

Dejero

**Titan Command
User Guide
September 2025
UG-150-001**

Dejero

Dejero Labs Inc.

410 Albert Street, Suite 200
Waterloo, Ontario, N2L 3V3
+1 519 772 4824

Copyright, Trademarks, and Patents

Copyright © 2025 Dejero Labs Inc.

Dejero is a trademark of Dejero Labs Inc. Wi-Fi is a trademark of the Wi-Fi Alliance.

All other trademarks are the property of their respective owners.

Dejero products or portions thereof are protected by patents granted and pending.

Actual product might vary from the images in this guide.

Symbols and Conventions

This document uses the following symbols and conventions:



Note: Shares important related information, reminders, recommendations, and suggestions.



Tip: Shares helpful tips or alternative ways to accomplish a goal.



Caution: Means that the action you take could cause harm to your equipment or device, cause you to lose data, or void your warranty.



Warning: Describes an action that could cause you physical harm. Follow the guidelines in this document or the device itself when handling electrical equipment.

Contents

Safety Warnings and Hazards	4
Handling and Operating Conditions	6
About the Dejero Titan solution	6
What's included	8
About WAN and LAN connections	9
I/O Overview	10
Setting up the Titan device	11
Using the Titan device	15
Connecting Titan with other devices	16
Configuring Titan with Control	16
Managing device profiles	26
Using the Titan Web User Interface	29
Using routed mode and multi-WAN routing	35
Enable Static Routing for a router	37
Configuring the VPN Client	42
Configuring the device with the Titan local user interface	43
Monitoring the Titan device	45
Troubleshooting	51
Technical specifications	53
Additional help	56
Document revision history	56

Warranty and Liability

Reasonable care has been taken in preparing the information in this document. However, this document may contain omissions, technical inaccuracies, or typographical errors. Dejero Labs Inc. does not accept responsibility of any losses due to the use of this document. Product specifications are subject to change without notice.

Due to the nature of wireless communication, transmission and reception of data can never be guaranteed. While Dejero strives to provide high-quality video and seamless data transmission without significant delays, environmental and cellular network conditions beyond Dejero's control may result in data delay, corruption, or loss.

Dejero accepts no responsibility for and is not liable for any loss or damage, including, but not limited to, revenue or personal injury, resulting from delays in, errors in, or failure to transmit or receive data using the Dejero platform.

Warranty on the Dejero Titan solution is voided if the case is opened by anyone who has not been trained and certified by Dejero. For details, see Handling and Operating Conditions below.

Safety Warnings and Hazards

Read this section in its entirety before operating the Titan device.

Class A device

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 at his own expense.

Federal Communications Commission statement

The Titan device complies with Part 15 of the FCC rules for a Class A device.

Industry Canada statement

The Titan device complies with Industry Canada ICES-003 Class A specifications.

RF Exposure Notice

THIS DEVICE MEETS THE GOVERNMENT REQUIREMENTS FOR EXPOSURE TO RADIO WAVES.

The Titan device is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government and Industry Canada.

The Titan device has internal cellular and Wi-Fi antennas.

At least 20 cm (8 inches) separation must be maintained between the antennas and the user's body or nearby people at all times.

Explosive Atmosphere

The Titan device should be powered off in an area with a potentially explosive atmosphere such as fueling areas, fuel or chemical transfer or storage areas, below deck on boats, or in areas where the air contains chemicals or particles such as grain, dust or metal powders. It is rare, but there is potential for PC-like devices, such as the Titan device, to generate sparks, which could trigger an explosion. Do not store the Titan device in the compartment of a vehicle that contains flammable gas, liquid, or explosives.

Blasting or Construction Sites

The Titan device should be powered off in areas where blasting is in progress, where explosives may be present, or near any other equipment that is susceptible to radio interference.

Hospitals

The Titan device should be powered off near medical equipment or life support systems, or near any other equipment that is susceptible to radio interference. Hospitals or other medical facilities often ask visitors, patients, and staff to switch off all electronic devices in some areas. Please make sure that you follow any local rules and regulations.

