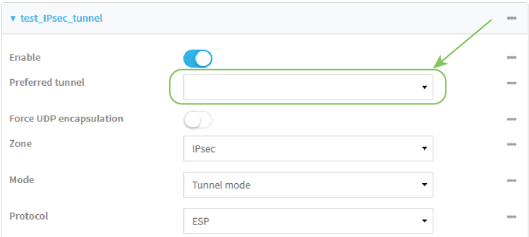
During configuration of the backup IPsec tunnel, identify the primary IPsec tunnel in the **Preferred tunnel** parameter. The **Preferred tunnel** parameter instructs the backup IPsec tunnel to start only when the preferred tunnel has been determined to have failed. It will continue to operate until the preferred tunnel returns to full operational status.

Required configuration items

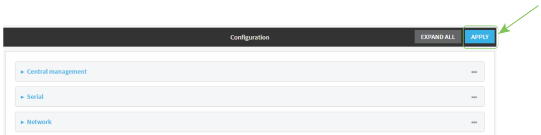
- Two configured IPsec tunnels: The primary tunnel, and the backup tunnel.
- Identify the primary tunnel during configuration of the backup tunnel.

WebUI

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.



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



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)>
```

4. Save the configuration and apply the change:

```
(config vpn ipsec tunnel backup_ipsec_tunnel)> 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 SureLink active recovery for IPsec

You can configure the Connect IT device to regularly probe IPsec client connections 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 active recovery.
- The behavior of the Connect IT device upon IPsec failure: either
  - Restart the IPsec interface
  - Reboot the device.

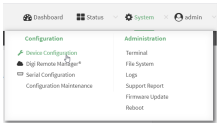
Additional configuration items

- 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 attempts before the IPsec connection 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.

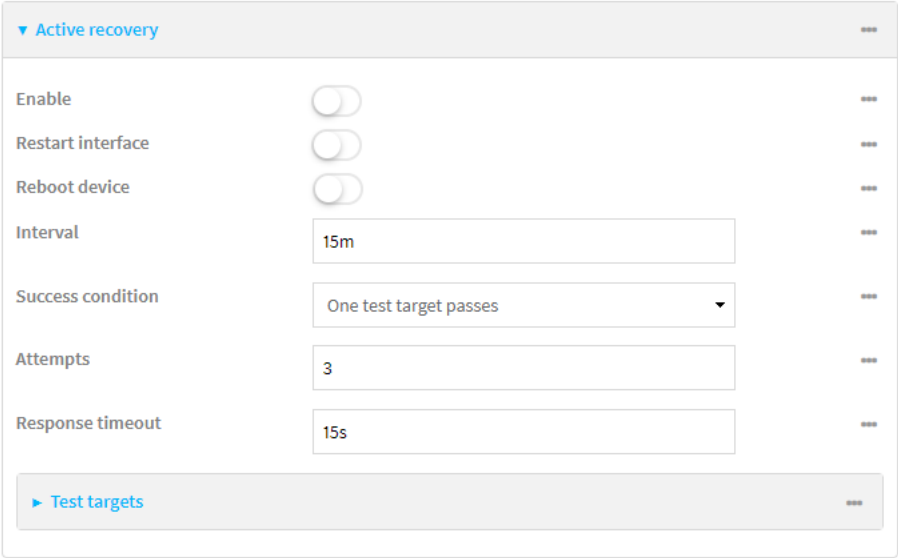
To configure the Connect IT device to regularly probe the IPsec connection:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 **Active recovery**.



6. **Enable** active recovery.
7. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
8. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.
9. Change the **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.
10. For **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
11. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.

12. For **Response timeout**, type the amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

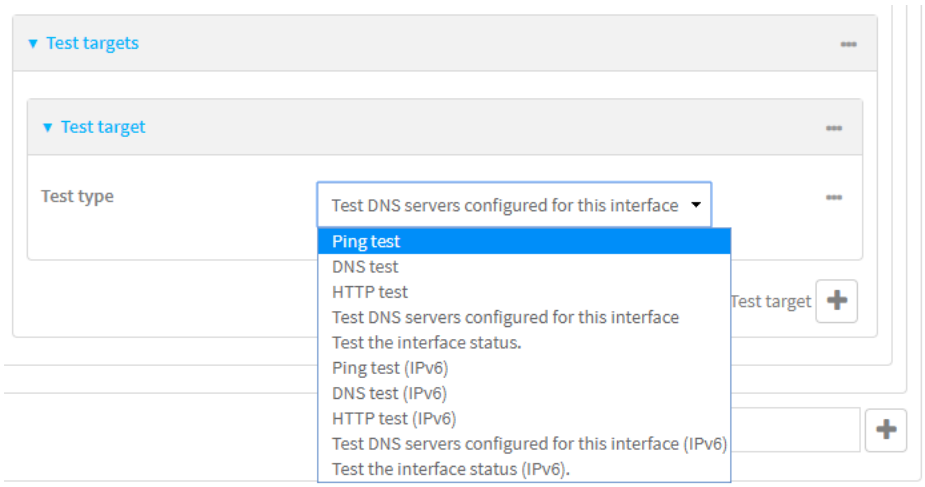
    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

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

    The default is 15 seconds.

13. Add a test target:

    a. Click to expand **Test targets**.



    b. For **Add Test target**, click ♑

    c. Select the **Test type**:

    - **Ping test** or **Ping test (IPv6)**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
    - **DNS test** or **DNS test (IPv6)**: Tests connectivity by sending a DNS query to the specified **DNS server**.
    - **HTTP test HTTP test (IPv6)**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
    - **Test DNS servers configured for this interface** or **Test DNS servers configured for this interface (IPv6)**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
    - **Test the interface status** or **Test the interface status IPv6**: The interface is considered to be down based on:
      - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

        The default is 60 seconds.

- **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

  The default is 60 seconds.

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

Command line

1. Log into the Connect IT 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 active recovery:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor enable true
(config vpn ipsec tunnel ipsec_example)>
```

5. To configure the device to restart the interface when its connection is considered to have failed:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor restart true
(config vpn ipsec tunnel ipsec_example)>
```

   This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

6. To configure the device to reboot when the interface is considered to have failed:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor reboot enable
(config vpn ipsec tunnel ipsec_example)>
```

7. Set the **Interval** between connectivity tests:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor interval 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 **interval** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor interval 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is 15 minutes.

8. Determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor success_condition value
(config vpn ipsec tunnel ipsec_example)>
```

Where *value* is either **one** or **all**.

9. Set the number of probe attempts before the WAN is considered to have failed:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor attempts num
(config vpn ipsec tunnel ipsec_example)>
```

The default is **3**.

10. Set the amount of time that the device should wait for a response to a probe attempt before considering it to have failed:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor timeout 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> connection_monitor interval 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is 15 seconds.

11. Configure test targets:
    a. Add a test target:

```
(config vpn ipsec tunnel ipsec_example)> add connection_monitor target end
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
```

    b. Set the test type:

```
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)> test value
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
```

where *value* is one of:

- **ping** (IPv4) or **ping6** (IPv6): Tests connectivity by sending an ICMP echo request to a specified hostname or IP address.
  - Specify the hostname or IP address by using **ping_host** or **ping_host6**:

    ```
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)> ping_host
    host
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
    ```

  - (Optional) Set the size, in bytes, of the ping packet by using **ping_size** or **ping_size6**:

    ```
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)> ping_size
    [num]
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
    ```

- **dns** (IPv4) or **dns6** (IPv6): 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 vpn ipsec tunnel ipsec_example connection_monitor target 0)> dns_
    server ip_address
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
    ```

- **dns_configured** (IPv4) or **dns_configured6** (IPv6): Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **http** (IPv4) or **http6** (IPv6): Tests connectivity by sending an HTTP or HTTPS GET request to the specified URL.
  - Specify the url. Allowed value uses the format **http[s]://*hostname*/[*path*]**.

    ```
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)> http_url url
    (config vpn ipsec tunnel ipsec_example connection_monitor target 0)>
    ```

- **interface_up** (IPv4) or **interface_up6** (IPv6): : 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 vpn ipsec tunnel ipsec_example connection_monitor target 0)> interface_
    down_time value
    (config vpn ipsec tunnel ipsec_example connection_monitor 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 ipsec tunnel ipsec_example connection_monitor target 0)> interface_
down_time 600s
(config ipsec tunnel ipsec_example connection_monitor 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 vpn ipsec tunnel ipsec_example connection_monitor target 0)> interface_
timeout value
(config vpn ipsec tunnel ipsec_example connection_monitor 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 my_wan ipv4 connection_monitor target 0)> interface_
timeout 600s
(config network interface my_wan ipv4 connection_monitor target 0)>
```

The default is 60 seconds.

12. Save the configuration and apply the change:

```
(config ipsec tunnel ipsec_example connection_monitor target 0)> 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.

Show IPsec status and statistics

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, select **Status** > **IPsec**.

   The **IPsec** page appears.
3. 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. Log into the Connect IT command line as a user with Admin access.

   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 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 server:

```
> 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.

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 Connect IT 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 Connect IT 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 Connect IT device supports two mechanisms for configuring an OpenVPN server in TAP mode:

- OpenVPN managed—The Connect IT 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 Connect IT 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).

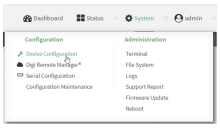
- Active recovery configuration. See Configure active recovery for OpenVPN for information about OpenVPN active recovery.

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 Connect IT device uses port **1194**.
- Access control list configuration to restrict access to the OpenVPN server through the firewall.
- Additional OpenVPN parameters.

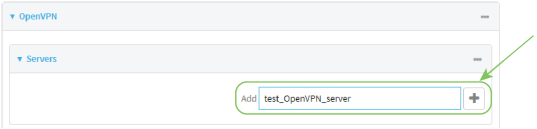
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

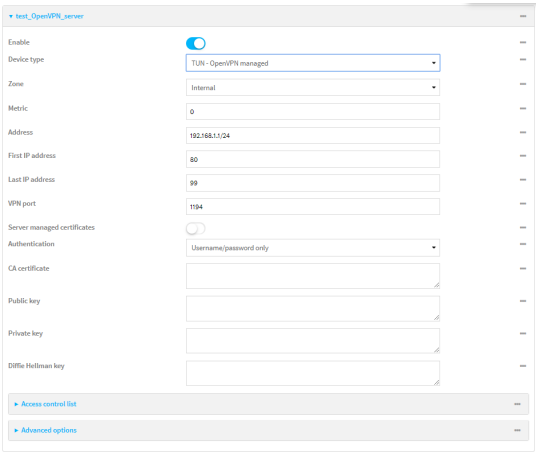


The **Configuration** window is displayed.

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, click **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 Connect IT 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**.
  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. Log into the Connect IT 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 Connect IT 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 Connect IT 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
     ----------------------------------------
      defaultip          Default IP
      defaultlinklocal      Default Link-local IP
      lan               LAN
      loopback          Loopback
      modem             Modem
      wan               WAN
     ```

```
(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
```

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 list 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.

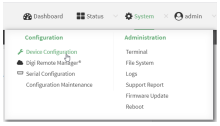
Configure an OpenVPN Authentication Group and User

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 Connect IT user authentication for more information about creating authentication groups and users.

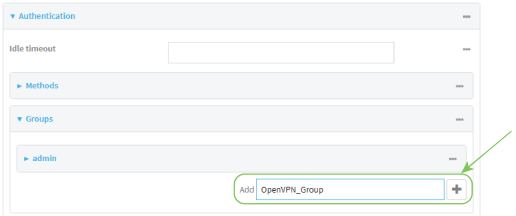
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

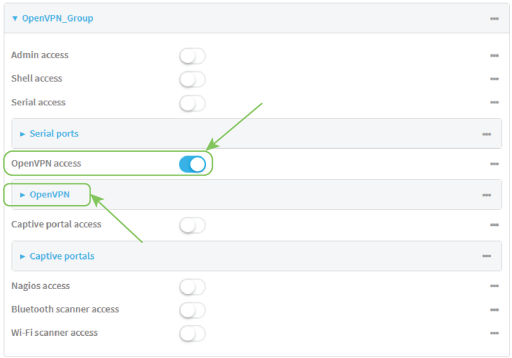


   The **Configuration** window is displayed.

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 ♑



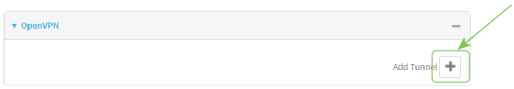
   The new authentication group configuration is displayed.



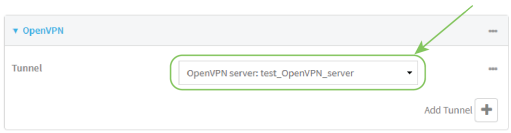
c. Click **OpenVPN access** to enable OpenVPN access rights for users of this group.

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.

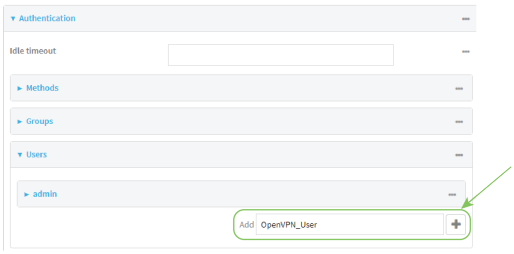


g. Repeat to add additional OpenVPN tunnels.

4. Add an OpenVPN authentication user:

a. Click **Authentication** > **Users**.

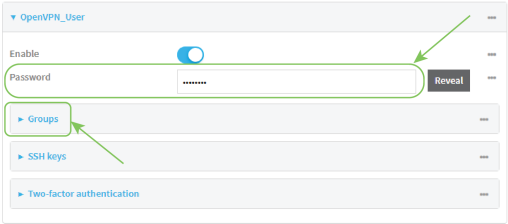
b. For **Add**, type a name for the user (for example, **OpenVPN_User**) and click



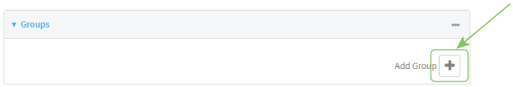
c. Type a password for the user.

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.

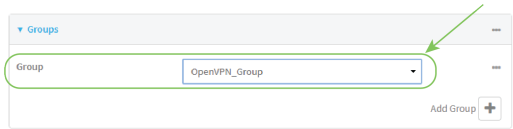
d. Click to expand the **Groups** node.



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. Log into the Connect IT 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.

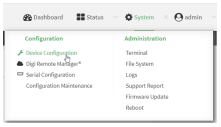
Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.

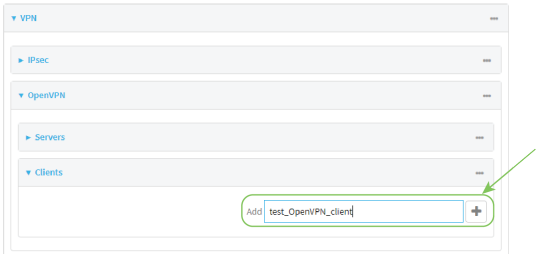
See Configure active recovery for OpenVPN for information about OpenVPN active recovery.

WebUI

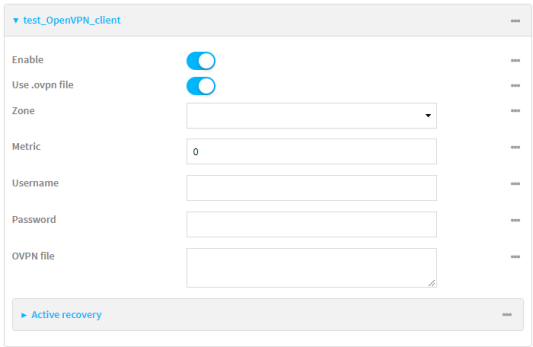
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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, click **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. Log into the Connect IT 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).

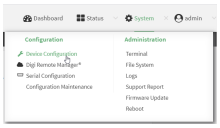
Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.
- Additional OpenVPN parameters.

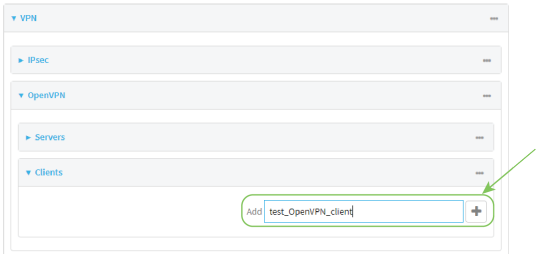
See Configure active recovery for OpenVPN for information about OpenVPN active recovery.

WebUI

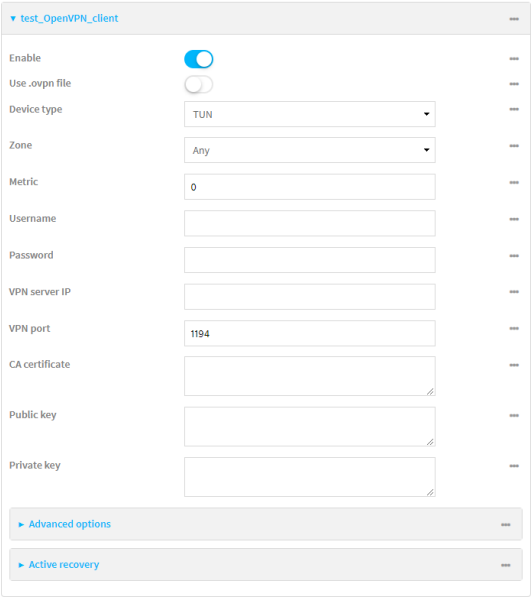
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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, click **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. Log into the Connect IT 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 active recovery for OpenVPN

You can configure the Connect IT 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 active recovery.
- The behavior of the Connect IT device upon OpenVPN failure: either
  - Restart the OpenVPN interface
  - Reboot the device.

Additional configuration items

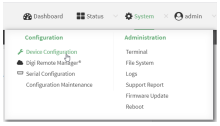
- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.
- The number of probe attempts before the OpenVPN connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

To configure the Connect IT device to regularly probe the OpenVPN connection:

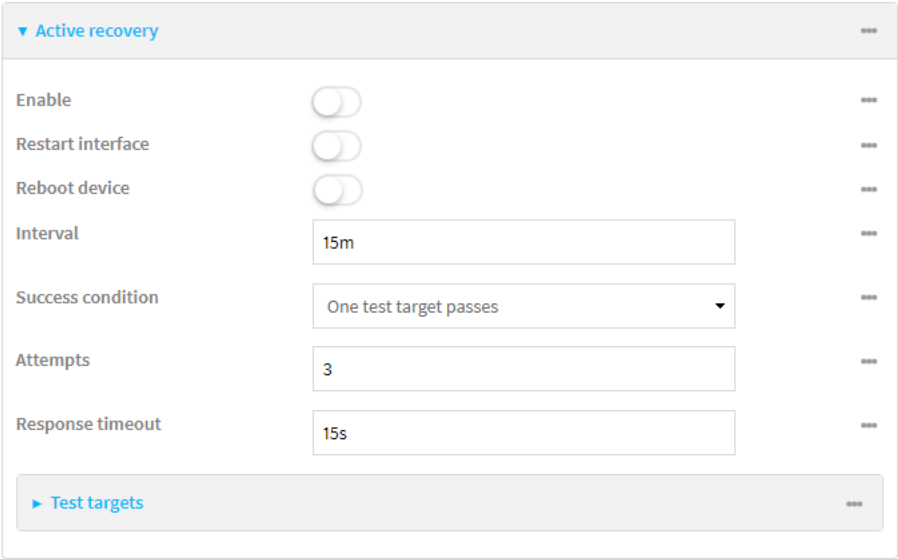
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.

2. 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 **Active recovery**.



6. **Enable** active recovery.
7. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
8. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.
9. Change the **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.
10. For **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
11. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.

12. For **Response timeout**, type the amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

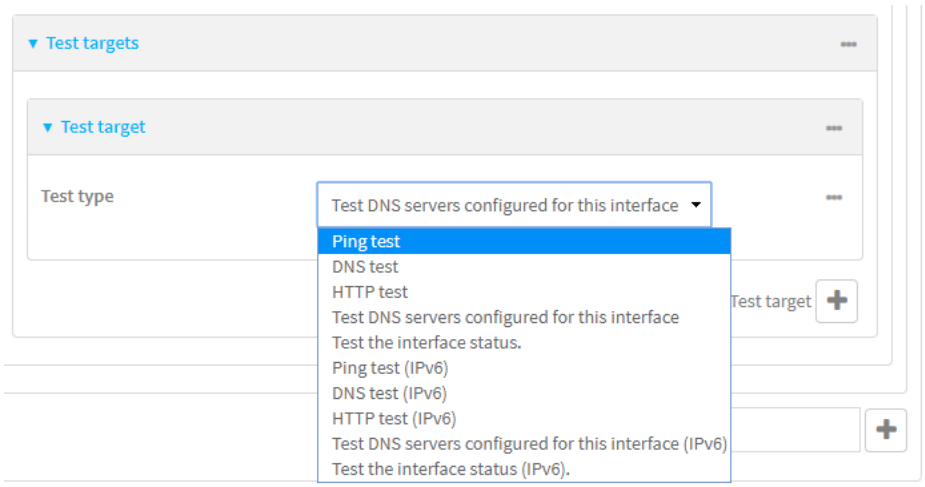
    Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}.

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

    The default is 15 seconds.

13. Add a test target:

    a. Click to expand **Test targets**.



    b. For **Add Test target**, click ♑

    c. Select the **Test type**:

    - **Ping test** or **Ping test (IPv6)**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
    - **DNS test** or **DNS test (IPv6)**: Tests connectivity by sending a DNS query to the specified **DNS server**.
    - **HTTP test HTTP test (IPv6)**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
    - **Test DNS servers configured for this interface** or **Test DNS servers configured for this interface (IPv6)**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
    - **Test the interface status** or **Test the interface status IPv6**: The interface is considered to be down based on:
      - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

        The default is 60 seconds.

- **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

  The default is 60 seconds.

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

Command line

1. Log into the Connect IT 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 active recovery:

```
(config vpn openvpn client openvpn_client1)> connection_monitor enable true
(config vpn openvpn client openvpn_client1)>
```

5. To configure the device to restart the interface when its connection is considered to have failed:

```
(config vpn openvpn client openvpn_client1)> connection_monitor restart true
(config vpn openvpn client openvpn_client1)>
```

   This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

6. To configure the device to reboot when the interface is considered to have failed:

```
(config vpn openvpn client openvpn_client1)> connection_monitor reboot enable
(config vpn openvpn client openvpn_client1)>
```

7. Set the **Interval** between connectivity tests:

```
(config vpn openvpn client openvpn_client1)> connection_monitor interval value
(config vpn openvpn client openvpn_client1)>
```

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)> connection_monitor interval 600s
(config vpn openvpn client openvpn_client1)>
```

The default is 15 minutes.

8. Determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

```
(config vpn openvpn client openvpn_client1)> connection_monitor success_condition value
(config vpn openvpn client openvpn_client1)>
```

Where *value* is either **one** or **all**.

9. Set the number of probe attempts before the WAN is considered to have failed:

```
(config vpn openvpn client openvpn_client1)> connection_monitor attempts num
(config vpn openvpn client openvpn_client1)>
```

The default is **3**.

10. Set the amount of time that the device should wait for a response to a probe attempt before considering it to have failed:

```
(config vpn openvpn client openvpn_client1)> connection_monitor timeout value
(config vpn openvpn client openvpn_client1)>
```

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)> connection_monitor interval 600s
(config vpn openvpn client openvpn_client1)>
```

The default is 15 seconds.

11. Configure test targets:
    a. Add a test target:

```
(config vpn openvpn client openvpn_client1)> add connection_monitor target end
(config vpn openvpn client openvpn_client1 connection_monitor target 0)>
```

b. Set the test type:

```
(config vpn openvpn client openvpn_client1 connection_monitor target 0)> test value
(config vpn openvpn client openvpn_client1 connection_monitor target 0)>
```

where *value* is one of:

- **ping** (IPv4) or **ping6** (IPv6): Tests connectivity by sending an ICMP echo request to a specified hostname or IP address.
  - Specify the hostname or IP address by using **ping_host** or **ping_host6**:

    ```
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)> ping_
    host host
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)>
    ```

  - (Optional) Set the size, in bytes, of the ping packet by using **ping_size** or **ping_ size6**:

    ```
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)> ping_
    size [num]
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)>
    ```

- **dns** (IPv4) or **dns6** (IPv6): 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 vpn openvpn client openvpn_client1 connection_monitor target 0)> dns_
    server ip_address
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)>
    ```

- **dns_configured** (IPv4) or **dns_configured6** (IPv6): Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **http** (IPv4) or **http6** (IPv6): Tests connectivity by sending an HTTP or HTTPS GET request to the specified URL.
  - Specify the url. Allowed value uses the format **http[s]://*hostname*/[*path*]**.

    ```
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)> http_
    url url
    (config vpn openvpn client openvpn_client1 connection_monitor target 0)>
    ```

- **interface_up** (IPv4) or **interface_up6** (IPv6): : 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 vpn openvpn client openvpn_client1 connection_monitor target 0)>
    interface_down_time value
    (config vpn openvpn client openvpn_client1 connection_monitor 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 openvpn client openvpn_client1 connection_monitor target 0)> interface_
down_time 600s
(config openvpn client openvpn_client1 connection_monitor 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 vpn openvpn client openvpn_client1 connection_monitor target 0)>
interface_timeout value
(config vpn openvpn client openvpn_client1 connection_monitor 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 my_wwan ipv4 connection_monitor target 0)> interface_
timeout 600s
(config network interface my_wwan ipv4 connection_monitor target 0)>
```

The default is 60 seconds.

12. Save the configuration and apply the change:

```
(config openvpn client openvpn_client1 connection_monitor target 0)> 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.

Show OpenVPN server status and statistics

You can view status and statistics for OpenVPN servers from either the web interface or the command line:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, select **Status** > **OpenVPN** > **Servers**.

   The **OpenVPN Servers** page appears.
3. 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. Log into the Connect IT command line as a user with Admin access.

   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     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
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:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, select **Status** > **OpenVPN** > **Clients**.

   The **OpenVPN Clients** page appears.
3. 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. Log into the Connect IT command line as a user with Admin access.

   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 server:

```
> show openvpn client name OpenVPN_client1
```

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.

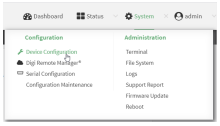
Additional configuration items

- A GRE key.
- Enable the device to respond to keepalive packets.

Task One: Create a GRE loopback endpoint interface

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, or to enable if it has been disabled, click **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. Log into the Connect IT 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.
>
```

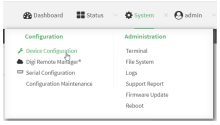
8. Type **exit** to exit the Admin CLI.

   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

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, or to enable if it has been disabled, click **Enable**.
6. For **Local endpoint**, select the GRE endpoint interface created in Task One.
7. For **Remote endpoint**, type the IP address of the GRE endpoint on the remote peer.
8. (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 interger between 0 and 4294967295, or an IP address.
9. (Optional) **Enable keepalive reply** to enable the device to reply to Cisco GRE keepalive packets.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 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)>
```

5. 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)>
```

6. (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 interger between 0 and 4294967295, or an IP address.

7. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

```
(config vpn iptunnel gre_example)> keepalive true
(config vpn iptunnel gre_example)>
```

8. Save the configuration and apply the change:

```
(config vpn iptunnel gre_example)> 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 GRE tunnels

To view information about currently configured GRE tunnels:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **Status** > **IP tunnels**.

   The **IP Tunnels**page appears.
3. To view configuration details about a GRE tunnel, click the ✸ (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Log into the Connect IT 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 vpn iptunnel** command:

```
(config)> show vpn iptunnel
gre_tunnel
    enable true
    keepalive false
    no key
    local /network/interface/gre_endpoint
    remote 172.168.1.2
    type gre
(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.

Example: GRE tunnel over an IPSec tunnel

The Connect IT 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 Connect IT device with a GRE tunnel through IPsec.

Connect IT-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 Connect IT-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 Connect IT-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**.

Connect IT-2 configuration tasks

1. Create an IPsec tunnel named **ipsec_gre2** with:
   - The same pre-shared key as the **ipsec_gre1** tunnel on Connect IT-1.
   - **Remote endpoint** set to the public IP address of Connect IT-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**.

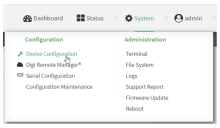
3. Create a GRE tunnel named **gre_tunnel2**:
   a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec_endpoint2**.
   b. Remote endpoint set to the IP address of the GRE tunnel on Connect IT-1, **172.30.0.1**.
4. Create an interface named **gre_interface2** and add it to the 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, **172.31.1.1/30**.

Configuration procedures

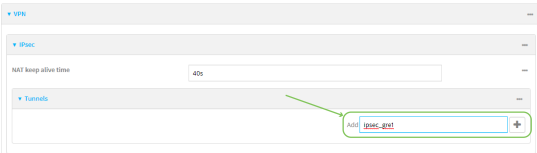
Configure the Connect IT-1 device
Task one: Create an IPsec tunnel

WebUI

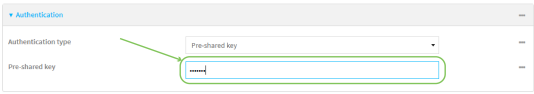
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



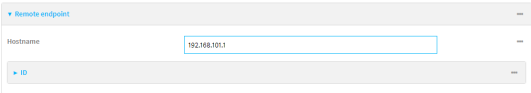
   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec** > **Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec_gre1** and click ♑



5. Click to expand **Authentication**.
6. For **Pre-shared key**, type **testkey**.

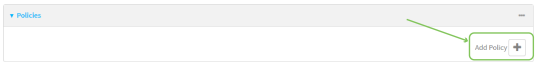


7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the Connect IT-2 device.

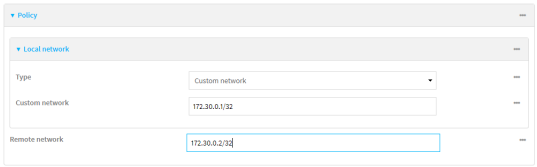


9. Click to expand **Policies**.

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. Log into the Connect IT 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 Connect IT-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:

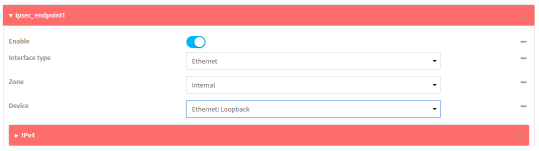
```
(config ipsec tunnel ipsec_gre1 policy 0)> save
Configuration saved.
>
```

Task two: Create an IPsec endpoint interface

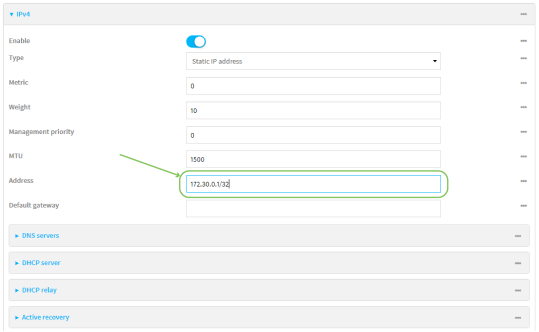
WebUI

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.
>
```

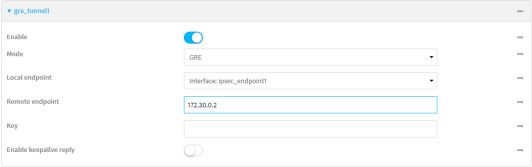
Task three: Create a GRE tunnel

WebUI

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 Connect IT-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 Connect IT-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:

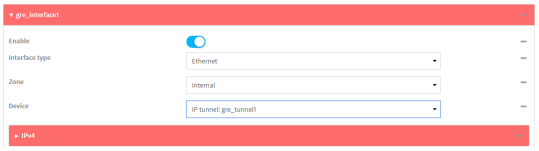
```
(config vpn iptunnel gre_tunnel1)> save
Configuration saved.
>
```

Task four: Create an interface for the GRE tunnel device

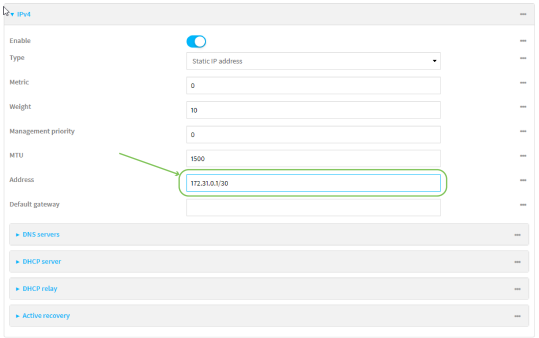
WebUI

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.
>
```

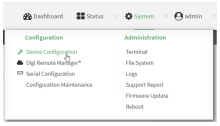
7. Type **exit** to exit the Admin CLI.

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

Configure the Connect IT-2 device
Task one: Create an IPsec tunnel

WebUI

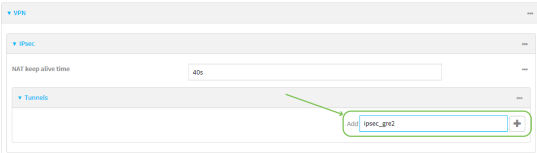
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



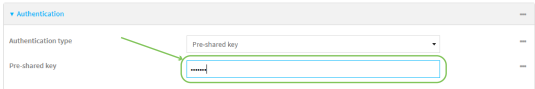
   The **Configuration** window is displayed.

3. Click **VPN** > **IPsec** > **Tunnels**.

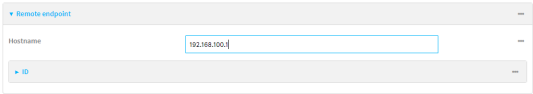
4. For **Add IPsec Tunnel**, type **ipsec_gre2** and click ♑



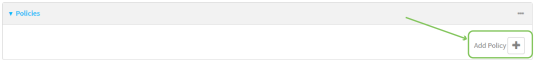
5. Click to expand **Authentication**.
6. For **Pre-shared key**, type the same pre-shared key that was configured for the Connect IT-1 (**testkey**).



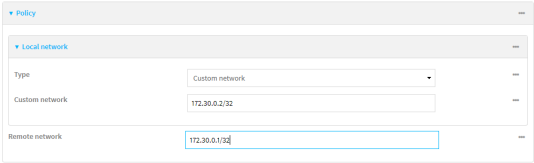
7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the Connect IT-1 device.



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. Log into the Connect IT 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 Connect IT-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 Connect IT-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)>
```

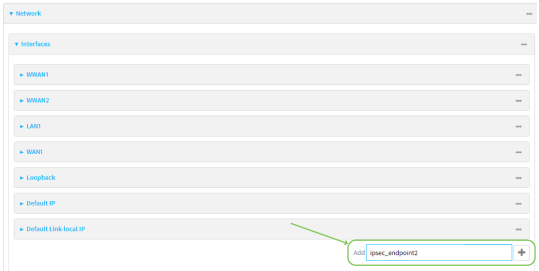
10. Save the configuration and apply the change:

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> save
Configuration saved.
>
```

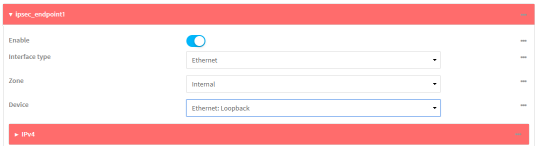
Task two: Create an IPsec endpoint interface

WebUI

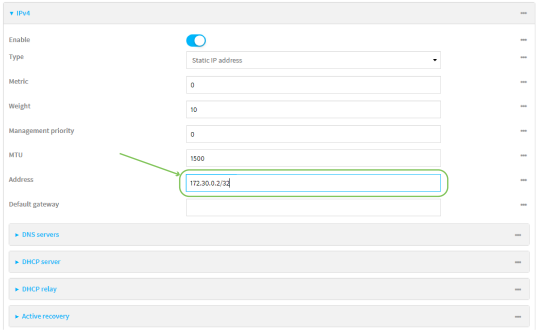
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **ipsec_endpoint2** and click ♑



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:

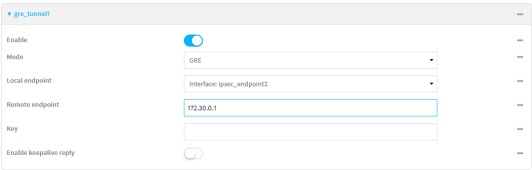
```
(config vpn ipsec tunnel ipsec_endpoint2)> save
Configuration saved.
>
```

Task three: Create a GRE tunnel

WebUI

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 Connect IT-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 Connect IT-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.
>
```

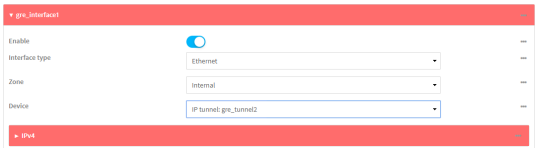
Task four: Create an interface for the GRE tunnel device

WebUI

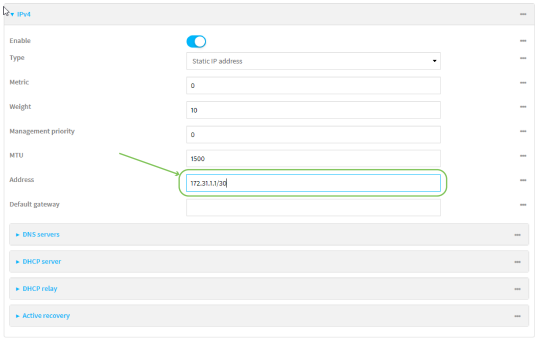
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **gre_interface2** and click ♑

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 **172.31.1.1/30** 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_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 **172.31.0.1/30** as the virtual IP address on the GRE tunnel:

```
(config network interface gre_interface2)> ipv4 address 172.31.1.1/30
(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.

Services

This chapter contains the following topics:

Allow remote access for web administration and SSH 261
Configure the web administration service 264
Configure SSH access 271
Use SSH with key authentication 277
Configure telnet access 279
Configure DNS 283
Simple Network Management Protocol (SNMP) 291
System time 297
Configure the system time 297
Network Time Protocol 299
Configure the device as an NTP server 300
Configure a multicast route 306
Enable service discovery (mDNS) 309
Use the iPerf service 312

Allow remote access for web administration and SSH

By default, only devices connected to the Connect IT's LAN have access to the device via web administration and SSH. To enable these services for access from remote devices:

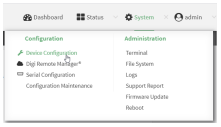
- The Connect IT device must have a publicly reachable IP address.
- The **External** firewall zone must be added to the web administration or SSH service. See Firewall configuration for information on zones.
- See Set the idle timeout for Connect IT users for information about setting the inactivity 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

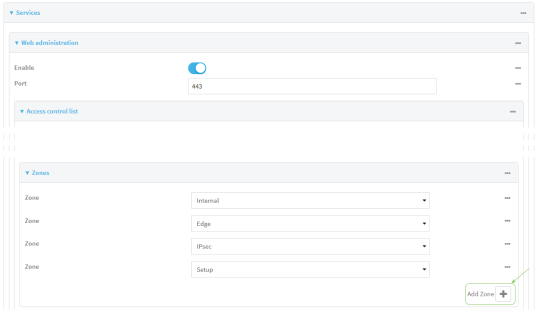
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

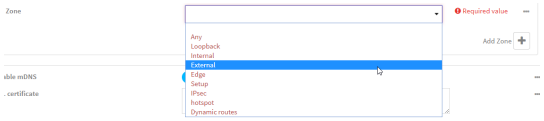


The **Configuration** window is displayed.

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. Log into the Connect IT 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.
>
```

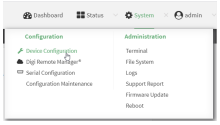
5. Type **exit** to exit the Admin CLI.

   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

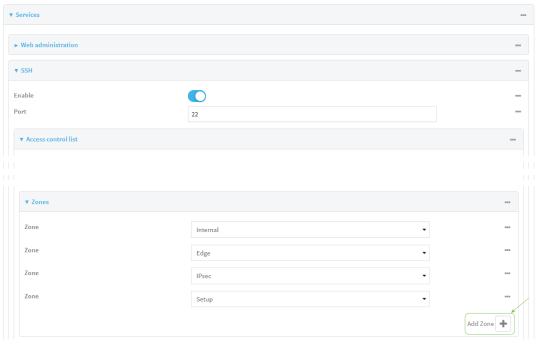
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

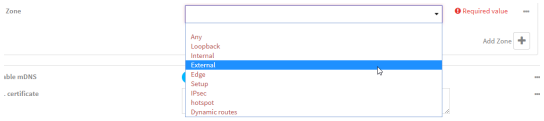


   The **Configuration** window is displayed.
3. Click **Configuration** > **Services** > **SSH** > **Access Control List** > **Zones**.

4. For **Add Zone**, click ♑



5. Select **External**.



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

Command line

1. Log into the Connect IT 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 Connect IT 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 Connect IT'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.

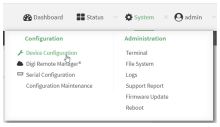
See Set the idle timeout for Connect IT users for information about setting the inactivity timeout for the web administration services.

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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.
>
```

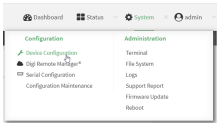
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
  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, type the certificate and private key in PEM format. If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
8. For **Allow legacy encryption protocols**, enable this option to allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.
9. **View** is set to **Auto** by default and normally should not be changed.
10. **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**.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Connect IT 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
-----------------------------------------
defaultip          Default IP
defaultlinklocal     Default Link-local IP
lan              LAN
loopback           Loopback
modem              Modem
wan              WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service web_admin acl zone end value
```

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 list additional firewall zones.

4. (Optional) If you have your own signed SSL certificate, set the certificate and private key in PEM format. If not set, the device will use an automatically-generated key.

```
(config)> service web_admin cert cert.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 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) Configure the device to allow legacy encryption protocols.

   Legacy encryption protocols allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.

To enable legacy encryption protocols:

```
(config)> service web_admin legacy_encryption true
(config)>
```

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 Connect IT'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.

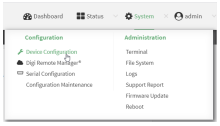
See Set the idle timeout for Connect IT users for information about setting the inactivity timeout for the SSH service.

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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.
>
```

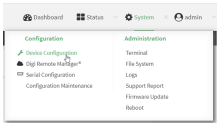
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
  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. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Connect IT 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
     ----------------------------------------
     defaultip          Default IP
     defaultlinklocal     Default Link-local IP
     lan              LAN
     loopback           Loopback
     modem              Modem
     ```

```
wan             WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service ssh acl zone end value
```

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 list 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. 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.

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 Connect IT 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 Connect IT 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

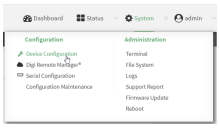
- Name for the user
- SSH public key for the user

Additional configuration items

- If you want to access the Connect IT 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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

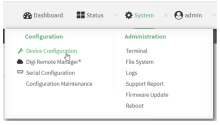
See Set the idle timeout for Connect IT users for information about setting the inactivity timeout for the telnet service.

Enable the telnet service

The telnet service is disabled by default. To enable the service:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.
>
```

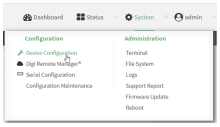
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
  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. Log into the Connect IT 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 Connect IT 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
-----------------------------------------
 defaultip          Default IP
 defaultlinklocal      Default Link-local IP
 lan               LAN
 loopback           Loopback
 modem              Modem
 wan               WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service telnet acl zone end value
```

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 list 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 Connect IT 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.

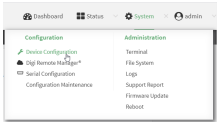
Additional configuration items

- 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.

To configure the DNS server:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
     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 **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 **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) 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.
10. (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.
11. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Connect IT 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
     ----------------------------------------
      defaultip          Default IP
      defaultlinklocal      Default Link-local IP
      lan               LAN
      loopback            Loopback
      modem               Modem
      wan               WAN

     (config)>
     ```

     Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service dns acl zone end value
```

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 list 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) 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)>
```

9. (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)>
```

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.

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 Connect IT device supports SNMPv3, read-only mode. SNMPv1 and v2 are not supported.

SNMP Security

By default, the Connect IT device automatically blocks SNMP packets from being received over WAN and LAN interfaces. As a result, if you want a Connect IT 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).

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.

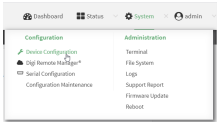
Additional configuration items

- The port used by the SNMP agent.
- Authentication type (either MD5 or SHA).
- Privacy protocol (either DES or AES).
- Privacy passphrase, if different that the SNMP user password.
- Enable Multicast DNS (mDNS) support.

To configure the SNMP agent on your Connect IT device:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
  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 **SHA**. 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 **AES**. The default is **DES**.
13. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Connect IT 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
-------------------------------------------
 defaultip            Default IP
 defaultlinklocal      Default Link-local IP
 lan                LAN
 loopback            Loopback
 modem               Modem
 wan                WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service snmp acl zone end value
```

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 list 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 **SHA**. The default is **MD5**.

```
(config)> service snmp auth_type SHA
(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 **AES**. The default is **DES**.