Medical Implant Devices

It is possible that the radio modems in the Titan device may interfere with some types of medical devices (such as cardiac pacemakers or implant defibrillators), when operated close to the device. If you have one of these devices, you should seek advice from your doctor before operating the Titan device.

Hearing Devices

People with hearing aids or cochlear implants may experience interfering noises when using or when nearby mobile devices. The level of interference depends on the type of aid or implant, the type of mobile device, and the distance between the two. Increasing the distance between the Titan device and the hearing device may reduce interference.

Electrical Safety

Disconnect all power sources before servicing the unit. The Titan device should only be serviced by **authorized Dejero personnel**.

The power-outlet shall be installed near the equipment and shall be easily accessible.

The integrity of the protective earth must be ensured.

Battery



Warning: There is a risk of explosion if the CMOS battery is replaced with an incorrect type. The Titan device should only be serviced by authorized Dejero personnel.

Handling and Operating Conditions

Read this section in its entirety before operating the Titan device.

Handle Device with Care

It is possible to damage or knock loose the electronics inside of the Titan device if it is dropped or thrown. Please handle with care. Damage sustained as the result of mishandling the Titan renders the warranty null and void.

Do Not Disassemble the Product

Only authorized Dejero personnel can open, modify, or repair the Titan unit. Unless authorized by Dejero personnel, any attempt by the user to open, disassemble, or repair the device renders the warranty null and void.

Keep Device as Cool as Possible

For optimal performance, keep the Titan device in a well-ventilated area, with 0.6 m/s airflow around it. Keep the device away from heat sources and direct exposure to sunlight. Do not operate the Titan device in temperatures outside of the ambient range (-40°C to +70° C /-40°F to 158°F)

Keep Device Dry

Keep the Titan device dry. Do not expose it to liquid, moisture, or excessive humidity.

Data Usage

With the Titan solution, data is billed monthly per unit. If you use the cellular network for extended periods of time or you transfer large files (such as video files) over the cellular network, you will use large amounts of data. If you use more than your monthly data allocation, additional charges apply.

About the Dejero Titan solution

The Titan Command devices are designed to deliver reliable connectivity for general-purpose applications, including voice, video, and data while in nomadic or mobile environments, as well as add wireless connectivity to fixed locations.

Powered by Dejero Smart Blending Technology, Titan devices aggregate diverse connectivity paths from multiple providers to deliver enhanced reliability, expanded coverage, and greater bandwidth. With integrated modems that connect to internal antennas, Titan devices provide optimal performance and support VPN tunneling for secure access to private networks.

The Dejero Titan Command network aggregation devices provide reliable connectivity to the internet, cloud applications, and private networks. The ruggedized and fan-less chassis is ideal for installation in vehicles and portable kits.

Enhanced reliability

Titan devices blend 4G / 5G cellular connections and any other wired or wireless IP connection from multiple network providers to achieve diversity and deliver greater reliability.

Expanded coverage

Avoid location-based coverage gaps. Aggregate multiple network services into a single virtual “network of networks,” providing a greater coverage area than what a single provider can deliver alone.

Greater bandwidth

By continuously measuring each connection in real-time, the Titan devices dynamically distribute packets across the multiple connections. Using the bandwidth potential of all connections to achieve greater upload and download capacity.

Cloud management

Remotely configure devices without field user interventions, monitor device status in real time, set proactive alerts, and view detailed analytics on data usage and performance – anywhere from a web browser in Dejero Control.

Additional features

- **Always connected:** Superior to a failover solution, stay connected using Dejero’s patented Smart Blending Technology.
- **Connection priority:** Define priority connections to help manage costs and customize network utilization.
- **Enhanced security:** Keep your real-time video and data secure by dynamically routing packets over multiple connections.
- **Reliable cloud access:** Access cloud-based applications without fear of losing connectivity in mobile environments.

- **Easy to use:** Simple, intuitive user interface requires minimal effort for field operatives.
- **Rapid development:** Easy installation, setup, and remote configuration using a web interface.
- **VPN support:** Transparent, high-speed VPN support provides secure access to private networks from remote locations. For more information on optimizing the configuration of your VPN, contact Dejero Support.
- **Software updates:** Performance, feature, and security enhancements are provided with software updates.
- **FirstNet Capable™**
- **Verizon Frontline Verified**
- **Private Wi-Fi® hotspot**

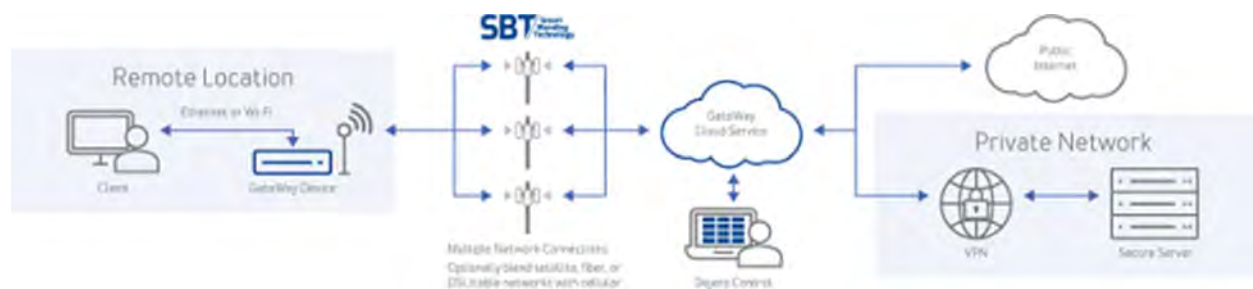
Solution elements

The Titan solution includes the following elements:

- The Titan device, which features blended network capabilities and multiple Ethernet, cellular, GPS, and Wi-Fi connections.
- Dejero platform cloud components that transition blended traffic from the Titan device to the internet.



Tip: If you need to provide multiple mobile network access points, your Titan solution might include more than one Titan device.



What's included

The Titan device is the physical device that you install as part of the Titan solution. It comes with the following items:

- Titan Command device
- 1 DC power input connector
- 1 DIO connector

- 1 mounting bracket
- 6 M4 x 6mm screws
- QR code for Quick Start Guide
- Optional accessories (not included): AC/DC Power Supply, IP67 rated enclosure and IP54 rated case

To secure the Titan device to your installation location, use 4x M6 screws. These screws are not included with the device.

An external GPS antenna is also required if GPS location data is desired from the Titan device. GPS antenna is not included.

About WAN and LAN connections

The Titan device includes Ethernet ports for both WAN (Wide Area Network) and LAN (Local Area Network) connections.

WAN connections

Use the WAN Ethernet port for blended connections to the internet. This connection must have access to the public internet and the firewall must allow outgoing TCP/UDP network traffic (and their corresponding stateful responses).

You might connect to a WAN in one of the following ways:

- Hard-wired Ethernet connection to access the internet.
- Ethernet connection to a satellite modem that can access the internet.
- Ethernet connection to a Wi-Fi device that can connect to a local access point with an internet connection.

LAN connections

Use the LAN Ethernet ports to connect devices to the Titan device.

You might connect to a LAN in one of the following ways:

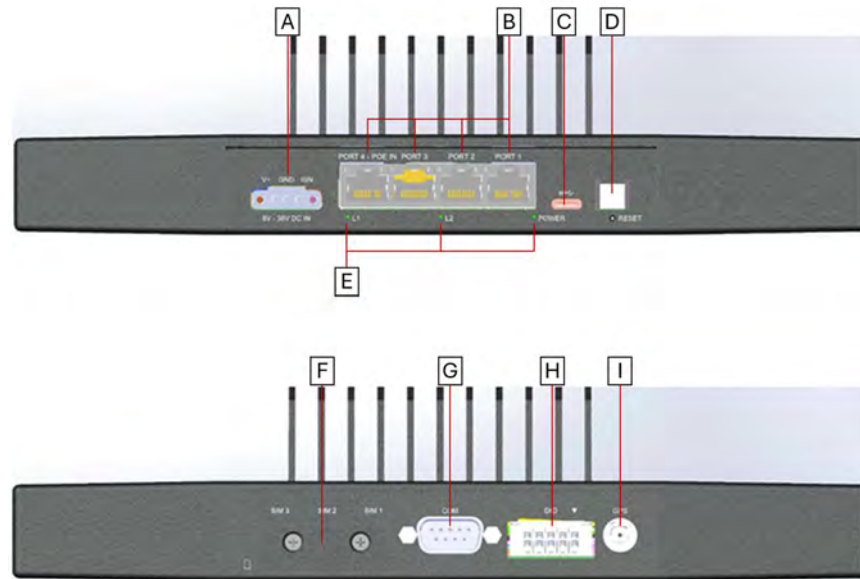
- Hard-wired Ethernet connection directly from a computer.
- Ethernet connection to a wireless access point that provides a hotspot for mobile devices.