```
(config)> service snmp privacy_protocol AES
(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.

Download MIBs

This procedure is available from the WebUI only.

Required configuration items

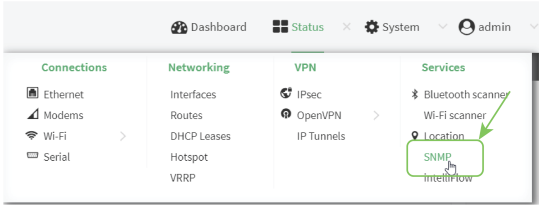
- Enable SNMP.

To download a .zip archive of the SNMP MIBs supported by this device:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. Enable SNMP.

   See Configure Simple Network Management Protocol (SNMP) for information about enabling and configuring SNMP support on the Connect IT device.
3. On the main menu, click **Status**. Under **Services**, click **SNMP**.



   The **SNMP** page is displayed.

4. Click **Download**.

System time

By default, the Connect IT device synchronizes the system time by periodically connecting to the Digi NTP server, **time.devicecloud.com**. In this mode, the device queries the time server based on following events and schedule:

- At boot time.
- Once a day.

The default configuration has the system time zone set to UTC. No additional configuration is required for the system time if the default configuration is sufficient. However, you can change the default time zone and the default NTP server, as well as configuring additional NTP servers. 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 system time for details about changing the default configuration.

The Connect IT device can also be configured to use Network Time Protocol (NTP). In this configuration, the device serves as an NTP server, providing NTP services to downstream devices. See Network Time Protocol for more information about NTP server support.

Configure the system time

This procedure is optional.

The Connect IT device's default system time configuration uses the Digi NTP server, **time.devicecloud.com**, and has the time zone set to **UTC**. You can change the default NTP server and the default time zone, as well as configuring additional NTP servers.

Required Configuration Items

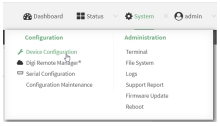
- The time zone for the Connect IT device.
- At least one upstream NTP server for synchronization.

Additional Configuration Options

- Additional upstream NTP servers.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **System** > **Time**
4. (Optional) Select the **Timezone** for the location of your Connect IT device.
5. (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 ♑
  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 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.

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

Command line

1. Log into the Connect IT 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 timezone for the location of your Connect IT 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)>
```

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
     ```

   - 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 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.

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.

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 Connect IT 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**.

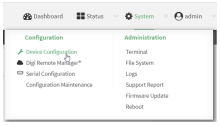
Additional Configuration Options

- Additional upstream NTP servers.
- Access control list to limit downstream access to the Connect IT device's NTP service.
- The time zone setting, if the default setting of UTC is not appropriate.

To configure the Connect IT device's NTP service:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Services** > **NTP**.
4. Enable the Connect IT device's NTP service by clicking **Enable**.
5. (Optional) Configure the access control list to limit downstream access to the Connect IT 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 ♑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 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 ♋again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the Connect IT 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**.
  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.

Note By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the Connect IT device can use the NTP service.

6. (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 ♋
     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 for more information about NTP client configuration.

7. (Optional) Configure the system time zone. The default is **UTC**.

a. Click **System** > **Time**

b. Select the **Timezone** for the location of your Connect IT device.

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

Command line

1. Log into the Connect IT 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
```

   - 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 for more information about NTP client configuration.

5. (Optional) Configure the access control list to limit downstream access to the Connect IT

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 Connect IT 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
-------------------------------------------
 defaultip          Default IP
 defaultlinklocal     Default Link-local IP
 lan              LAN
 loopback           Loopback
 modem              Modem
 wan              WAN

(config)>
```

  Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service ntp acl zone end value
```

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 list 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 Connect IT device can use the NTP service.

6. (Optional) Set the timezone for the location of your Connect IT 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)>
```

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.

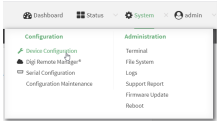
Configure a multicast route

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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, uncheck **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. Type the **Source port**. Ensure the port is not used by another protocol.
8. Select a **Source interface** where multicast packets will arrive.
9. Select a **Destination interface** that the Connect IT device will use to send mutlicast packets.
10. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 port for the route. Ensure the port is not used by another protocol.

```
(config service multicast test)> port port
(config service multicast test)>
```

7. Set the source interface for the route where multicast packets will arrive:
   a. Use the **?** to determine available interfaces:

```
(config service multicast test)> src_interface ?

Source interface: Where the multicast packets will arrive. IP routes do not have an effect in the
incoming stream.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config service multicast test)> src_interface
```

   b. Set the interface. For example:

```
(config service multicast test)> src_interface /network/interface/wan
(config service multicast test)>
```

8. Set the destination interface that the Connect IT device will use to send mutlicast packets.

```
(config service multicast test)> interface interface
(config service multicast test)>
```

   a. Use the **?** to determine available interfaces:

```
(config service multicast test)> interface ?

Destination interface: Which interface to send the multicast packets.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
```

```
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config service multicast test)> interface
```

b. Set the interface. For example:

```
(config service multicast test)> interface /network/interface/wan
(config service multicast test)>
```

9. Save the configuration and apply the change:

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

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

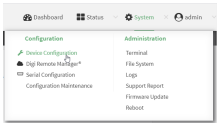
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable 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 Connect IT device to use mDNS.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 Connect IT 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**.
  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. Log into the Connect IT 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 Connect IT 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
-------------------------------------------
 defaultip            Default IP
 defaultlinklocal     Default Link-local IP
 lan                  LAN
 loopback             Loopback
 modem                Modem
 wan                  WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service mdns acl zone end value
```

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 list 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 iPerf service

Your Connect IT 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 Connect IT 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 Connect IT 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 Connect IT device's iPerf3 server.

Required configuration items

- Enable the iPerf server on the Connect IT device.
- An iPerf3 client installed on a remote host. iPerf3 software can be downloaded at https://iperf.fr/iperf-download.php.

Additional configuration Items

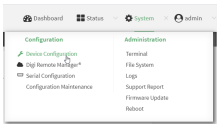
- The port that the Connect IT device's iPerf server will use to listen for incoming connections.
- The access control list for the iPerf server.

  When the iPerf server is enabled, the Connect IT 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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 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 Connect IT 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**.
  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. Log into the Connect IT 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 Connect IT 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
-----------------------------------------
defaultip          Default IP
defaultlinklocal     Default Link-local IP
lan              LAN
loopback           Loopback
modem              Modem
wan              WAN

(config)>
```

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service iperf acl zone end value
```

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 list 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 Connect IT 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.
$
```

User authentication

This chapter contains the following topics:

Connect IT user authentication 318
User authentication methods 318
Authentication groups 325
Local users 334
Terminal Access Controller Access-Control System Plus (TACACS+) 345
Remote Authentication Dial-In User Service (RADIUS) 353
LDAP 360
Disable shell access 367
Set the idle timeout for Connect IT users 368
Example user configuration 370

Connect IT user authentication

User authentication on the Connect IT 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 Connect IT.	■ **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.

User authentication methods

Authentication methods determine how users of the Connect IT 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

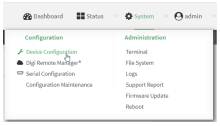
Required configuration items

- The types of authentication method to be used:

To add an authentication method:

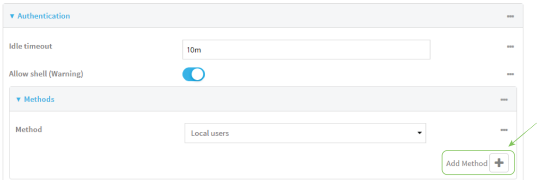
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

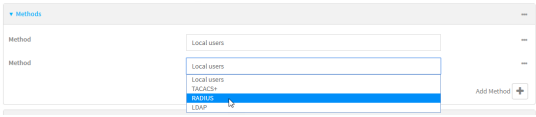


The **Configuration** window is displayed.

3. Click **Authentication** > **Methods**.
4. For **Add Method**, click ♑

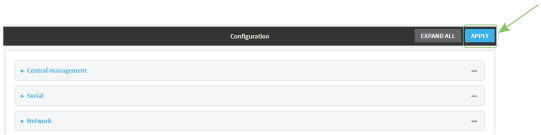


5. Select the appropriate authentication type for the new method from the **Method** drop-down.



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. Log into the Connect IT 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. Log into the Connect IT 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.
>
```

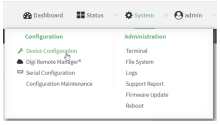
5. Type **exit** to exit the Admin CLI.

   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

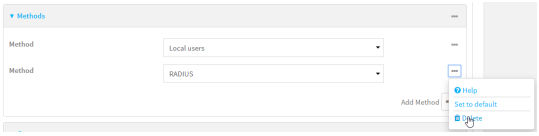
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

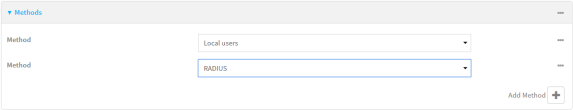
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Rearrange the position of authentication methods

WebUI

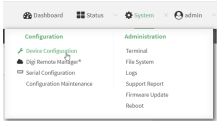
Authentication methods are reordered by changing the method type in the **Method** drop-down for each authentication method to match the appropriate order.

For example, the following configuration has **Local users** as the first method, and **RADIUS** as the second.



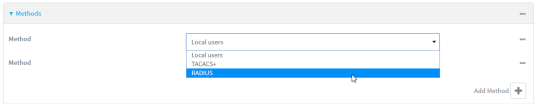
To reorder these so that **RADIUS** is first and **Local users** is second:

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

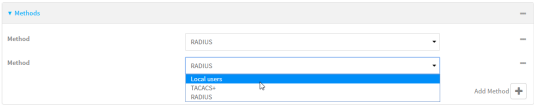


The **Configuration** window is displayed.

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. Log into the Connect IT 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 Connect IT 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 Connect IT 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 Connect IT 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.
- **Serial access**: Users with Serial access have the ability to log into the Connect IT device by using the serial console.

Preconfigured authentication groups

The Connect IT device has two preconfigured authentication groups:

- The **admin** group is configured by default to have full **Admin access** and **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.
- 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:

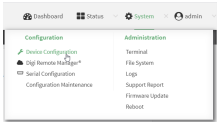
Change the access rights for a predefined group 326
Add an authentication group 328
Delete an authentication group 332

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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

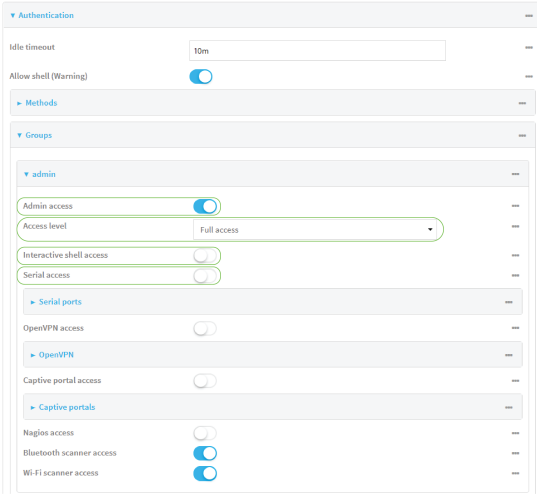


   The **Configuration** window is displayed.
3. Click **Authentication** > **Groups**.
4. Click the authentication group to be changed, either **admin** or **serial**, to expand its configuration node.
5. Click the box next to the following options, as appropriate, to enable or disable access rights for each:
   - **Admin access**

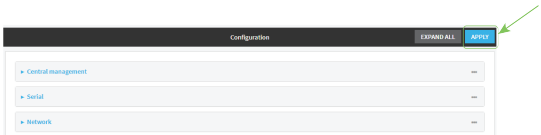
     For groups assigned Admin access, you can also determine whether the **Access level** should be **Full access** or **Read-only access**.
     - **Full access** provides users of this group with the ability to manage the Connect IT device by using the WebUI or the Admin CLI.
     - **Read-only access** provides users of this group with read-only access to the WebUI and Admin CLI.

     The default is **Full access**.
   - **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.
   - **Serial access**



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



Command line

1. Log into the Connect IT 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 Connect IT 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

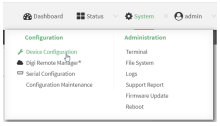
- The serial ports that the user can access.
- Access rights to OpenVPN tunnels, and the tunnels to which they have access.
- Access rights to captive portals, and the portals to which they have access.
- Access rights to query the device for Nagios monitoring.

To add an authentication group:

WebUI

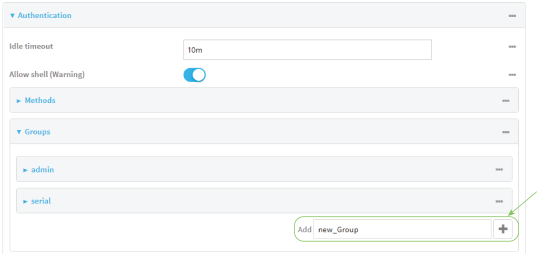
1. Log into the Connect IT WebUI as a user with full Admin access rights.

2. 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 Connect IT 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**.
   - **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.
   - **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. (Optional) Enable users that belong to this group to query the device for Nagios monitoring by checking the box next to **Nagios access**.
10. (Optional) Enable users that belong to this group to access the Bluetooth scanning service by checking the box next to **Bluetooth scanner access**.
11. (Optional) Enable users that belong to this group to access the Wi-Fi scanning service by checking the box next to **Wi-Fi scanner access**.
12. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Connect IT 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 the serial ports to which users of the group have access.

```
(config auth group test)> acl serial add ports end port1
(config auth group test)>
```

6. (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)>
```

7. (Optional) Configure Nagios monitoring:

```
(config)> auth group test acl nagios enable true
(config)>
```

8. (Optional) Enable users that belong to this group to access the Bluetooth scanning service:

```
(config)> auth group test acl bluetooth_scanner enable true
(config)>
```

9. (Optional) Enable users that belong to this group to access the Wi-Fi scanning service:

```
(config)> auth group group test acl wifi_scanner enable 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.

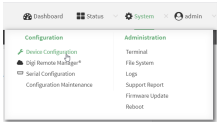
Delete an authentication group

By default, the Connect IT device has two preconfigured authentication groups: **admin** and **serial**. These groups cannot be deleted.

To delete an authentication group that you have created:

WebUI

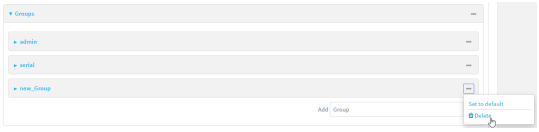
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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. Log into the Connect IT 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 Connect IT 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 Connect IT 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:

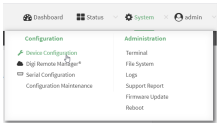
Change a local user's password 335
Configure a local user 336
Delete a local user 342

Change a local user's password

To change a user's password:

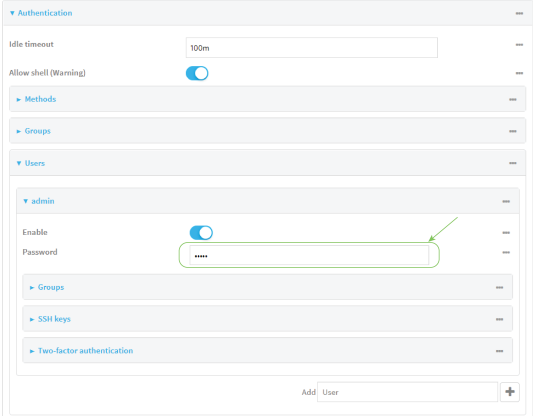
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

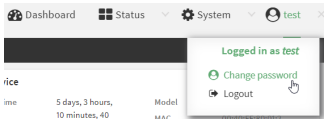


The **Configuration** window is displayed.

3. Click **Authentication** > **Users**.
4. Click the username to expand the user's configuration node.
5. For **Password**, enter the new password.



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. Log into the Connect IT 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.
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. 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**.
- The authentication group or groups from which the user will inherit access rights. See Authentication groups for information about configuring groups.

Additional configuration items

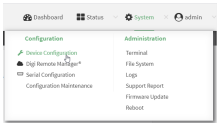
- An optional public ssh key, to authenticate the user when using passwordless SSH login.
- Two-factor authentication information for user login over SSH, telnet, and the serial console:
  - The verification type for two-factor authentication: Either time-based or counter-based.
  - The security key.
  - 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.

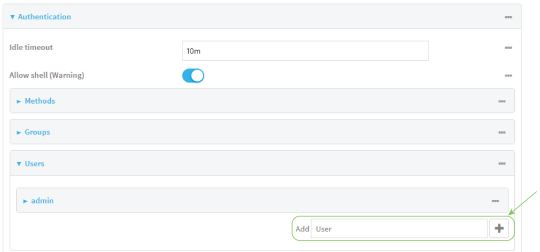
To configure a local user:

WebUI

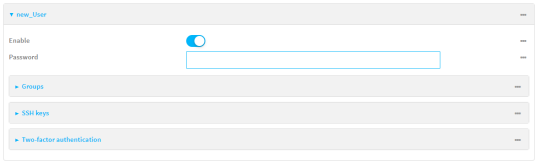
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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.

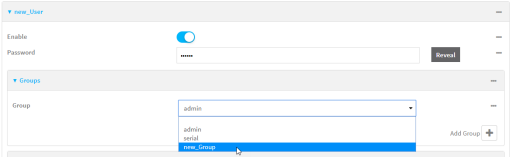


   The user is enabled by default. To disable, click to toggle off **Enable**.
5. Enter a password for the user.
6. Add groups for the user.

   Groups define user access rights. See Authentication groups for information about configuring groups.

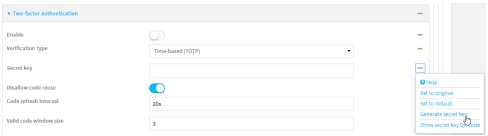
   a. Click **Groups**.
   b. For **Add Group**, click ♑

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.

7. (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 ♑
8. (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. To display the QR code for the secret key, click **...** next to the field label and select **Show secret key QR code**.
      iii. Copy the secret key, or scan or copy the QR code, for use with an application or mobile device to generate passcodes.

      Note To copy the QR code, right-click the QR code and select your browser's save image functionality.

   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.

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

Command line

1. Log into the Connect IT 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. Assign a password to the user:

```
(config auth user new_user> password pwd
(config auth user new_user)>
```

5. 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)>
```

6. (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)>
```

7. (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.

8. Save the configuration and apply the change:

```
(config auth user new 2fa scratch_code)> save
Configuration saved.
>
```

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

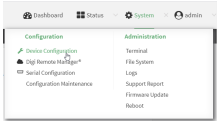
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a local user

To delete a user from your Connect IT:

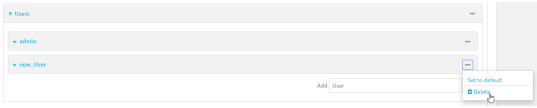
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT 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 Connect IT 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 Connect IT 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 346
TACACS+ server failover and fallback to local authentication 347
Configure your Connect IT device to use a TACACS+ server 347

TACACS+ user configuration

When configured to use TACACS+ support, the Connect IT 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 Connect IT 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 Connect IT"
      pap = cleartext password1
      service = system {
        groupname = admin,serial
      }
}
user = user2 {
      name ="User2 for Connect IT"
      pap = cleartext password2
      service = system {
        groupname = serial
      }
}
```

   The **groupname** attribute is optional. If used, the value must correspond to authentication groups configured on your Connect IT. Alternatively, if the user is also configured as a local user on the Connect IT 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 Connect IT 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 Connect IT 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 Connect IT 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 Connect IT device to use a TACACS+ server

This section describes how to configure a Connect IT 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 Connect IT device.

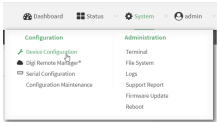
Additional configuration items

- The TACACS+ server port. It is configured to 49 by default.
- Add additional TACACS+ servers in case the first TACACS+ server is unavailable.

WebUI

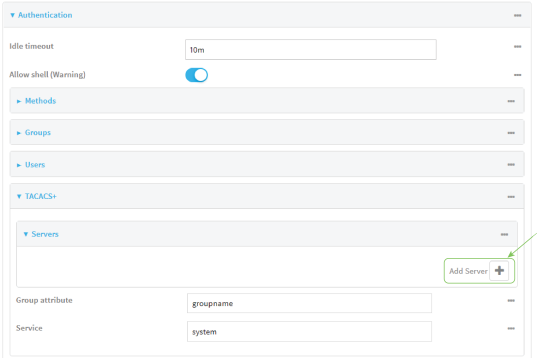
1. Log into the Connect IT WebUI as a user with full Admin access rights.

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

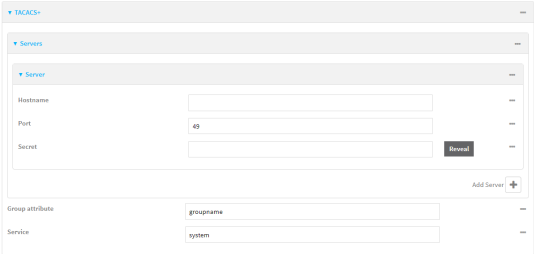


The **Configuration** window is displayed.

3. Click **Authentication** > **TACACS+** > **Servers**.
4. For **Add server**, click ♑



The TACACS+ server configuration window is displayed.

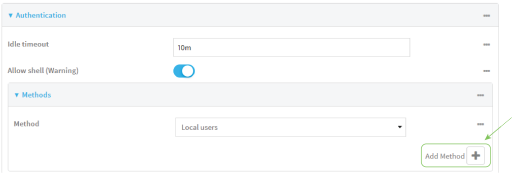


5. For **Hostname**, type the hostname or IP address of the TACACS+ server.
6. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 49.
7. For **Secret**, type the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's tac_plus.conf file, for example:

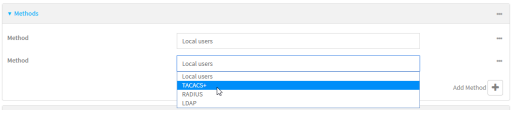
```
key = testing123
```

8. (Optional) For **Group attribute**, type the name of the attribute used in the TACACS+ server's configuration to identify the Connect IT 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 Connect IT configuration.
9. (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 Connect IT configuration.
10. (Optional) Click ♑again to add additional TACACS+ servers.

11. 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 the first successful authentication result is returned. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.

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

Command line

1. Log into the Connect IT 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 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**.

4. 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**.

5. 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)>
```

6. 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)>
```

7. 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)>
```

8. (Optional) Set the name of the user attribute that contains the list of Connect IT 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)>
```

9. Configure the amount of time in seconds to wait for the TACACS+ server to respond.

```
(config)> auth ldap timeout value
(config)>
```

where *value* is any integer from **3** to **60**. The default value is **3**.

10. Add an TACACS+ server:

```
(config)> add auth tacacs+ server end
(config auth tacacs+ server 0)>
```

11. Enter the TACACS+ server's IP address or hostname:

```
(config auth tacacs+ server 0)> hostname hostname|ip-address
(config auth tacacs+ server 0)>
```

12. (Optional) Change the default port setting to the appropriate port:

```
(config auth tacacs+ server 0)> port port
(config auth tacacs+ server 0)>
```

13. Enter the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's tac_plus.conf file. For example:

```
(config auth tacacs+ server 0)> secret testing123
(config auth tacacs+ server 0)>
```

14. Return to the config prompt by typing three periods:

```
(config auth tacacs+ server 0)> ...
(config)>
```

15. (Optional) Configure the group_attribute. This is the name of the attribute used in the TACACS+ server's configuration to identify the Connect IT 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 Connect IT configuration.

```
(config)> auth tacacs+ group_attribute attribute-name
(config)>
```

16. (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 Connect IT configuration.

```
(config)> auth tacacs+ service service-name
(config)>
```

17. (Optional) Repeat the above steps to add additional TACACS+ servers.
18. 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)>
```

19. Save the configuration and apply the change:

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

20. 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 Connect IT 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 Connect IT 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 Connect IT 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 354
RADIUS server failover and fallback to local configuration 354
Configure your Connect IT device to use a RADIUS server 355

RADIUS user configuration

When configured to use RADIUS support, the Connect IT 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 Connect IT 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 Connect IT. Alternatively, if the user is also configured as a local user on the Connect IT 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 Connect IT 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 Connect IT 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 Connect IT 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 Connect IT device to use a RADIUS server

This section describes how to configure a Connect IT device to use a RADIUS server for authentication and authorization.

Required configuration items

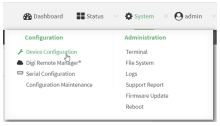
- Define the RADIUS server IP address or domain name.
- Define the RADIUS server shared secret.
- Add RADIUS as an authentication method for your Connect IT device.

Additional configuration items

- 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 Connect IT device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are access the Connect IT 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.

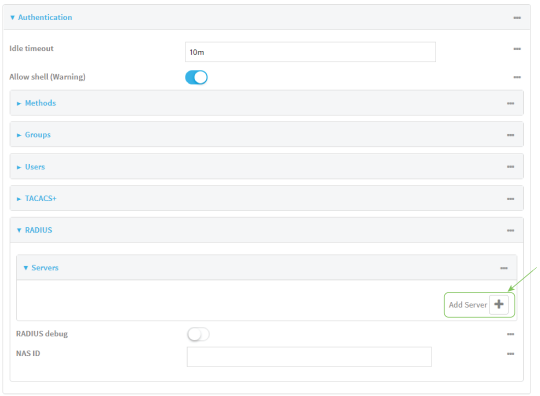
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

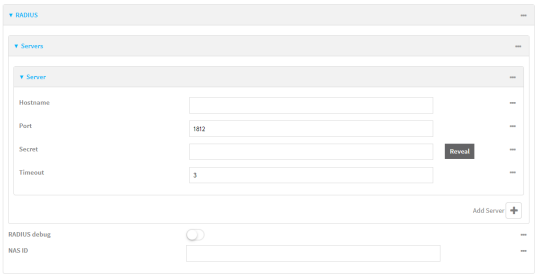


   The **Configuration** window is displayed.
3. Click **Authentication** > **RADIUS** > **Servers**.

4. For **Add server**, click ♑



The RADIUS server configuration window is displayed.

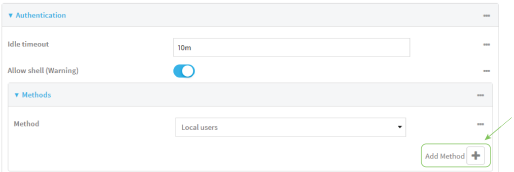


5. For **Hostname**, type the hostname or IP address of the RADIUS server.
6. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 1812.
7. For **Secret**, type the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file, for example:

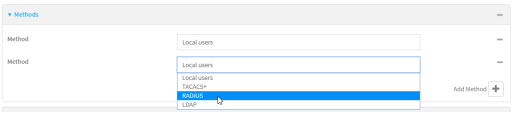
```
secret=testing123
```

8. 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**.
9. (Optional) Click **RADIUS debug** to enable additional debug messages from the RADIUS client.
10. (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 Connect IT device by using the WebUI, the default value is for NAS ID is **httpd**.
    - If you are accessing the Connect IT device by using ssh, the default value is **sshd**.
11. (Optional) Click ♑again to add additional RADIUS servers.

12. 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 the first successful authentication result is returned. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.

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

Command line

1. Log into the Connect IT 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 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**.

4. 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**.

5. 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)>
```

6. 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)>
```

7. 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)>
```

8. (Optional) Set the name of the user attribute that contains the list of Connect IT 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)>
```

9. Configure the amount of time in seconds to wait for the RADIUS server to respond.

```
(config)> auth ldap timeout value
(config)>
```

where *value* is any integer from **3** to **60**. The default value is **3**.

10. Add an RADIUS server:

```
(config)> add auth radius server end
(config auth radius server 0)>
```

11. Enter the RADIUS server's IP address or hostname:

```
(config auth radius server 0)> hostname hostname|ip-address
(config auth radius server 0)>
```

12. (Optional) Change the default port setting to the appropriate port:

```
(config auth radius server 0)> port port
(config auth radius server 0)>
```

13. Enter the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file. For example:

```
(config auth radius server 0)> secret testing123
(config auth radius server 0)>
```

14. 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)>
```

15. Return to the config prompt by typing three periods:

```
(config auth radius server 0)> ...
(config)>
```

16. (Optional) Enable debug messages from the RADIUS client:

```
(config)> auth radius debug true
```

17. (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 Connect IT device by using the WebUI, the default value is for NAS ID is **httpd**.
    - If you are accessing the Connect IT device by using ssh, the default value is **sshd**.

```
(config)> auth radius nas_id id
(config)>
```

18. (Optional) Repeat the above steps to add additional RADIUS servers.
19. 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)>
```

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.

LDAP

Your Connect IT device supports LDAP (Lightweight Directory Access Protocol), a protocol used for directory information services over an IP network. LDAP can be used with your Connect IT device for centralized authentication and authorization management for users who connect to the device. With LDAP support, the Connect IT 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 Connect IT 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 361
LDAP server failover and fallback to local configuration 362
Configure your Connect IT device to use an LDAP server 362

LDAP user configuration

When configured to use LDAP support, the Connect IT 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 Connect IT 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 Connect IT device.
   - The **ou** attribute is optional. If used, the value must correspond to authentication groups configured on your Connect IT. Alternatively, if the user is also configured as a local user on the Connect IT 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 Connect IT 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 Connect IT 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 Connect IT 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 Connect IT device to use an LDAP server

This section describes how to configure a Connect IT 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 Connect IT device.

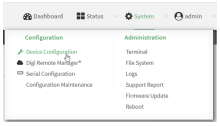
Additional configuration items

- 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.

WebUI

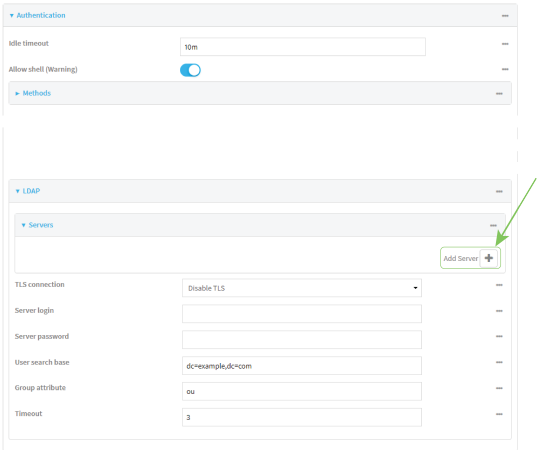
1. Log into the Connect IT WebUI as a user with full Admin access rights.

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

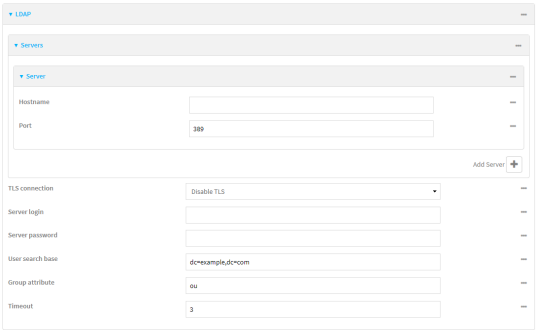


The **Configuration** window is displayed.

3. Click **Authentication** > **LDAP** > **Servers**.
4. For **Add server**, click ♑

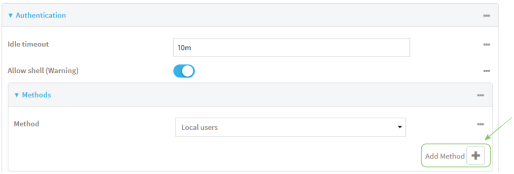


The LDAP server configuration window is displayed.

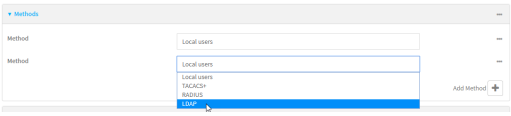


5. For **Hostname**, type the hostname or IP address of the LDAP server.
6. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 389.
7. (Optional) Click ♑again to add additional LDAP servers.
8. For **TLS connection**, select 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.

9. 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.
10. (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.
11. (Optional) For **Server password**, type the password used to log into the LDAP server. Leave this field blank if the server allows anonymous connections.
12. 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**).
13. (Optional) For **Group attribute**, type the name of the user attribute that contains the list of Connect IT authentication groups that the authenticated user has access to. See LDAP user configuration for further information about the group attribute.
14. 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.
15. 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 the first successful authentication result is returned. See Rearrange the position of authentication methods for information about rearranging the position of the methods in the list.

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

Command line

1. Log into the Connect IT 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 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**.

4. 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**.

5. 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)>
```

6. 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)>
```

7. 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)>
```

8. (Optional) Set the name of the user attribute that contains the list of Connect IT 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)>
```

9. 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**.

10. Add an LDAP server:

```
(config)> add auth ldap server end
(config auth ldap server 0)>
```

11. Enter the LDAP server's IP address or hostname:

```
(config auth ldap server 0)> hostname hostname|ip-address
(config auth ldap server 0)>
```

12. (Optional) Change the default port setting to the appropriate port:

```
(config auth ldap server 0)> port port
(config auth ldap server 0)>
```

13. (Optional) Repeat the above steps to add additional LDAP servers.
14. 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)>
```

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.

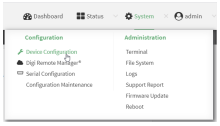
Disable shell access

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.

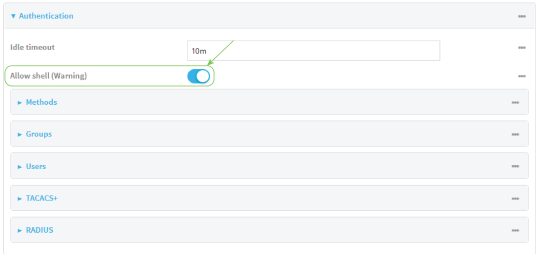
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



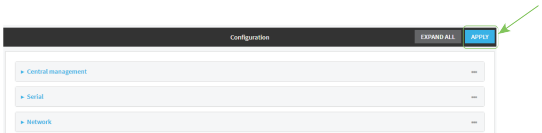
   The **Configuration** window is displayed.

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. Log into the Connect IT 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.

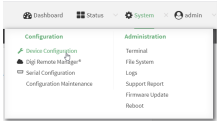
Set the idle timeout for Connect IT users

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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

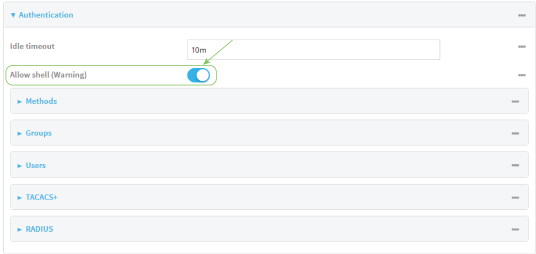


   The **Configuration** window is displayed.

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. Log into the Connect IT 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.

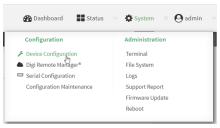
Example user configuration

Example 1: Administrator user with local authentication

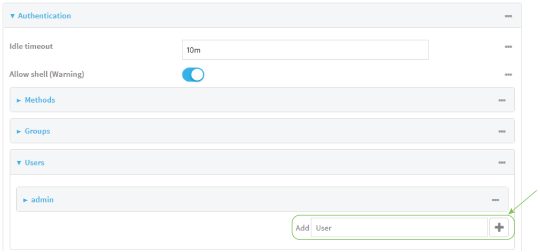
Goal: To create a user with administrator rights who is authenticated locally on the device.

WebUI

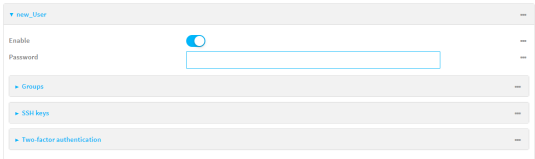
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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. Log into the Connect IT 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 Connect IT 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 Connect IT 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.

WebUI

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 Connect IT 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:

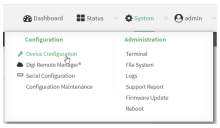
      ```
      $ sudo gedit /etc/tacacs+/tac_plus.conf
      ```

   b. Add a TACACS+ user to the **tac_plus.conf** file:

      ```
      user = admin1 {
          name ="Admin1 for TX64"
          pap = cleartext password1
          service = system {
              groupname = admin
              }
          }
      }
      ```

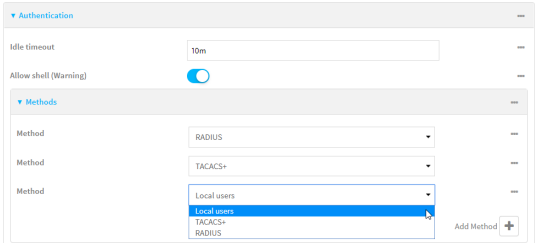
      In this example:
      - The user's username is **admin1**.
      - The user's password is **password1**.
      - The authentication group on the Connect IT device, **admin**, is identified in the **groupname** parameter.

   c. Save and close the **tac_plus.conf** file.
3. Log into the Connect IT WebUI as a user with full Admin access rights.
4. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

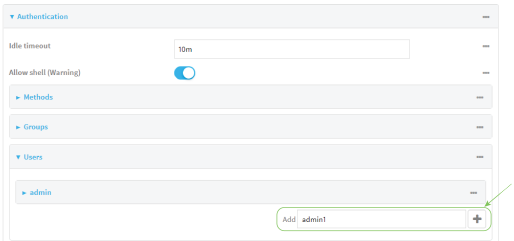


The **Configuration** window is displayed.

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**.

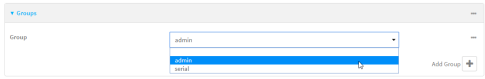


6. Create the local user:
   a. Click **Authentication** > **Users**.
   b. In **Add User:**, type **admin1** and click



   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.



   c. 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 Connect IT 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 Connect IT device, **admin**, is identified in the **groupname** parameter.

c. Save and close the **tac_plus.conf** file.

3. Log into the Connect IT 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.

Example 3: Multiple users with specific serial port access

Goal: To create two RADIUS users that do not have configuration access to the Connect IT but have access rights to specific serial ports.

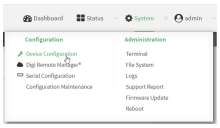
In this example, we will create two users:

- **serialuser1** with access to serial port 1.
- **serialuser2** with access to serial ports 2, 4, and 8.

This example uses a FreeRadius 3.0 server running on ubuntu. Server configuration may vary depending on the platforms or type of servers used in your environment.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Configure the device to use RADIUS authentication:
   a. Click **Authentication** > **Methods**.
   b. For **Add Method**, click to add a new method.
   c. For the new method, select **RADIUS**.

   Note If you want other users to authenticate via other authentication methods, you should include those authentication methods in this list. For example, if you want administrators of the Connect IT to log into the device using local authentication, make sure that **Local users** authentication is included in the **Methods** list. Otherwise they will not be able to log into the device.

4. Create the authentication groups.

   In this example, we are adding two groups, **serialgroup1** and **serialgroup2**.
   a. In **Add Group**, type **serialgroup1** and click
   b. Repeat for the second group: For **Add Group:**, type **serialgroup2** and click
   c. For **serialgroup1**:
      i. Click **Serial access** to enable serial access.
      ii. Click **Serial ports**.
      iii. For **Add Port**, click
      iv. For **Port**, select **Port 1**.
   d. For **serialgroup2**:
      i. Click **Serial access** to enable serial access.
      ii. Click **Serial ports**.
      iii. For **Add Port**, click
      iv. For **Port**, select **Port 2**.
      v. Click again.
      vi. Select **Port 4**.
      vii. Click again.
      viii. Select **Port 8**.
5. Create the users.

   In this example, we are adding two users, **serialuser1** and **serialuser2**, and adding them to the groups that we created in the previous step .
   a. Click **Authentication** > **Users**.
   b. In **Add User**, type **serialuser1** and click
   c. Repeat for the second user: For **Add User**, type **serialuser2** and click
   d. For **serialuser1**:
      i. For **password**, enter **password1**.
      ii. Click **Groups**.
      iii. For **Add Group**, click
      iv. For **Group**, select **serialgroup1**.

e. For **serialuser2**:
   i. For **password**, enter **password2**.
   ii. Click **Groups**.
   iii. For **Add Group**, click ♋
   iv. For **Group**, select **serialgroup2**.

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

7. Configure the users 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 the users to the **users** file:

```
serialuser1 Cleartext-Password := "password1"
      Unix-FTP-Group-Names := "serialgroup1"
serialuser2 Cleartext-Password := "password2"
      Unix-FTP-Group-Names := "serialgroup2"
```

   c. Save and close the **users** file.

Command line

1. Log into the Connect IT 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 the device to use RADIUS authentication:

```
(config)> add auth method end radius
```

Note If you want other users to authenticate via other authentication methods, you should include those authentication methods in this list. For example, if you want administrators of the Connect IT to log into the device using local authentication, make sure that **local** authentication is included in the **auth method** list. Otherwise they will not be able to log into the device. To view the current **auth method** list:

```
(config)> show auth method
0 local
```

```
1 radius
(config)>
```

4. Create the first authentication group:

```
(config)> add auth group serialgroup1
(config auth group serialgroup1)>
```

5. Enable serial access for **serialgroup1**:

```
(config auth group serialgroup1)> acl serial enable true
(config auth group serialgroup1)>
```

6. Limit the user's access to serial port 1:

```
(config auth group serialgroup1)> add acl serial ports end port1
(config auth group serialgroup1)>
```

7. Move down one step in the configuration by typing two periods (**..**):

```
(config auth group serialgroup1)> ..
(config auth group)>
```

8. Create the second authentication group:

```
(config auth group)> add serialgroup2
(config auth group serialgroup2)>
```

9. Enable serial access for **serialgroup2**:

```
(config auth group serialgroup2)> acl serial enable true
(config auth group serialgroup2)>
```

10. Limit the user's access to serial ports 2, 4, and 8:

```
(config auth group serialgroup2)> add acl serial ports end port2
(config auth group serialgroup2)> add acl serial ports end port4
(config auth group serialgroup2)> add acl serial ports end port8
```

11. Save the configuration and apply the change:

```
(config auth user serialuser2)> 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.

13. Configure the users 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 the users to the **users** file:

```
serialuser1 Cleartext-Password := "password1"
    Unix-FTP-Group-Names := "serialgroup1"
serialuser2 Cleartext-Password := "password2"
    Unix-FTP-Group-Names := "serialgroup2"
```

c. Save and close the **users** file.

Firewall

This chapter contains the following topics:

Firewall configuration 383
Port forwarding rules 387
Packet filtering 394
Configure custom firewall rules 401
Configure Quality of Service options 403

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 Connect IT 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 Connect IT.
- **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.

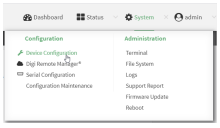
Create a custom firewall zone

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:

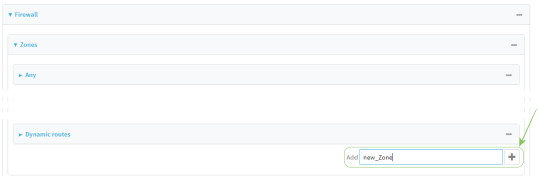
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

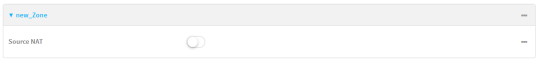


   The **Configuration** window is displayed.
3. Click **Firewall** > **Zones**.

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. Log into the Connect IT 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.

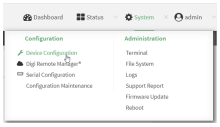
Configure the firewall zone for a network interface

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.

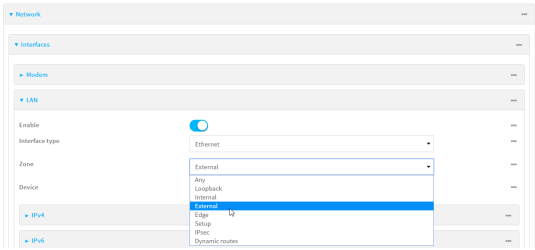
This example procedure uses an existing network interface named and changes the firewall zone from the default zone, **Internal**, to **External**.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **Interfaces** > **LAN**.
4. For **Zone**, select **External**.



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

Command line

1. Log into the Connect IT 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 lan zone my_zone
(config)>
```

4. Save the configuration and apply the change:

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

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

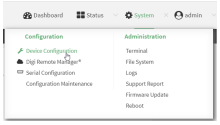
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a custom firewall zone

You cannot delete preconfigured firewall zones. To delete a custom firewall zone:

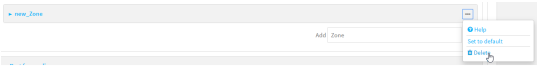
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 on the server to which traffic should be forwarded.

Additional configuration items

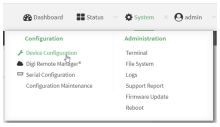
- A label for the port forwarding rule.
- The IP version (either IPv4 or IPv6) that incoming network connections must match.
- The protocols that incoming network connections must match.

- 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:

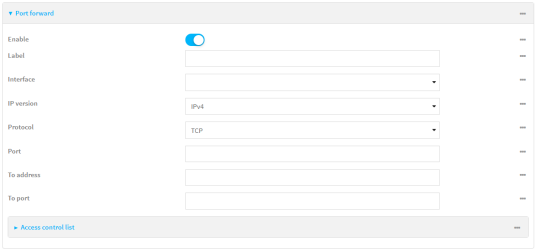
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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, click to 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 **Port**, 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 **To port**, type the port number of the port on the server to which traffic should be forwarded.

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. Log into the Connect IT 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:

```
(config firewall dnat 0)> interface ?
```

```
Interface: Network connections will only be forwarded if their destination address matches the
IP address of this network interface.
Format:
  defaultip
  defaultlinklocal
  eth1
  eth2
  loopback
Current value:

(config firewall dnat 0)> interface
```

b. Set the interface. For example:

```
(config firewall dnat 0)> interface wan
(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 that network connections must use for their traffic to be forwarded.

```
(config firewall dnat 0)> to_port port
(config firewall dnat 0)>
```

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.