Note: The Wi-Fi router that you connect to using a LAN connection is different than the Wi-Fi router inside the Titan.

I/O Overview

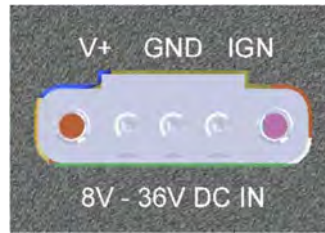
The Titan device provides the following I/O and access features:



Letter	Description	Letter	Description
A	DC Power Port with Optional IGN Input	F	SIM Cover
B	4 x RJ-45 2.5 Gigabit Ethernet 1, 2 and 3: WAN, 4: LAN/POE++	G	Serial (COM) port
C	USB-C Port	H	DIO Port
D	Power Button	I	GPS Antenna Port
E	3x LEDs L1, L2, Power		

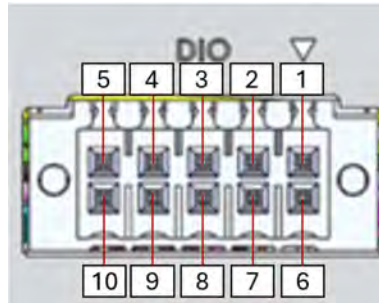
DC Power Port with Optional IGN Input

The power supply and remote switch port consists of three pins: V+, GND, and IGN. The DC power input allows a voltage input range from 8 to 36 VDC. IGN can optionally be used to switch Titan on and off with a vehicle ignition signal or remote power switch.



DIO Port

The DIO port consists of 10 pins. The DIO input voltage range is 8 – 36 VDC; the outputs are open-drain type.



Pin	Description
1	Wheel Tick (WT) Input for GPS ADR Mode
2, 7	GND
3, 4, 5	General Digital Input
6	Direction (DIR) Input for GPS ADR Mode
8, 9, 10	General Digital Output



Note: If the Titan is used in an IP67 enclosure supplied with M12 connectors, the DIO input and output voltage range on the DIO is limited to 8 – 30 V.

Setting up the Titan device

Before setting up the Titan device, choose a suitable location for the device as part of your solution.

As part of planning where to position the device, ensure that there is sufficient access for the GPS antenna and cables that connect to the back of the Titan device. If installed, you must position the GPS antenna correctly for optimal network connectivity. The antenna cable cannot make sharp bends and should not be crimped, so position the antenna carefully to avoid doing so.

You should also ensure that the placement of the Titan device and its integrated antennas provides the best possible cellular network signal reception. In some cases, you might need to position the device closer to the outside of a building or structure.

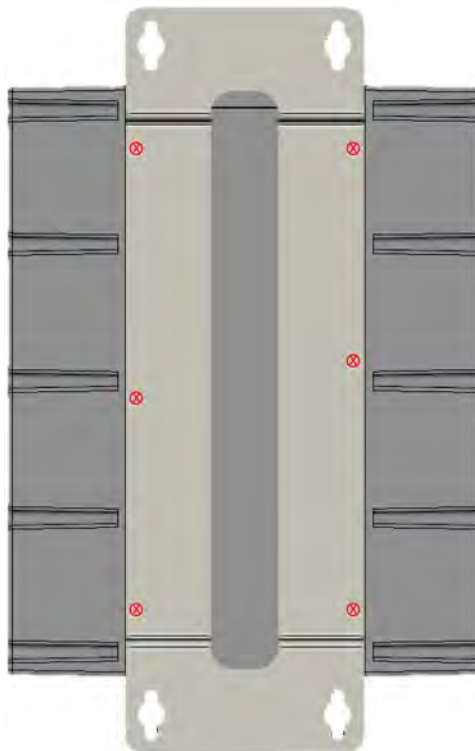
GPS Antenna installation notes

When connecting the GPS antenna to the Titan device, follow the instructions on the GPS antenna label. Always follow the manufacturer's instructions for information on installing the antenna. Both active and passive GPS antennas are supported.