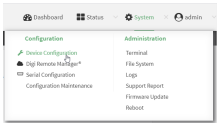
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a port forwarding rule

To delete a port forwarding rule:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 lan1
    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 lan1
    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

By default, one preconfigured packet filtering rule, **Allow all outgoing traffic**, is enabled and monitors traffic going to and from the Connect IT device. The predefined settings are intended to block unauthorized inbound traffic while providing an unrestricted flow of outgoing data. You can modify the default packet filtering rule and create additional rules to define how the device accepts or rejects traffic that is forwarded through the device.

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.

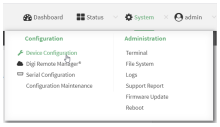
Additional configuration requirements

- 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:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

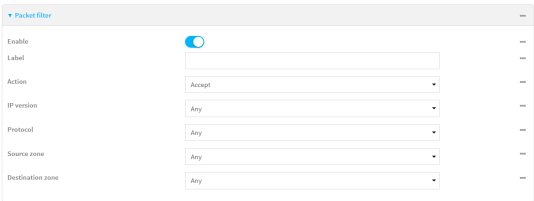


The **Configuration** window is displayed.

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, click to 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. Log into the Connect IT 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.

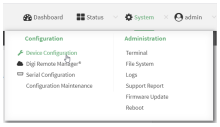
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable or disable a packet filtering rule

To enable or disable a packet filtering rule:

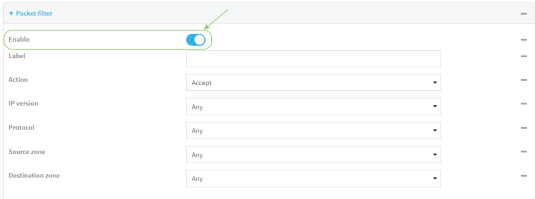
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

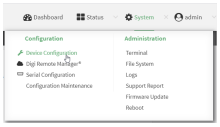
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a packet filtering rule

To delete a packet filtering rule:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

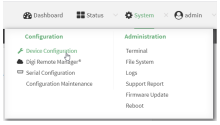
Configure custom firewall rules

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:

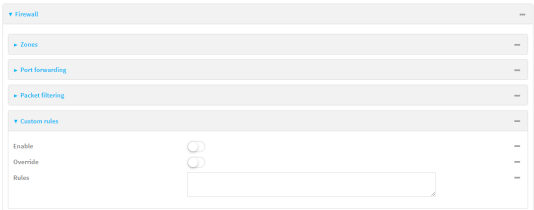
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT device on the binding's interface. By default, the Connect IT device has two preconfigured QoS bindings, **Outbound** and **Inbound**. These bindings are an example configuration designed for a typical VoIP site:

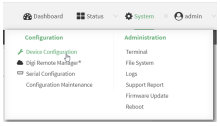
- **Outbound** provides an example of matching packets as they are routed from the device onto the WAN interface.
- **Inbound** provides an example of matching packets as they are routed from the device onto a LAN interface.

These example bindings are disabled by default.

Enable the preconfigured bindings

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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:

```
(config)> firewall qos 0 interface ?

Interface: The network interface.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config)> firewall qos 0 interface
```

b. Set the interface. For example:

```
(config)> firewall qos 0 interface /network/interface/wan
(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.
>
```

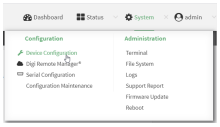
7. Type **exit** to exit the Admin CLI.

   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

WebUI

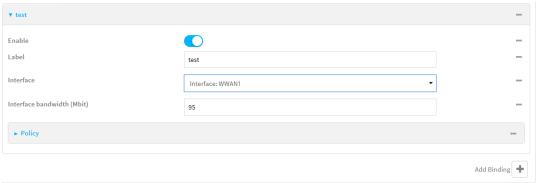
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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.

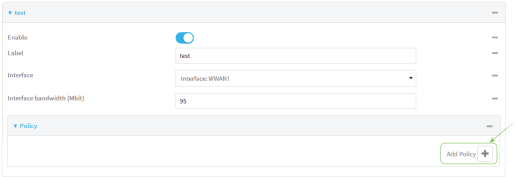


5. **Enable** the binding.
6. (Optional) Type a **Label** for the binding.
7. Select an **Interface** to queue egress packets on. The binding will only match traffic that is being sent out on this interface.
8. (Optional) For **Interface bandwidth (Mbit)**, set the maximum egress bandwidth of the interface, 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:

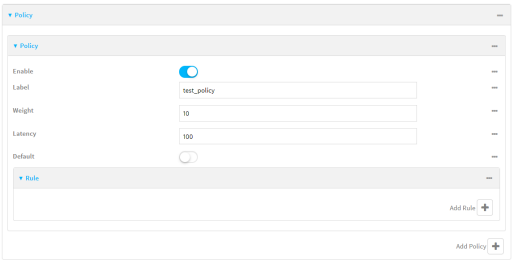
   At least one policy is required for each binding. Each policy can contain up to 30 rules.

   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, click **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.

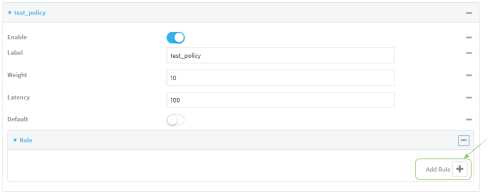
   e. For **Latency**, type the maximum delay before the transmission of packets. A lower latency means that the packets will be scheduled more quickly for transmission.

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.

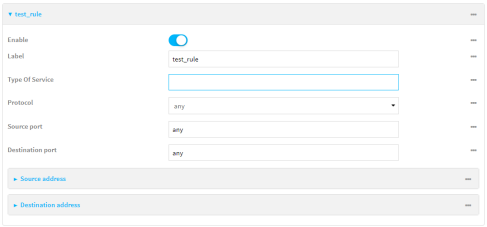
g. If **Default** is disabled, you must configure at least one rule:

   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, click **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. Log into the Connect IT 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:

```
(config firewall qos 2)> interface ?

Interface: The network interface.
Format:
  /network/interface/defaultip
  /network/interface/defaultlinklocal
  /network/interface/eth1
  /network/interface/eth2
  /network/interface/loopback
Current value:

(config firewall qos 2)> interface
```

   b. Set the interface. For example:

```
(config firewall qos 2)> interface /network/interface/wan
(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:

  ```
  (config network qos 2 policy 0 rule 0)> src interface ?

  Interface: Match the IP address with the specified interface's network
  address.
  Format:
    /network/interface/defaultip
    /network/interface/defaultlinklocal
    /network/interface/eth1
    /network/interface/eth2
    /network/interface/loopback
  Current value:

  (config network qos 2 policy 0 rule 0)> src interface
  ```

  ii. Set the interface. For example:

  ```
  (config network qos 2 policy 0 rule 0)> src interface /network/interface/wan
  (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:

  ```
  (config network qos 2 policy 0 rule 0)> dst interface ?

  Interface: Match the IP address with the specified interface's network
  address.
  Format:
    /network/interface/defaultip
    /network/interface/defaultlinklocal
    /network/interface/eth1
    /network/interface/eth2
    /network/interface/loopback
  Current value:

  (config network qos 2 policy 0 rule 0)> dst interface
  ```

  ii. Set the interface. For example:

  ```
  (config network qos 2 policy 0 rule 0)> dst interface /network/interface/wan
  (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.

System administration

This chapter contains the following topics:

Review device status 416
Configure system information 417
Update system firmware 419
Update cellular module firmware 422
Reboot your Connect IT device 423
Reset the device to factory defaults 425
Configuration files 429
Schedule system maintenance tasks 434

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:

WebUI

To display system information:

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **Status**.

   A secondary menu appears, along with a status panel.
3. 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. Log into the Connect IT command line as a user with Admin access.

     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 Connect IT
  Serial Number      : Connect IT-000065
  SKU                : Connect IT
  Hostname           : Connect IT
  MAC                : DF:DD:E2:AE:21:18

  Hardware Version   : 50001947-01 1P
  Firmware Version   : 20.5.38.39
  Alt. Firmware Version : 20.5.38.39
  Bootloader Version : 19.7.23.0-15f936e0ed

  Current Time       : Fri, 29 May 2020 21:14:12 +0000
  CPU                : 1.4%
  Uptime             : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature        : 40C

>
```

- Show more detailed system information:

1. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT
  Serial Number         : Connect IT-000065
  SKU                   : Connect IT
  Hostname              : Connect IT
  MAC                   : DF:DD:E2:AE:21:18

  Hardware Version      : 50001947-01 1P
  Firmware Version      : 20.5.38.39
  Alt. Firmware Version : 20.5.38.39
  Bootloader Version    : 19.7.23.0-15f936e0ed

  Schema Version        : 715
  Timezone              : UTC
  Current Time          : Fri, 29 May 2020 21:14:12 +0000
  CPU                   : 1.4%
  Uptime                : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature           : 40C

  Disk
  ----
  Load Average          : 0.09, 0.10, 0.08
  RAM Usage             : 127.843MB/1880.421MB(6%)
  Disk /etc/config Usage : 18.421MB/4546.371MB(0%)
  Disk /opt Usage       : -4523.-46MB/549.304MB(-822%)
  Disk /overlay Usage   : MB/MB(%)
  Disk /tmp Usage       : 0.007MB/256.0MB(0%)
  Disk /var Usage       : 1.765MB/256.0MB(1%)

>
```

Configure system information

You can configure information related to your Connect IT device, such as providing a name and location for the device.

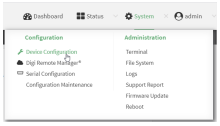
Configuration items

- 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.

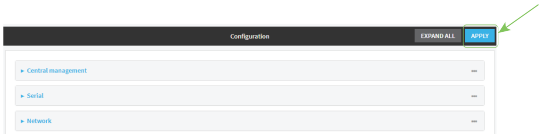
To enter system information:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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 Connect IT."
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 Connect IT operating system firmware images consist of a single file with the following naming convention:

***platform-version*.bin**

For example, **Connect IT-20.5.38.39.bin**.

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*.

Certificate management for firmware images

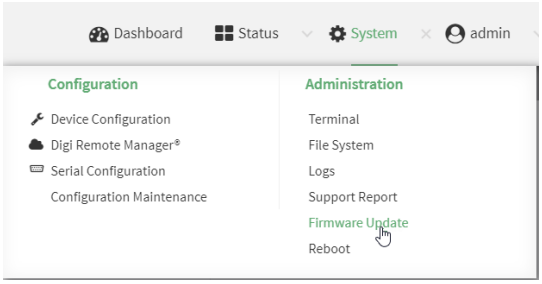
The system firmware files are signed to ensure that only Digi-approved firmware load onto the device. The Connect IT device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

WebUI

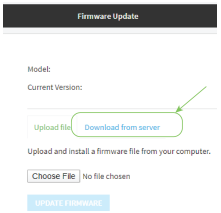
Install firmware from the Digi firmware server

1. Log into the Connect IT WebUI as a user with Admin access.

2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



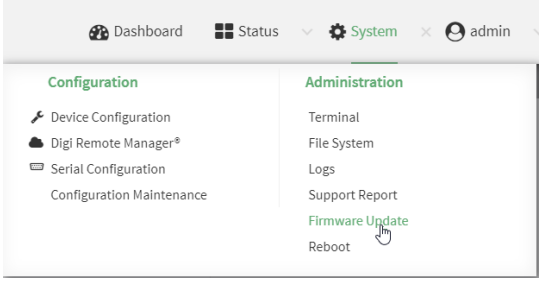
3. Click **Download from server**.



4. For **Version:**, select the appropriate version of the device firmware.
5. Click **Update Firmware**.

Update firmware from a local file

1. Download the Connect IT operating system firmware from the Digi Support FTP site to your local machine.
2. Log into the Connect IT WebUI as a user with Admin access.
3. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



4. Click **Choose file**.
5. Browse to the location of the firmware on your local file system and select the file.
6. Click **Update Firmware**.

Command line

1. Download the Connect IT operating system firmware from the Digi Support FTP site to your local machine.

2. Log into the Connect IT command line as a user with Admin access.

   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:

```
> 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 Connect IT device.
   - *local-path* is the location on the Connect IT device where the copied file will be placed.

   For example:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect IT-20.5.38.39.bin local
/etc/config/ to local
admin@192.168.4.1's password: adminpwd
Connect IT->20.5.38.39.bin                100%    36MB    11.1MB/s       00:03
>
```

4. Verify that the firmware file has been successfully uploaded to the device:

```
> ls /etc/config/
-rw-r--r--    1 root     root     37511229 May 16 20:10 Connect IT-20.5.38.39.bin
-rw-r--r--    1 root     root         2580 May 16 16:44 accns.json
drw-------    2 root     root         4096 Apr 29 18:51 analyzer
-rw-r--r--    1 root     root           47 Apr 30 06:59 dhcp.leases
drwxr-xr-x    2 root     root         4096 May 15 17:53 fcron
...
>
```

5. Update the firmware by entering the update firmware command, specifying the firmware file name:

```
> update firmware file Connect IT-20.5.38.39.bin
36632K
netflash: got "/etc/config/Connect IT-20.5.38.39.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 Connect IT's command line as a user with Admin access and verify the running firmware version by entering the show system command.

```
> show system

Hostname          : Connect IT
FW Version        : 20.5.38.39
MAC               : 0040FF800120
Model             : Digi Connect IT
Current Time      : Fri, 29 May 2020 21:14:12 +0000
Uptime            : 42 seconds (42s)

>
```

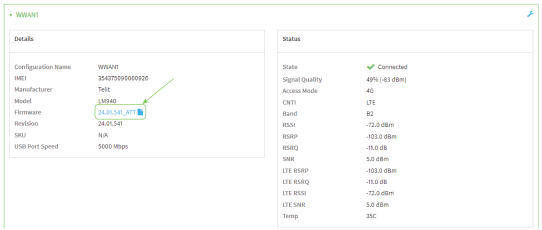
Update cellular module firmware

You can update modem firmware by downloading firmware from the Digi firmware repository, or by uploading firmware from your local storage onto the device.

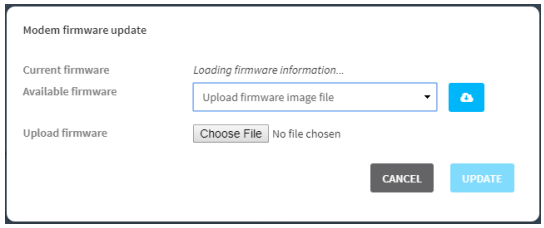
WebUI

This operation is available from the WebUI only. There is no equivalent functionality at the CLI.

1. (Optional) Download the appropriate modem firmware from the Digi repository to your local machine.
2. Log into the Connect IT WebUI as a user with Admin access.
3. From the main menu, click **Status** > **Modems**.
4. Click the modem firmware version.



The **Modem firmware update** window opens.



5. To update using firmware from the Digi firmware repository:
   a. Click to view availabled versions.
   b. For Available firmware, select the firmware.

6. To update using firmware from your local filesystem:
   a. Click **Choose File**.
   b. Select the firmware.
7. Click **Update**.

Reboot your Connect IT device

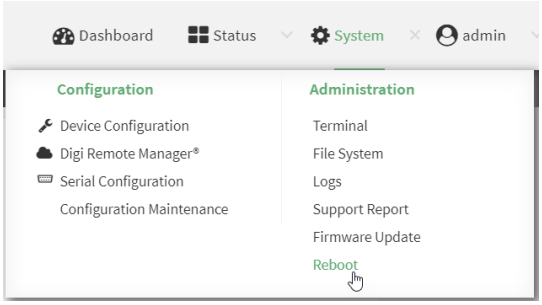
You can reboot the Connect IT device immediately or schedule a reboot for a specific time every day.

Note You may want to save your configuration settings to a file before rebooting. See Save configuration to a file.

Reboot your device immediately

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. From the main menu, click **System**.
3. Click **Reboot**.



4. Click **Reboot** to confirm that you want to reboot the device.

Command line

1. Log into the Connect IT command line as a user with Admin access.

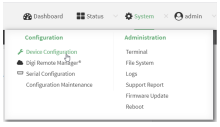
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

```
> reboot
```

Schedule reboots of your device

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 a value is set for **Reboot time** 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 for information about configuring NTP servers.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 a value is set for **reboot_time** 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 for information about configuring NTP servers.

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.

Reset the device to factory defaults

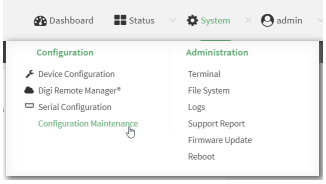
Resetting the device to factory defaults performs the following actions:

- Clears all configuration settings. When the device restarts, it uses the default configuration.
- Deletes all user files.
- Erases all automatically generated keys.
- Clears event and system log files.

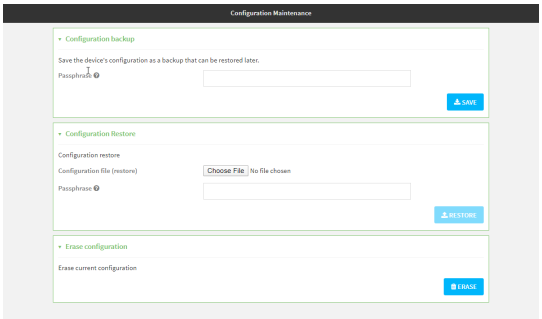
You can reset the device in the WebUI, at the command line, or by using the **Reset** button on the device. You can also reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command.

WebUI

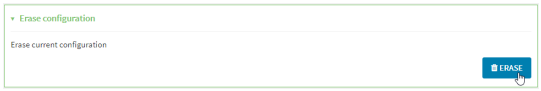
1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



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 Connect IT by using the serial port or by using an Ethernet cable to connect the Connect IT **LAN** port to your PC.
   b. Log into the Connect IT:

      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).

      Note If your device was manufactured prior to the release of firmware version 19.11.x, the default user name may be **root**.

   c. Reset the default password for the admin account. See Reset default password for the default admin user for further information.

Command line

1. Log into the Connect IT command line as a user with Admin access.

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
```

3. After resetting the device:
   a. Connect to the Connect IT by using the serial port or by using an Ethernet cable to connect the Connect IT **LAN** port to your PC.
   b. Log into the Connect IT:

      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).

      Note If your device was manufactured prior to the release of firmware version 19.11.x, the default user name may be **root**.

   c. Reset the default password for the admin account. See Reset default password for the default admin user for further information.

Reset the device by using the ERASE button.

1. Locate the **ERASE** button on your device.
2. Press and hold the **ERASE** button perform a device reset. The **ERASE** button has two 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.
3. After resetting the device:
   a. Connect to the Connect IT by using the serial port or by using an Ethernet cable to connect the Connect IT **LAN** port to your PC.
   b. Log into the Connect IT:

      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).

      Note If your device was manufactured prior to the release of firmware version 19.11.x, the default user name may be **root**.

   c. Reset the default password for the admin account. See Reset default password for the default 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. Log into the Connect IT 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.

Configuration files

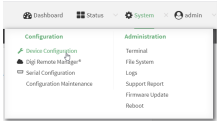
The Connect IT configuration file, /etc/config/accns.json, contains all configuration changes that have been made to the device. It does not contain the complete device configuration; it only contains changes to the default configuration. Both the default configuration and the changes contained in the accns.json file are applied when the device reboots.

Save configuration changes

When you make changes to the Connect IT 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.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

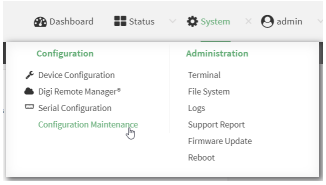
Save configuration to a file

You can save your Connect IT device's configuration to a file and use this file to restore the configuration, either to the same device or to similar devices.

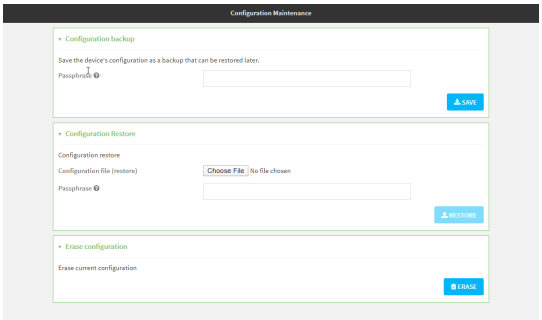
WebUI

This procedure creates a binary archive file containing the device's configuration, certificates and keys, and other information.

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



   The **Configuration Maintenance** windows is displayed.



3. 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. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT'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/ 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 Connect IT device.

For example:

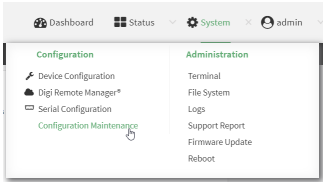
```
> scp host 192.168.4.1 user admin remote /home/admin/bin/ local /etc/config/backup-archive-0040FF800120-19.05.17-19.01.17.bin to remote
```

Restore the device configuration

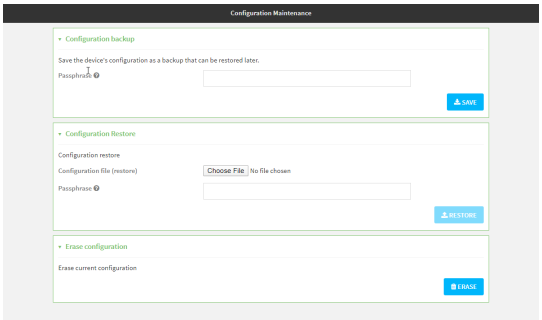
You can restore a configuration file to your Connect IT device by using a backup from the device, or a backup from a similar device.

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



3. 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**.
4. Click **CONFIRM**.

   The configuration will be restored and the device will be rebooted.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT device.
   - *local-path* is the location on the Connect IT device where the copied file will be placed.

   For example:

   > scp host 192.168.4.1 user admin remote /home/admin/bin/backup-archive-0040FF800120-19.05.17-19.01.17.bin local /etc/config/ to local

3. Enter the following:

   > system restore *path* [passphrase *passphrase*]

   where

- *path* is the location of configuration backup file on the Connect IT'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 /etc/config/
```

Schedule system maintenance tasks

You can configure tasks and custom scripts to be run during a specified maintenance window.

Required configuration items

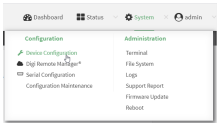
- The time that the system maintenance tasks will start.
- The duration window during which the system maintenance tasks can run.
- The frequency (either daily or weekly) that the tasks will run.
- The tasks to be performed. Options are:
  - Modem firmware update.
  - Configuration check.

Additional configuration items

- Custom scripts that should be run as part of the configuration check.

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



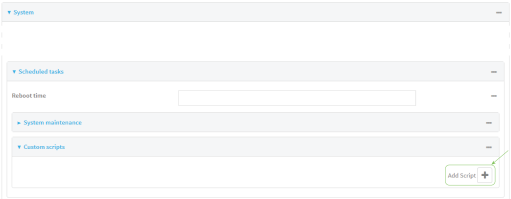
   The **Configuration** window is displayed.
3. Click **System** > **Scheduled tasks** > **System maintenance**.
4. For **Start time**, type the time of day that the maintenance window should start, using the syntax *HH*:*MM*. If **Start time** is not set, maintenance tasks are not scheduled and will not 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.

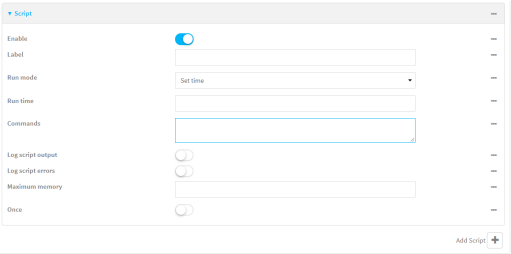
5. For **Duration window**, select the amount of time that the maintenance tasks will be run. If **Immediately** is selected, all scheduled tasks will begin at the exact time specified in **Start time**.
6. For **Frequency**, select either **Daily** or **Weekly** for the frequency that the maintenance tasks should be run.
7. (Optional) 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.
8. (Optional) Click to enable **Configuration check** to allow for the configuration to be updated, including by custom scripts, during the maintenance window.
9. (Optional) To schedule custom scripts:
   a. Click **Custom scripts**.

   Note This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care. Scripts created here are also automatically entered in **Configuration** > **Applications**.

   b. For **Add Script**, click ♑



   The schedule script configuration window is displayed.



   Scheduled scripts are enabled by default. To disable, click **Enable** to toggle off.

   c. (Optional) For **Label**, provide a label for the script.
   d. 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 selected, 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.

e. For **Commands**, enter the commands that will execute the script.

   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**).

f. Script logging options:

   i. Click to enable **Log script output** to log the script's output to the system log.

   ii. 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.

g. 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**}.

h. 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**.

i. **Sandbox** is enabled by default. This option protects the script from accidentally destroying the system it is running on.

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

Command line

1. Log into the Connect IT 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. Schedule system maintenance:
   a. 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 from HH:MM
   (config)>
   ```

   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.

   b. 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.

   ```
   system schedule maintenance length num
   (config)>
   ```

   where *num* is any whole number between **0** and **24**.

   c. Configure the frequency that the maintenance tasks should be run:

   ```
   system schedule maintenance frequency value
   (config)>
   ```

   where *value* is either **daily** or **weekly**. **Daily** is the default.

   d. 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.

   ```
   system schedule maintenance modem_fw_update value
   (config)>
   ```

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

e. Allow for the configuration to be updated, including by custom scripts, during the maintenance window:

```
system schedule maintenance config_check value
(config)>
```

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

4. (Optional) Schedule custom scripts:

a. 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)>
```

b. (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.

c. 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.

d. 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 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**).

e. 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.

f. 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**}.

g. 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**.

h. **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)>
```

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.

Monitoring

This chapter contains the following topics:

intelliFlow 442
Configure NetFlow Probe 449

intelliFlow

intelliFlow monitors system information, network data usage, and traffic information, and displays the information in a series of charts available in the local WebUI. To use intelliFlow, the Connect IT must be powered on and 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.

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.

Note When intelliFlow is enabled, it adds an estimated 50MB of data usage for the device by reporting the metrics to Digi Remote Manager.

Enable intelliFlow

Required configuration items

- Enable intelliFlow.

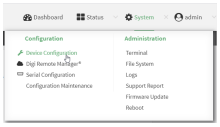
Additional configuration items

- The firewall zone for internal clients being monitored by intelliFlow.

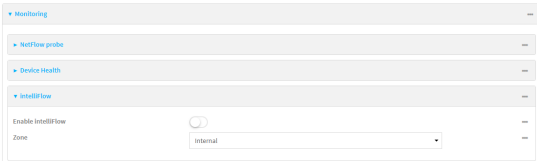
To enable intelliFlow:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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.

Use intelliFlow to display average CPU and RAM usage

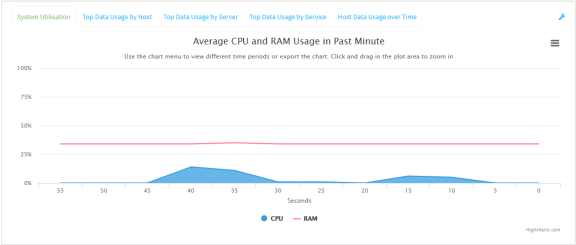
This procedure is only available from the WebUI.

To display display average CPU and RAM usage:

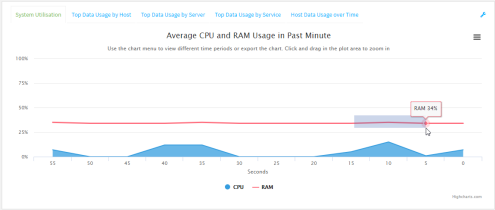
WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.

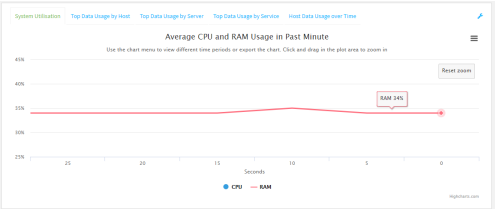
The System Utilisation chart is displayed:



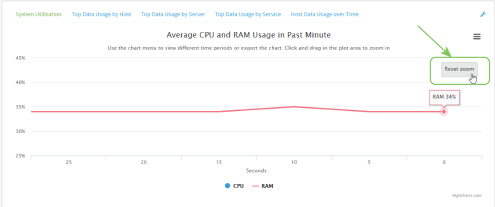
- Display more granular information:
  1. Click and drag over an area in the chart to zoom into that area and provide more granular information.



  2. Release to display the selected portion of the chart:



3. Click **Reset zoom** to return to the original display:

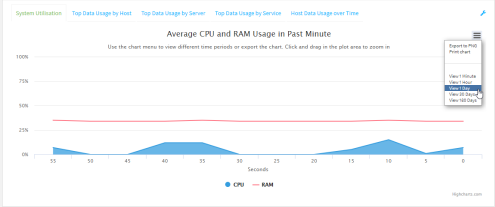


- Change the time period displayed by the chart.

  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

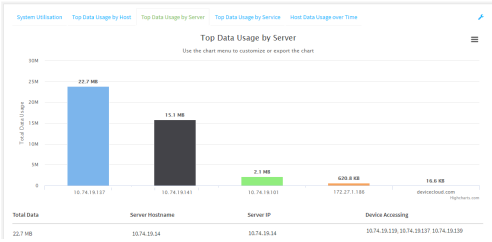
To generate a top data usage chart:

WebUI

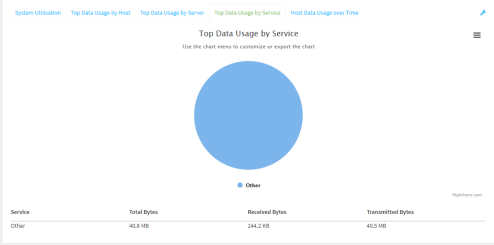
1. Log into the Connect IT WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.

4. Display a data usage chart:
   - To display the **Top Data Usage by Host** chart, click **Top Data Usage by Host**.

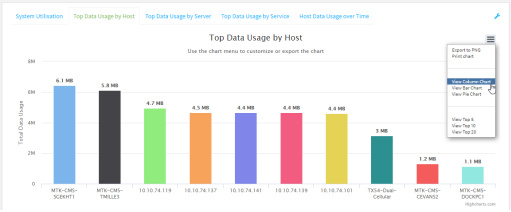
   - To display the **Top Data Usage by Server** chart, click **Top Data Usage by Server**.



   - To display the **Top Data Usage by Service** chart, click **Top Data Usage by Service**.

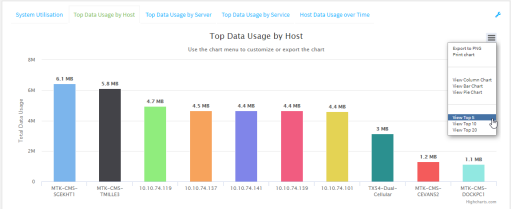


5. Change the type of chart that is used to display the data:
   a. Click the menu icon ( ).
   b. Select the type of chart.



6. 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.



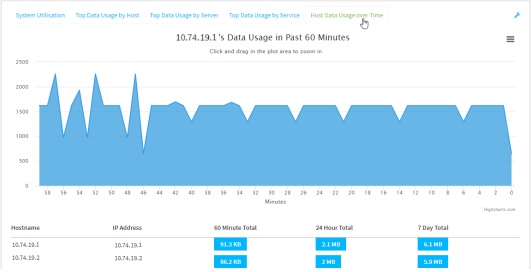
7. Save or print the chart.
   a. Click the menu icon ( ).
   b. To save the chart to your local filesystem, select **Export to PNG**.
   c. To print the chart, select **Print chart**.

Use intelliFlow to display data usage by host over time

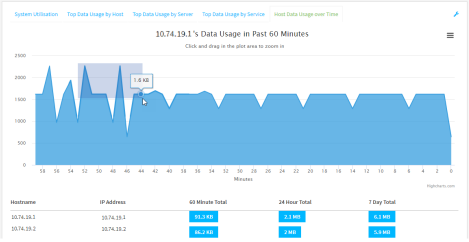
To generate a chart displaying a host's data usage over time:

WebUI

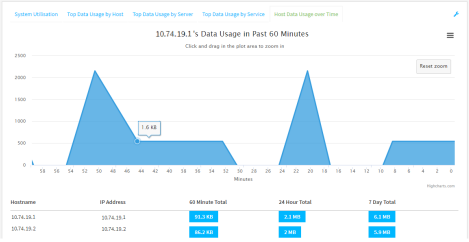
1. Log into the Connect IT WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.
4. Click **Host Data Usage Over Time**.



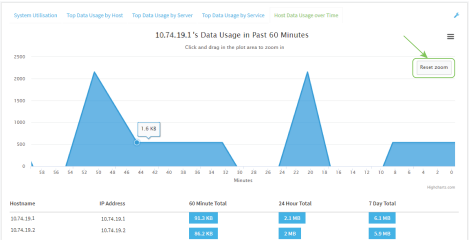
- Display more granular information:
  a. Click and drag over an area in the chart to zoom into that area and provide more granular information.



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 Connect IT device and export statistics to NetFlow collectors.

Required configuration items

- Enable NetFlow.
- The IP address of a NetFlow collector.

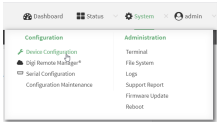
Additional configuration items

- 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.

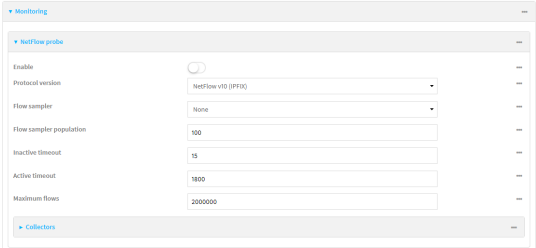
To probe network traffic and export statistics to NetFlow collectors:

WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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. Log into the Connect IT 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**.
4. 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.

Central management with Digi Remote Manager

This chapter contains the following topics:

Digi Remote Manager support 455
Configure Digi Remote Manager 455
Collect device health data and set the sample interval 460
Log into Digi Remote Manager 462
Use Digi Remote Manager to view and manage your device 463
Add a device to Digi Remote Manager 464
View Digi Remote Manager connection status 464
Use the Digi Remote Manager mobile app 465
Configure multiple devices using profiles 466
Learn more 466

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.

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 www.digi.com/products/cloud/digi-remote-manager.

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

Configure Digi Remote Manager

By default, your Connect IT device is configured to use central management using Digi Remote Manager.

Additional configuration options

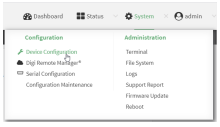
These additional configuration settings are not typically configured, but you can set them as needed:

- 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 Digi Remote Manager:

WebUI

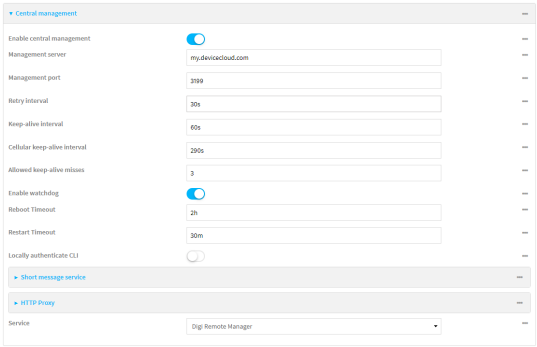
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



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, click **Enable central management**.

4. (Optional) For **Management server**, type the URL for the central management server. The default is the Digi Remote Manager server, my.devicecloud.com.
5. (Optional) For **Management port**, type the destination port for the remote cloud services connection. The default is **3199**.
6. (Optional) For **Retry interval**, type the amount of time that the Connect IT 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**.
7. (Optional) For **Keep-alive interval**, type the amount of time that the Connect IT 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**.
8. (Optional) For **Cellular keep-alive interval**, type the amount of time that the Connect IT 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**.
9. (Optional) For **Allowed keep-alive misses**, type the number of allowed keep-alive misses. The default is **3**.
10. **Enable 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.

11. 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.
12. (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.
13. (Optional) Configure the Connect IT 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.
    d. (Optional) Type the **Service identifier**.
14. (Optional) Configure the Connect IT device to communicate with remote cloud services by using an HTTP proxy server:
    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**.
15. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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 Digi Remote Manager support:

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

4. (Optional) Set the URL for the central management server. The default is the Digi Remote Manager server, my.devicecloud.com.

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

5. (Optional) Set the amount of time that the Connect IT 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 Connect IT 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 Connect IT 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. (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**.

12. (Optional) Configure the Connect IT 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 drm_phone_number
(config)>
```

c. (Optional) Set the service identifier:

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

3. (Optional) Configure the Connect IT 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)>
```

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.

Collect device health data and set the sample interval

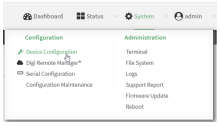
You can enable or disable the collection of device health data to upload to Digi Remote Manager, and configure the interval between health sample uploads. By default, device health data upload is enabled, and the health sample interval is set to 60 minutes.

To avoid a situation where several devices are uploading health metrics information to Remote Manager at the same time, the Connect IT 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:

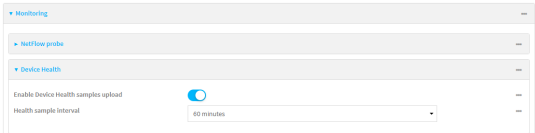
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

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



Device health data upload is enabled by default. To disable, click to toggle off **Enable Device Health samples upload**.

4. For **Health sample interval**, select the interval between health sample uploads.
5. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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
```

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

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.

Log into Digi Remote Manager

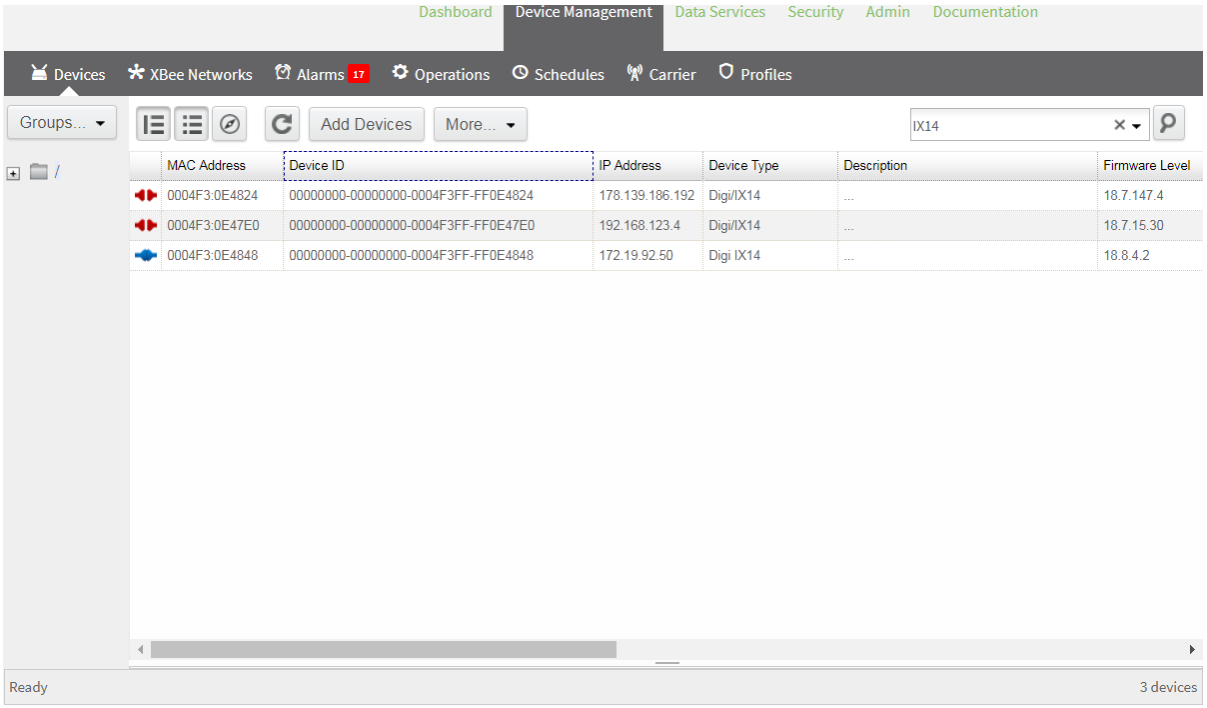
To start Digi Remote Manager

1. If you have not already done so, click here 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. Log into your Digi Remote Manager account.

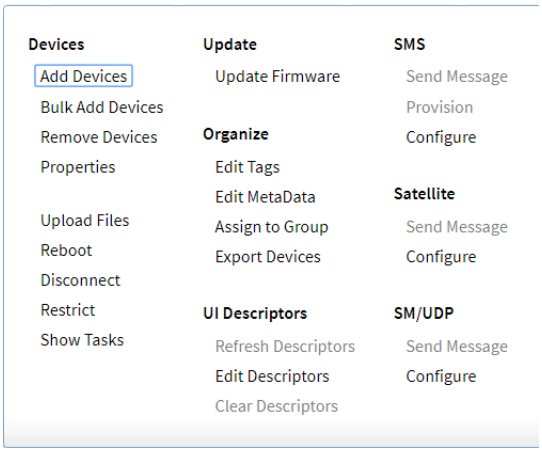
Use Digi Remote Manager to view and manage your device

To view and manage your device:

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. Use the Search bar to locate the device you want to manage.



4. Select the device and click **Properties** to view general information for the device.
5. Click the **More** menu to perform a task.



Add a device to Digi Remote Manager

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. Click **Add Devices**.
4. Select **MAC Address** and enter the Ethernet MAC address for your device.
5. For **Install Code**, 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. Click **Add**.
7. Click **OK**.

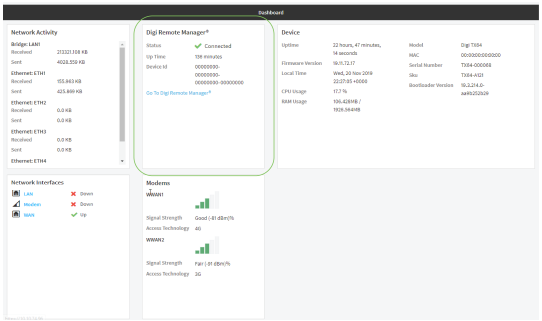
Digi Remote Manager adds your Connect IT device to your account and it appears in the **Device Management** view.

View Digi Remote Manager connection status

To view the current Digi Remote Manager configuration:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. The dashboard includes a Digi Remote Manager status pane:



Command line

1. Log into the Connect IT 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. View the central management configuration:

```
(config)> show cloud
drm
    cellular_keep_alive 290s
    drm_url my.devicecloud.com
    keep_alive 60s
    keep_alive_misses 3
    retry_interval 30s
enable true
(config)>
```

1. Type **cancel** to exit configuration mode:

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

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.

To view the status of your device's connection to Remote Manager, use the show cloud command at the command line:

Command line

```
> show cloud

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

 Status    : Connected
 Server    : my.devicecloud.com
 Device ID : 00000000-00000000-0040FFFF-FF0F4594
>
```

The **Device ID** is the unique identifier for the device, as used by the Remote Manager.

Use the Digi Remote Manager mobile app

If you have a smart phone or tablet, you can use the Digi Remote Manager mobile app to automatically provision a new devices and monitor devices in your account.

To download the mobile app:

- For iPhone, go to the **App Store**
- For Android phones, go to **Google Play**

To sign up for a new Digi Remote Manager account using the mobile app:

1. From the menu, click **Log in or Sign Up**.
2. Click **Sign up** to create a new account.

3. You'll receive an email with login instructions.
4. From the **Digi Remote Manager** mobile app, click **Log in** and log into your new account.

   To register a new device:

   1. From the menu, select **Install a device with a QR or bar code** and scan the installation QR code on the label.
   2. Follow the prompts to complete your Connect IT registration.

   Digi Remote Manager registers your Connect IT and adds it to your Digi Remote Manager device list. You can now manage the device remotely using Digi Remote Manager.

Configure multiple devices using profiles

Digi recommends you take advantage of Digi Remote Manager profiles to manage multiple Connect IT routers. Typically, if you want to provision multiple Connect IT routers:

1. Using the Connect IT local WebUI, configure one Connect IT router to use as the model configuration for all subsequent Connect ITs you need to manage.
2. Register the configured Connect IT device in your Digi Remote Manager account.
3. In Digi Remote Manager, create a profile based on the configured Connect IT.
4. Apply the profile to the Connect IT devices you need to configure.

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

Learn more

- For information on using Digi Remote Manager to configure and manage Connect IT routers, see the *Digi Remote Manager User Guide*.
- For information on using Digi Remote Manager APIs to develop custom applications, see the *Digi Remote Manager Programmer Guide*.

File system

This chapter contains the following topics:

The Connect IT local file system 468
Display directory contents 468
Create a directory 469
Display file contents 470
Copy a file or directory 470
Move or rename a file or directory 471
Delete a file or directory 472
Upload and download files 473

The Connect IT local file system

The Connect IT local file system has approximately 30 MB of space available for storing files, such as alternative configuration files and firmware versions, and release files, such as cellular module images. The writable directories within the filesystem are:

- /tmp
- /opt
- /etc/config

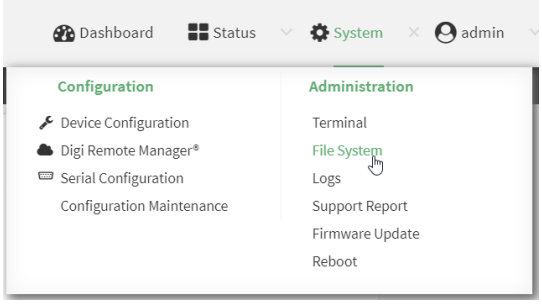
Files stored in the /tmp directory do not persist across reboots. Therefore, /tmp is a good location to upload temporary files, such as files used for firmware updates. Files stored in /opt and /etc/config do persist across reboots, but are deleted if a factory reset of the system is performed. See Reset the device to factory defaults for more information.

Display directory contents

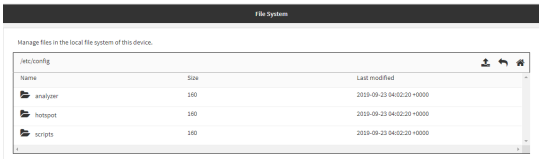
To display directory contents by using the WebUI or the Admin CLI:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight a directory and click ♎ to open the directory and view the files in the directory.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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 contenct 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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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.

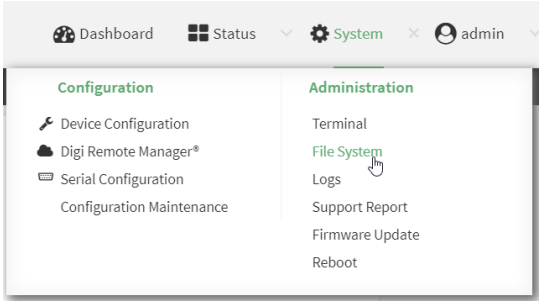
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a file or directory

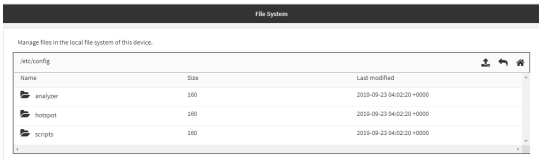
To delete a file or directory by using the WebUI or the Admin CLI:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the directory containing the file to be deleted and click to open the directory.
4. Highlight the file to be deleted and click .
5. Click **OK** to confirm.

Command line

To delete a file named **test.py** in **/etc/config/scripts**:

1. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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.

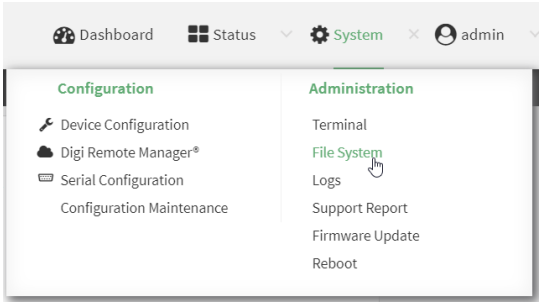
Upload and download files

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.

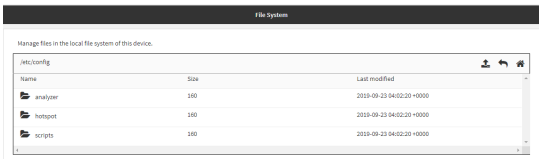
Upload and download files by using the WebUI

Upload files

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



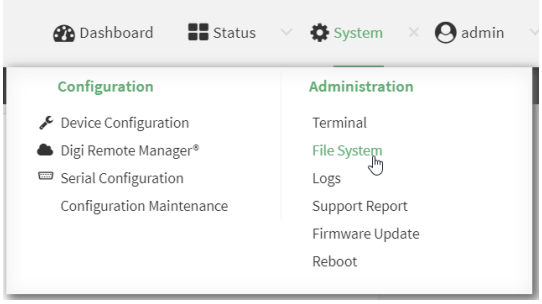
   The **File System** page appears.



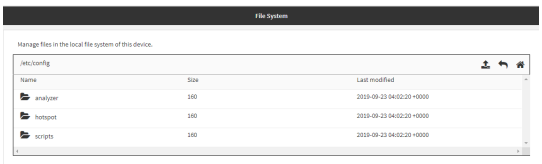
3. Highlight the directory to which the file will be uploaded and click ⏏ to open the directory.
4. Click ❽ (upload).
5. Browse to the location of the file on your local machine. Select the file and click **Open** to upload the file.

Download files

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the directory to which the file will be uploaded and click to open the directory.
4. 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 Connect IT device

To copy a file from a remote host to the Connect IT 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 Connect IT device.
- *local-path* is the location on the Connect IT 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 Connect IT device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect IT-20.5.38.39.bin local /etc/config/ to local
admin@192.168.4.1's password: adminpwd
Connect IT-20.5.38.39.bin          100%   36MB   11.1MB/s    00:03
>
```

Transfer a file from the Connect IT device to a remote host

To copy a file from the Connect IT 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 Connect IT device.

For example:

To copy a support report from the Connect IT 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 /etc/config/
Saving support report to /etc/config/support-report-0040D0133536-20-05-29-13.22.15.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 /etc/config/support-report-
00:40:D0:13:35:36-20-05-29-13.22.15.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-20-05-29-13.22.15.bin
>
```

Upload and download files using SFTP

Transfer a file from a remote host to the Connect IT device

This example uploads firmware from a remote host to the Connect IT 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 Connect IT-20.5.38.39
Uploading Connect IT-20.5.38.39 to Connect IT-20.5.38.39
Connect IT-20.5.38.39                                    100%  24M  830.4KB/s   00:00
sftp> exit
$
```

Transfer a file from the Connect IT device to a remote host

This example downloads a file named **test.py** from the Connect IT 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:

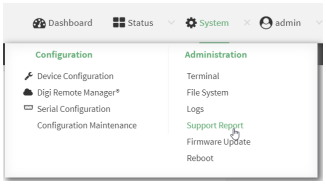
Generate a support report 478
View system event logs 479
Configure syslog servers 484
Configure options for the event and system logs 486
Analyze network traffic 490
Use the ping command to troubleshoot network connections 502
Use the traceroute command to diagnose IP routing problems 502

Generate a support report

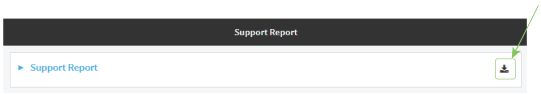
To generate and download a support report:

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Administration**, click **Support Report**.



3. Click to generate and download the support report.



Attach the support report to any support requests.

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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 /etc/config/
Saving support report to /etc/config/support-report-0040D0133536-20-05-29-13.22.15.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 /etc/config/support-report-
00:40:D0:13:35:36-20-05-29-13.22.15.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-20-05-29-13.22.15.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.

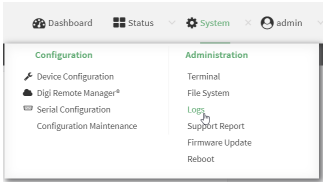
View system event logs

See Configure options for the event and system logs for information about configuring the information displayed in event and system logs.

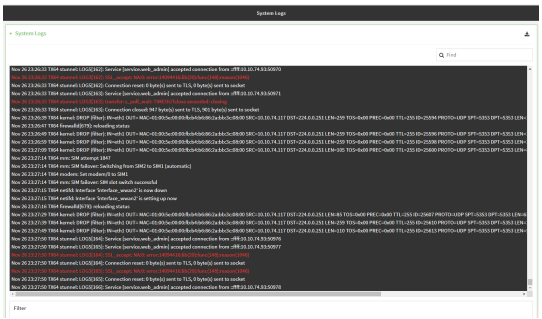
View System Logs

WebUI

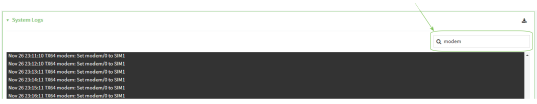
1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System** > **Logs**.



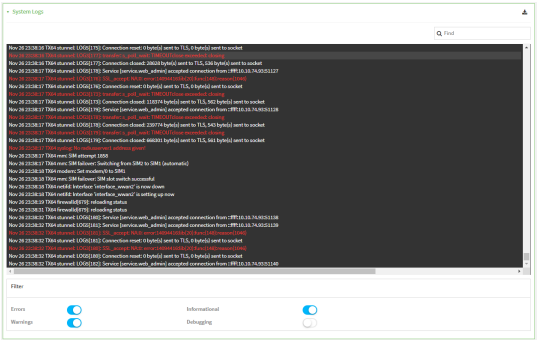
The system log displays:



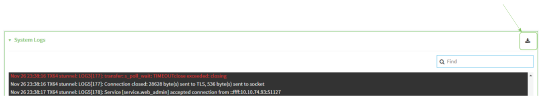
3. Limit the display in the system log by using the **Find** search tool.



4. Use filters to configure the types of information displayed in the system logs.



5. Click to download the system log.



Command line

1. Log into the Connect IT command line as a user with Admin access.

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

2. Use show log at the Admin CLI prompt:

```
> show log

Timestamp       Message
--------------  ------------------------------------------------------------
Nov 26 21:54:34  Connect IT netifd: Interface 'interface_wan' is setting up now
Nov 26 21:54:35  Connect IT 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  Connect IT netifd: Interface 'interface_wan' is setting up now
Nov 26 21:54:35  Connect IT 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
...
>
```

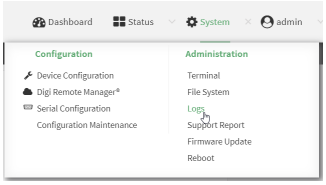
5. Type **exit** to exit the Admin CLI.

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

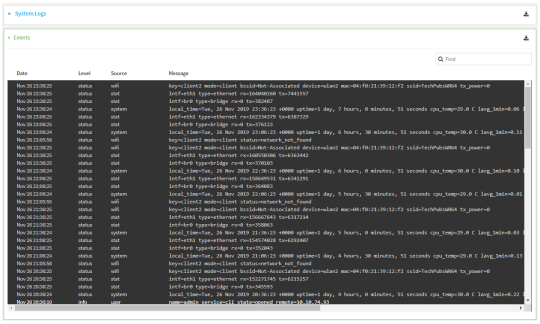
View Event Logs

WebUI

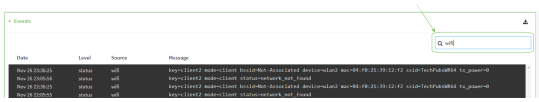
1. Log into the Connect IT WebUI as a user with Admin access.
2. On the main menu, click **System** > **Logs**.



3. Click **System Logs** to collapse the system logs viewer, or scroll down to **Events**.
4. Click **Events** to expand the event viewer.



5. Limit the display in the event log by using the **Find** search tool.



6. Click to download the event log.

Command line

1. Log into the Connect IT command line as a user with Admin access.

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

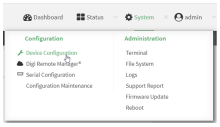
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure syslog servers

You can configure remote syslog servers for storing event and system logs.

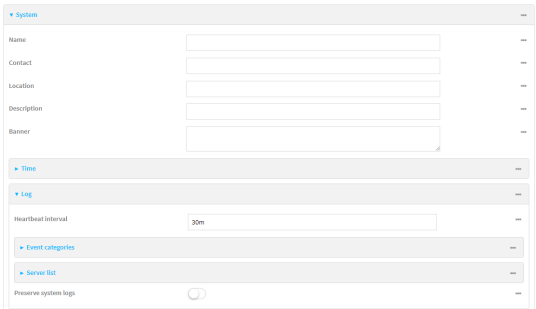
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

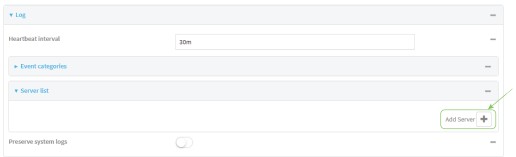


The **Configuration** window is displayed.

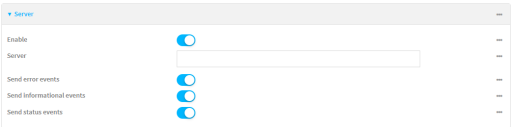
3. Click **System** > **Log**.



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, click to 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.

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

Command line

1. Log into the Connect IT 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 1)>
```

   b. Enable the server:

```
(config system log remote 1)> enable true
(config system log remote 1)>
```

   c. Set the host name or IP address of the server:

```
(config system log remote 1)> server hostname
(config system log remote 1)>
```

   d. The event categories that will be sent to the server are automatically enabled when the server is enabled. To disable:
      - To disable informational event messages:

```
(config system log remote 1)> info false
(config system log remote 1)>
```

      - To disable status event messages:

```
(config system log remote 1)> status false
(config system log remote 1)>
```

      - To disable informational event messages:

```
(config system log remote 1)> error false
(config system log remote 1)>
```

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 options for the event and system logs

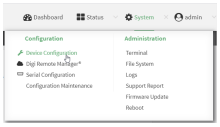
The default configuration for event and system logging is:

- 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:

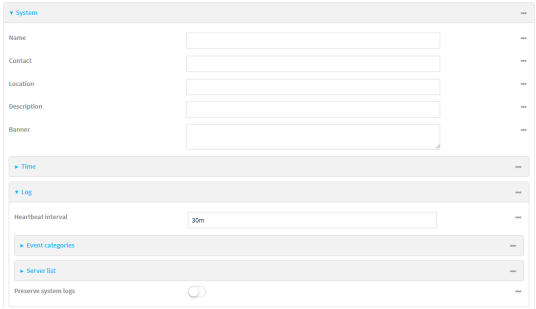
WebUI

1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. 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 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.
6. (Optional) See Configure syslog servers for information about configuring remote syslog servers to which log messages will be sent.
7. Enable **Preserve system logs** to save the current session's system log after a reboot.

   By default, the Connect IT 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.

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

Command line

1. Log into the Connect IT 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 Connect IT 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
 wireless            WiFi
 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.

Analyze network traffic

The Connect IT 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 491
Example filters for capturing data traffic 495
Capture packets from the command line 496
Stop capturing packets 497
Show captured traffic data 497
Save captured data traffic to a file 499
Download captured data to your PC 500
Clear captured data 501

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.

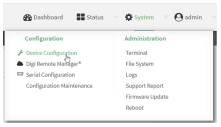
Additional configuration items

- 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.

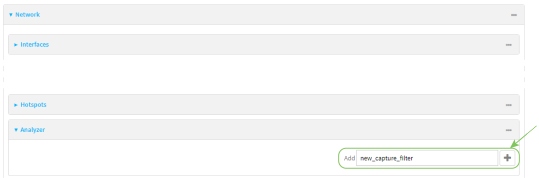
To configure a packet capture configuration:

WebUI

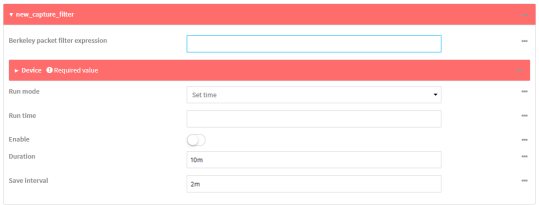
1. Log into the Connect IT WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   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. 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.
6. (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.
7. (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**.
8. Click **Apply** to save the configuration and apply the change.

Command line

1. Log into the Connect IT 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>
/network/device/lan              /network/device/loopback
/network/device/wan              /network/interface/defaultip
/network/interface/defaultlinklocal /network/interface/lan
/network/interface/loopback      /network/interface/modem
/network/interface/wan
(config network analyzer name)> add interface end /network/
```

   Repeat to add additional interfaces.

5. (Optional) Set a filter for the capture filter:

```
(config network analyzer name)> filter 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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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 : May-29-2020 20:34:19.287682, 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. Log into the Connect IT command line as a user with Admin access.

   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* name *capture_filter*
   >

   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
     ```

   - *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 save name ?

     name: Name of the capture filter to use.
     ```

```
Format:
  test_capture
  capture_ping

> analyzer save name
```

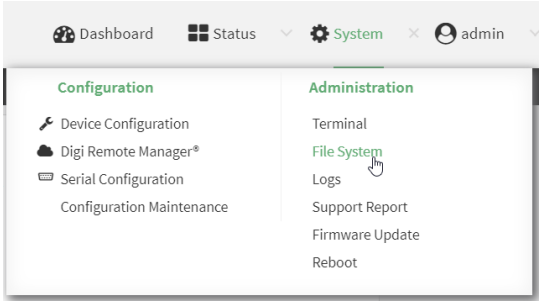
The file is stored in the **/etc/config/analyzer** directory. To transfer the file to your PC, see Download captured data to your PC.

Download captured data to your PC

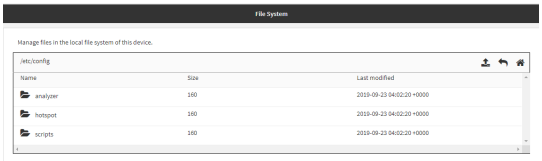
After saving captured data to a file (see Save captured data traffic to a file), you can download the file from the WebUI or from the command line by using the scp (secure copy file) command.

WebUI

1. Log into the Connect IT WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the **analyzer** directory and click to open the directory.
4. Select the saved analyzer report you want to download and click (download).

Command line

1. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT 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. Log into the Connect IT command line as a user with Admin access.

   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. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT 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. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT 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

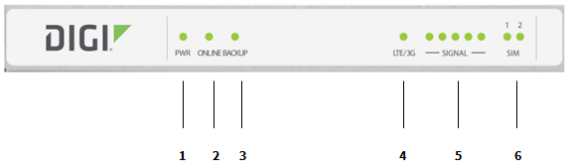
To stop the traceroute process, enter **Ctrl-C**.

Hardware

Connect IT 4 hardware and LEDs

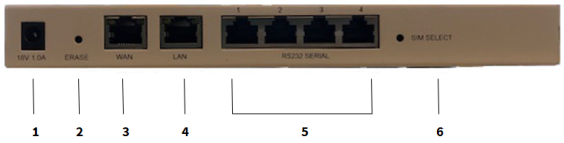
This section includes details about the front and back panels.

Front panel and LEDs



Item	Name	Description
1	PWR	Indicates whether unit is powered up. This LED is hardwired to the power input.
2	ONLINE	Indicates status of the cellular network connection. ■ Flashing: The unit is attempting to establish a cellular network connection. ■ Solid: A cellular connection has been established.
3	BACKUP	Indicates the status of the backup connection on the LAN. ■ Flashing: The unit is attempting to establish a backup connection on the LAN. ■ Solid: A backup network connection has been established on the LAN.
4	LTE/3G	Indicates a 4G\LTE or 2G/3G connection. See Cellular network fallback.
5	SIGNAL	Indicates the cellular network signal strength. See Signal strength.
6	SIM 1 SIM 2	Indicates which SIM has been selected, using the SIM SELECT button on the back of the unit. See Select SIM card.

Back panel



Item	Name	Description
1	Power	Connect the power supply unit to the device. For information about exchanging the power tips, see Exchange power tips.
2	Erase	Press this switch to reset the device. See Use the RESET button to reset your device to the factory defaults.
3	WAN	Indicates connection to Ethernet network. See Connect hardware and connect to site network using an Ethernet LAN.
4	LAN	Connect to an Ethernet port to establish backup connectivity, LAN connectivity using passthrough\bridge mode or DNCHP server\router mode.
5	Serial ports	Connect equipment to a serial port to provide console access to the equipment through the cellular network. See Connect equipment to the Connect IT serial ports.
6	SIM SELECT	Use the SIM SELECT button to select a SIM card: 1 or 2. See Select SIM card.

Signal strength

The signal bars show the strength of the cellular network connection.

See Cellular network fallback.

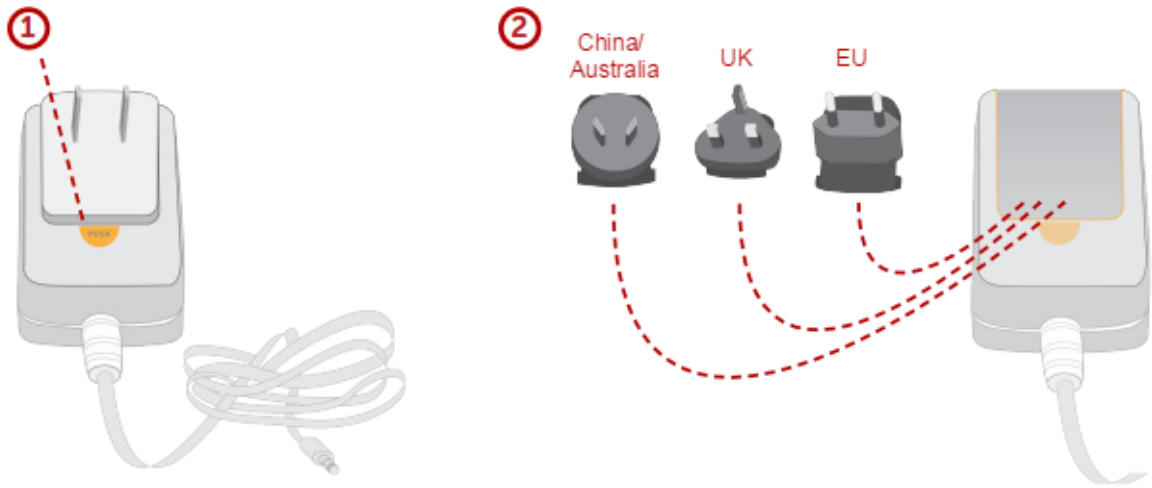
Signal Bars	dBm	Signal Strength Percent	Quality
	-110 to -106	0-11%	Bad
	-105 to -96	12-28%	Marginal
	-95 to -84	29-47%	OK
	-83 to -76	48-60%	Good
	-75 to -50	61-100%	Excellent

Exchange power tips

The Connect IT may include four interchangeable plug tips that allow the Power Supply Unit (PSU) to operate in most countries. The PSU comes with the United States style plug installed.

To change the plug tip:

1. Place the tip of a small flathead screw driver in the half-circle area below the power prongs (the **PUSH** button), and slide the current plug tip forward.
2. Pull off the attached plug converter.
3. Slide the new tip down into place until it clicks.



Note For more information regarding power-tip compatibility with global deployments, visit www.worldstandards.eu/electricity/plugs-and-sockets/.

Select SIM card

You can use the SIM button on the back of the unit to select which SIM card you want to use: first or second.

1. Power on the unit.
2. Press the SIM SELECT button on the back of the unit.
3. On the front of the device, verify which SIM LED is illuminated: SIM 1 or SIM 2.
    - If the LED for the desired SIM LED is illuminated, the process is complete.
    - If the LED for the desired SIM LED is not illuminated, press the SIM SELECT button again. Verify that the desired SIM LED is illuminated.

Troubleshooting

Cellular network fallback

If the Connect IT 4 doesn't recognize the available 4G/LTE network, the Connect IT 4 automatically falls back to the highest available 3G network.

Use the RESET button to reset your device to the factory defaults

You can reset the Connect IT to the factory default settings. Resetting the device to factory defaults performs the following actions:

- Clears all configuration settings.
- All firmware updates are deleted.
- Deletes all user files.
- Regenerates SSH keys.
- Clears event and system log files.
- Creates a new event in the event log, indicating a factory reset.

Note While the settings are reset, the device's firmware version remains the same.

1. Make sure that the Connect IT has been powered on for at least 30 seconds.
2. Locate the **ERASE** button on the back of the device.
3. Press and hold the **ERASE** button for 5 seconds. The device beeps five times during the reset.
4. The device resets to factory defaults and then reboots automatically.

Tips for improving cellular signal strength

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

- If available, connect a different set of antennas.
- Purchase a Digi Antenna Extender Kit: Antenna Extender Kit, 1 m.

Download a support report

You can download a support report from the device to provide to technical support. The report file contains all of the current details for the device's state, and a full record of the system logs from the device.

See Generate a support report.

Regulatory and safety information

FCC certifications

USA

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference as his own expense.

INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A)

This product is intended for operation in a commercial or industrial environment and should not be used in a residential environment. This product has been tested and found to comply with the requirements of:

ICES-003 -- Information Technology Equipment--Limits and Methods of Measurement Issue 5, August 2012

European Union

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Safety warnings

Review the following safety warnings for Connect IT.

WARNING! 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.

WARNING! 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.

WARNING! CA Prop 65 warning: This product contains chemicals known to the state of California to cause cancer, birth defects or other reproductive harm.

WARNING!

הוראות בטיחות לשימוש במטען

מטענים:

יש לפעול ע"פ כללי הבטיחות הבאים בעת שימוש במטענים:

- ודא שלמות ותקינות כבל החשמל והתקע.
- אין להכניס או להוציא את התקע מרשת החשמל בידיים רטובות
- אין לפתוח את המטען, במקרה של בעיה כלשהי, יש לפנות למעבדת השירות הקרובה
- יש להרחיק את המטען מנחלים
- במקרה של ריח מוזר, רעשים שמקורם במטען, יש לנתקו מיידית מרשת החשמל ולפנות למעבדת שירות
- המטען מיועד לשימוש בתוך המבנה בלבד, לא לשימוש חיצוני ולא לשימוש בסביבה לחה
- אין לחתוך, לשבור, ולעקם את כבל החשמל
- אין להניח חפצים על כבל החשמל או להניח לו להתחמם יתר על המידה, שכן הדבר עלול לגרום לנזק, דליקה או התחשמלות
- לפני ניקוי המטען יש לנתקו מרשת החשמל
- יש להקפיד לתחזק את התקן הניתוק במצב תפעולי ומוכן לשימוש

אזהרה:

- אין להחליף את כבל הזינה בתחליפים לא מקוריים, חיבור לקוי עלול לגרום להתחשמלות המשתמש
- בשימוש על כבל מאריך יש לוודא תקינות מוליך הארקה שבכבל
- מיועד לשימוש פנימי בלבד

CAUTION! Do not use an antenna that wasn't supplied by the manufacturer. If a different antenna is required, first consult Digi International Inc. for recommendations that suit your circumstances.

CAUTION! By pressing the ERASE button when powered up, the configuration of the Connect IT is **erased** and the unit reverts to factory default settings.

Command line interface

This chapter contains the following topics:

Access the command line interface 514
Log in to the command line interface 514
Exit the command line interface 515
Execute a command from the web interface 515
Display help for commands and parameters 516
Auto-complete commands and parameters 518
Available commands 519
Use the scp command 520
Display status and statistics using the show command 521
Device configuration using the command line interface 522
Execute configuration commands at the root Admin CLI prompt 523
Configuration mode 525
Command line reference 537

Access the command line interface

You can access the Connect IT 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: Configure the 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 Connect IT 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.
   - For serial connections, the default configuration is:
     - **115200** baud rate
     - **8** data bits
     - **no** parity
     - **1** stop bit
     - **no** flow control
   - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** 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
    1: Serial: port1      (9600,8,1,none,none)
    q: Quit

Select access or quit [admin] :
```

Type **a** or **admin** to access the Connect IT command line.

You will now be connected to the Admin CLI:

```
Connecting now, 'exit' to disconnect from 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
    1: Serial: port1      (9600,8,1,none,none)
    q: Quit

Select access or quit [admin] :
```

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

Execute a command from the web interface

1. Log into the Connect IT WebUI as a user with Admin access.
2. At the main menu, click **Terminal**. The device console appears.

```
Connect IT login:
```

3. Log into the Connect IT command line as a user with Admin access.

   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 Connect IT 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.
 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.
 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.
 dhcp-lease  Show DHCP leases.
 event       Show event list
 ipsec       Show IPsec statistics.
 log         Show syslog.
 manufacture Show manufacturer information.
 modem       Show modem statistics.
 network     Show network interface statistics.
 openvpn     Show OpenVPN statistics.
 route       Show IP routing information.
 serial      Show serial statistics.
 system      Show system statistics.
 version     Show firmware version.

 > 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>
..          ...          defaultip      defaultlinklocal 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.
cp	Copies a file or directory.
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.
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.
reboot	Reboots the Connect IT device.
rm	Removes a file.
scp	Uses the secure copy protocol (SCP) to transfer files between the Connect IT device and a 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.
system	Issues commands related to system functionality.
traceroute	Sends and tracks route packets to a destination host.
update	Updates the device firmware.

Note For commands that operate on the Connect IT'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 Connect IT 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 Connect IT device from a remote host, or to the remote host from the Connect IT device.
  - If the file is being copied to the Connect IT device from a remote host:
    - The path and filename of the file on the remote host that will be copied to the Connect IT device.
    - The location on the Connect IT device where the file will be copied.
  - If the file is being copied to a remote host from the Connect IT device:
    - The path and filename of the file on the Connect IT 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 Connect IT device

To copy a file from a remote host to the Connect IT 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 Connect IT device.
- *local-path* is the location on the Connect IT 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 Connect IT device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect IT-20.5.38.39.bin local /etc/config/ to local
admin@192.168.4.1's password: adminpwd
Connect IT-20.5.38.39.bin                100%    36MB    11.1MB/s       00:03
>
```

Transfer a file from the Connect IT device to a remote host

To copy a file from the Connect IT 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 Connect IT device.

For example:

To copy a support report from the Connect IT 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 /etc/config/
Saving support report to /etc/config/support-report-0040D0133536-20-05-29-13.22.15.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 /etc/config/support-report-
00:40:D0:13:35:36-20-05-29-13.22.15.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-20-05-29-13.22.15.bin
>
```

Display status and statistics using the show command

The Connect IT **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 Connect IT
  Serial Number        : Connect IT-000065
  SKU                  : Connect IT
  Hostname             : Connect IT
  MAC                  : DF:DD:E2:AE:21:18

  Hardware Version     : 50001947-01 1P
  Firmware Version     : 20.5.38.39
  Alt. Firmware Version : 20.5.38.39
  Bootloader Version   : 19.7.23.0-15f936e0ed

  Current Time         : Fri, 29 May 2020 21:14:12 +0000
  CPU                  : 1.4%
  Uptime               : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature          : 40C

>
```

show network

The show network command displays status and statistics for network interfaces.

```
> show network

 Interface        Proto  Status   Address
 ----------------  -----  -------  -------------------------------
 defaultip        IPv4   up       192.168.210.1/24
 defaultlinklocal 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 Connect IT 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.
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 Connect IT 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 Connect IT"
```

Example: Create a new user by using the command line

In this example, you will use the Connect IT command line to create a new user, provide a password for the user, and assign the user to authentication groups.

1. Log into the Connect IT 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

analyzer 538
cp 539
help 540
ls 541
mkdir 542
modem 543
modem puk status [imei STRING] [name STRING] 546
more 548
mv 549
ping 550
reboot 551
rm 552
scp 553
show 554
system 562
traceroute 564
update 567

analyzer

Analyzer commands.

analyzer clear name STRING

Clears the traffic captured by the analyzer.

Parameters

name

Name of the capture filter to use.

Syntax: STRING

analyzer save filename STRING name STRING

Saves the current captured traffic to a file.

Parameters

filename

The filename to save captured traffic to. The file will be saved to the device's /etc/config/analyzer directory.

Syntax: STRING

name

Name of the capture filter to use.

Syntax: STRING

analyzer start name STRING

Start a capture session of packets on this devices interfaces.

Parameters

name

Name of the capture filter to use.

Syntax: STRING

analyzer stop name STRING

Stops the traffic capture session.

Parameters

name

Name of the capture filter to use.

Syntax: STRING

cp

cp commands.

[force] SOURCE DESTINATION

Copy a file or directory.

Parameters

source

The source file or directory to copy.

Syntax: STRING

destination

The destination path to copy the source file or directory to.

Syntax: STRING

force

Do not ask to overwrite the destination file if it exists.

Syntax: BOOLEAN

Default: False

Optional: True

help

Show CLI editing and navigation commands.

Parameters

None

ls

Directory listing command.

ls [show-hidden] PATH

List a directory.

Parameters

path

List files and directories under this path.
Syntax: STRING

show-hidden

Show hidden files and directories. Hidden filenames begin with '.'.
Syntax: BOOLEAN
Default: False
Optional: True

mkdir

mkdir PATH

Create a directory. Parent directories are created as needed.

Parameters

path

The directory path to create.

Syntax: STRING

modem

Modem commands.

modem at [imei STRING] [name STRING] CMD

Send an AT command to the modem and display the response.

Parameters

cmd

The AT command string.
Syntax: STRING

imei

The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name

The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

modem at-interactive [imei STRING] [name STRING]

Start an AT command session on the modem's AT serial port.

Parameters

imei

The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name

The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

modem pin

PIN commands.

pin change [imei *STRING*] [name *STRING*] OLD-PIN NEW-PIN

Change the SIM's PIN code. Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Parameters

old-pin
The SIM's PIN code.
Syntax: STRING

new-pin
The PIN code to change to.
Syntax: STRING

imei
The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name
The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

pin disable [imei *STRING*] [name *STRING*] PIN
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.

Parameters

pin
The SIM's PIN code.
Syntax: STRING

imei
The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name
The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

pin enable [imei *STRING*] [name *STRING*] PIN
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.

Parameters

pin

The SIM's PIN code.

Syntax: STRING

imei

The IMEI of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

name

The configured name of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

pin status [imei *STRING*] [name *STRING*]

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

Parameters

imei

The IMEI of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

name

The configured name of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

pin unlock [imei *STRING*] [name *STRING*] PIN

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.

Parameters

pin

The SIM's PIN code.

Syntax: STRING

imei

The IMEI of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

name
The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

modem puk

PUK commands.

puk status [imei *STRING*] [name *STRING*]
Print the PUK status and the number of PUK unlock attempts remaining.

Parameters

modem puk status [*imei* STRING] [*name* STRING]

Print the PUK status and the number of PUK unlock attempts remaining.

imei
The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name
The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

puk unlock [imei *STRING*] [name *STRING*] PUK NEW-PIN
Unlock the SIM with a PUK code from the SIM provider.

Parameters

puk
The SIM's PUK code.
Syntax: STRING

new-pin
The PIN code to change to.
Syntax: STRING

imei
The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name
The configured name of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

modem reset [imei STRING] [name STRING]

Reset the modem hardware (reboot it). This can be useful if the modem has stopped responding to the network or is behaving inconsistently.

Parameters

imei

The IMEI of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

name

The configured name of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

modem sim-slot [imei STRING] [name STRING] SLOT

Show or change the modem's active SIM slot. This applies only to modems with multiple SIM slots.

Parameters

slot

The SIM slot to change to.

Syntax: (1|2|show)

imei

The IMEI of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

name

The configured name of the modem to execute this CLI command on.

Syntax: STRING

Optional: True

more

path

The file to view.

Syntax: STRING

mv

Move a file or directory.

mv [force] SOURCE DESTINATION

Parameters

source

The source file or directory to move.

Syntax: STRING

destination

The destination path to move the source file or directory to.

Syntax: STRING

force

Do not ask to overwrite the destination file if it exists.

Syntax: BOOLEAN

Default: False

Optional: True

ping

Ping a host using ICMP echo.

ping [ipv6] [countINTEGER] [interfaceSTRING] [sizeINTEGER] HOST

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.

Syntax: STRING

broadcast

Enable broadcast ping functionality

Syntax: BOOLEAN

Default: False

Optional: True

count

The number of ICMP ping requests to send before terminating.

Syntax: INT

Minimum: 1

Default: 100

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.

Syntax: STRING

Optional: True

ipv6

If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

Syntax: BOOLEAN

Default: False

Optional: True

size

The number of bytes sent in the ICMP ping request.

Syntax: INT

Minimum: 0

Default: 56

reboot

Reboot the system.

Parameters

None

rm

Remove a file or directory.

rm [force] PATH

Parameters

path

The path to remove.

Syntax: STRING

force

Force the file to be removed without asking.

Syntax: BOOLEAN

Default: False

Optional: True

scp

Copy a file or directory over SSH.

scp hostSTRINGlocalSTRING [portINTEGER] remoteSTRINGtoSTRINGuserSTRING

Parameters

host
The name or address of the remote host.
Syntax: STRING

local
The file to copy to or from on the local device.
Syntax: STRING

port
The SSH port to use to connect to the remote host.
Syntax: INT
Maximum: 65535
Minimum: 1
Default: 22

remote
The file to copy to or from on the remote host.
Syntax: STRING

to
Copy the file from the local device to the remote host, or from the remote host to the local device.
Syntax: (remote|local)

user
The username to use when connecting to the remote host.
Syntax: STRING

show

Show instance status statistics.

show analyzer name STRING

Show packets from a specified analyzer capture.

Parameters

name

Name of the capture filter to use.
Syntax: STRING

show arp [ipv4|ipv6|verbose]

Show ARP tables, if no IP version is specififed IPv4 IPV6 will be displayed.

Parameters

ipv4

Display IPv4 routes. If no IP version is specififed IPv4 and IPV6 will be displayed
Syntax: BOOLEAN
Default: False
Optional: True

ipv6

Display IPv6 routes. If no IP version is specififed IPv4 and IPV6 will be displayed
Syntax: BOOLEAN
Default: False
Optional: True

verbose

Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show cloud

Show Digi Remote Manager status statistics.

Parameters

None

show config

Show changes made to default configuration.

Parameters

None

show dhcp-lease [all|verbose]

Show DHCP leases.

Parameters

all

Show all leases (active and inactive (not in etc/config/dhcp.*lease)).
Syntax: BOOLEAN
Default: False
Optional: True

verbose

Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show event [number INTEGER] [table STRING]

Show event list (high level).

Parameters

number

Number of lines to retrieve from log.
Syntax: INT
Minimum: 1
Default: 20

table

Type of event log to be displayed (status, error, info).
Syntax: (status|error|info)
Optional: True

show hotspot [ip STRING] [name STRING]

Show hotspot statistics.

Parameters

ip

IP address of a specific client, to limit the status display to only this client.
Syntax: STRING
Optional: True

name

The configured instance name of the hotspot.

Syntax: STRING

Optional: True

show ipsec [all] [tunnel STRING]

Show IPsec status statistics.

Parameters

all

Display all tunnels including disabled tunnels.

Syntax: BOOLEAN

Default: False

Optional: True

tunnel

Display more details and config data for a specific IPsec tunnel.

Syntax: STRING

Optional: True

verbose

Display status of one or all tunnels in plain text.

Syntax: BOOLEAN

Default: False

Optional: True

show location

Show location information.

Parameters

None

show log [filter STRING] [number INTEGER]

Show system log (low level).

Parameters

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'.

Syntax: (critical|warning|debug|info)

Optional: True

number
Number of lines to retrieve from log.
Syntax: INT
Minimum: 1
Default: 20

show manufacture [verbose]

Show manufacturer information.

Parameters

verbose
Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show modem [verbose] [imei STRING] [name STRING]

Show modem status and statistics.

Parameters

imei
The IMEI of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

name
The configured name of the modem to execute this CLI command on.
Syntax: STRING
Optional: True

verbose
Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show network [all|verbose] [interface STRING]

Show network interface status and statistics.

Parameters

all
Display 4all interfaces including disabled interfaces.
Syntax: BOOLEAN

Default: False
Optional: True

interface
Display more details and config data for a specific network interface.
Syntax: STRING
Optional: True

verbose
Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show openvpn

Show OpenVPN status and statistics.

openvpn client [*all*] [name *STRING*]
Show OpenVPN client status statistics.

Parameters

all
Display all clients including disabled clients.
Syntax: BOOLEAN
Default: False
Optional: True

name
Display more details and config data for a specific OpenVPN client.
Syntax: STRING
Optional: True

openvpn server [*all*] [name *STRING*]
Show OpenVPN server status and statistics.

Parameters

all
Display all servers including disabled servers.
Syntax: BOOLEAN
Default: False
Optional: True

name
Display more details and config data for a specific OpenVPN server.
Syntax: STRING

Optional: True

show route [ipv4|ipv6|verbose]

Show IP routing information.

Parameters

ipv4

Display IPv4 routes.
Syntax: BOOLEAN
Default: False
Optional: True

ipv6

Display IPv6 routes.
Syntax: BOOLEAN
Default: False
Optional: True

verbose

Display more information (less concise, more detail).
Syntax: BOOLEAN
Default: False
Optional: True

show serial PORT

Show serial status and statistics.

Parameters

port

Display more details and config data for a specific serial port.
Syntax: STRING
Optional: True

show system [verbose]

Show system status and statistics.

Parameters

verbose

Display more information (disk usage, etc)
Syntax: BOOLEAN
Default: False
Optional: True

show usb

Show USB information.

Parameters

None

show version [verbose]

Show firmware version.

Parameters

verbose

Display more information (build date)

Syntax: BOOLEAN

Default: False

Optional: True

show web-filter

Show web filter status and statistics.

Parameters

None

show wifi

Show Wi-Fi status and statistics.

wifi ap [*all*] [name *STRING*]

Display details for Wi-Fi access points.

Parameters

all

Display all Wi-Fi access points including disabled Wi-Fi access points.

Syntax: BOOLEAN

Default: False

Optional: True

name

Display more details for a specific Wi-Fi access point.

Syntax: STRING

Optional: True

wifi client [*all*] [name *STRING*]

Display details for Wi-Fi client mode connections.

Parameters

all

Display all Wi-Fi clients including disabled Wi-Fi client mode connections.

Syntax: BOOLEAN

Default: False

Optional: True

name

Display more details for a specific Wi-Fi client mode connection.

Syntax: STRING

Optional: True

system

System commands.

system backup [passphrase STRING] type STRING PATH

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.

Parameters

path

The file path to save the backup to.

Syntax: STRING

passphrase

Encrypt the archive with a passphrase.

Syntax: STRING

Optional: True

Depends on: **type** equals 'archive'

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.

Syntax: (cli-config|archive)

Default: archive

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.

Parameters

None

system factory-erase

Erase the device to restore to factory defaults. All configuration and automatically generated keys will be erased.

Parameters

None

system restore [passphrase STRING] PATH

Restore the device's configuration from a backup archive or CLI commands file.

Parameters

path

The path to the backup file.

Syntax: STRING

passphrase

Decrypt the archive with a passphrase.

Syntax: STRING

Optional: True

system support-report PATH

Save a support report to a file and include with support requests.

Parameters

path

The file path to save the support report to.

Syntax: STRING

traceroute

Print the route packets trace to network host.

traceroute [bypass|debug|dontfragment|icmp|ipchecksums|nomap|verbose] [first_ttlINTEGER] [gatewaySTRING] [interfaceSTRING] [max_ttlINTEGER] [nqueriesINTEGER] [packetlenINTEGER] [pausemsecsINTEGER] [portINTEGER] [src_addrSTRING] [tosINTEGER] [waittimeINTEGER] HOST

Parameters

host

The host that we wish to trace the route packets for.

Syntax: STRING

bypass

Bypass the normal routing tables and send directly to a host on an attached network.

Syntax: BOOLEAN

Default: False

Optional: True

debug

Enable socket level debugging.

Syntax: BOOLEAN

Default: False

Optional: True

dontfragment

Do not fragment probe packets.

Syntax: BOOLEAN

Default: False

Optional: True

first_ttl

Specifies with what TTL to start.

Syntax: INT

Minimum: 1

Default: 1

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

Syntax: STRING

Optional: True

icmp

Use ICMP ECHO for probes.

Syntax: BOOLEAN

Default: False

Optional: True

interface

Specifies the interface through which traceroute should send packets. By default, the interface is selected according to the routing table.

Syntax: STRING

Optional: True

ipv6

If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

Syntax: BOOLEAN

Default: False

Optional: True

max_ttl

Specifies the maximum number of hops (max time-to-live value) traceroute will probe.

Syntax: INT

Minimum: 1

Default: 30

nomap

Do not try to map IP addresses to host names when displaying them.

Syntax: BOOLEAN

Default: False

Optional: True

nqueries

Sets the number of probe packets per hop. A value of -1 indicated

Syntax: INT

Minimum: 1

Default: 3

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.

Syntax: INT

Minimum: -1

Default: -1

pausemsecs

Minimal time interval between probes

Syntax: INT

Minimum: 0

Default: 0

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.

Syntax: INT

Minimum: -1

Default: -1

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.

Syntax: STRING

Optional: True

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.

Syntax: INT

Minimum: -1

Default: -1

waittime

Determines how long to wait for a response to a probe.

Syntax: INT

Minimum: 1

Default: 5

update

Update firmware.

update firmware file STRING

Update device firmware

Parameters

file

Firmware filename and path.

Syntax: STRING