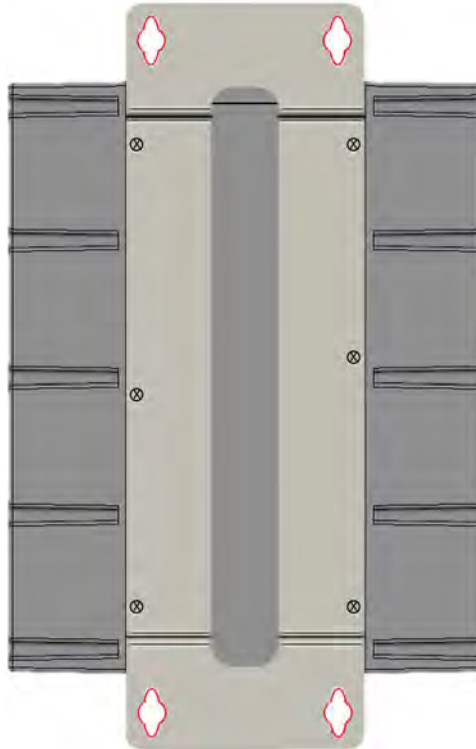
The Titan device supports Untethered Dead Reckoning (UDR) and Automotive Dead Reckoning (ADR) which combine inertial sensor data or wheel speed pulses with satellite position data, giving the best possible positioning accuracy in urban or tunnel environments. For best UDR performance, the GPS antenna should be located near to the Titan device's position in the vehicle. For best ADR performance, the Titan and GPS antenna should both be located near the wheel supplying speed pulses.

Mount the Titan device

1. Align the mounting bracket on the bottom of the device with the installation location.
2. Using the supplied six M4 x 6mm screws, attach the bracket to the base of the Titan device.



3. Secure the bracket to the installation location with four M6 screws through the keyhole openings.



4. Tighten all screws.

Connecting the Titan device

After installing the Titan device, you must set it up.

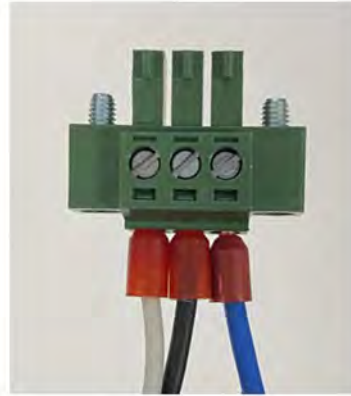
1. Screw the GPS antenna to the SMA connector on the back of the Titan device. Take care to tighten the SMA connector of the RF cable, not the hex lock nut on the chassis.
2. Connect your power source to the DC Power Input Connector. Insert the wires into the mating power connector as shown and tighten the clamping screws firmly onto the conductors.
 - Pin 1 (left): V+
 - Pin 2 (middle): GND
 - Pin 3 (right): IGN (optional)



Note: The IGN input is only required when powering the Titan on or off via vehicle ignition signal or a remote power switch.



Basic Power Wiring
(V+ and GND only)

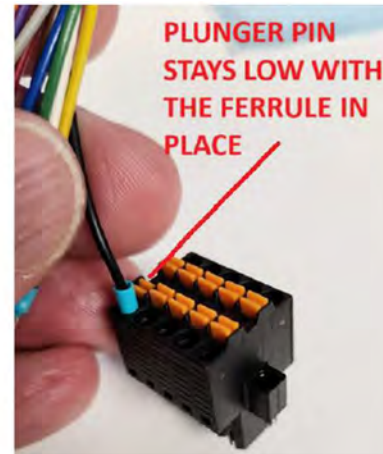


With Optional IGN Input



Note: Confirm your wiring. Wire colors may vary.

3. For vehicle installations, verify that your power source and fuses are adequate to meet the maximum power specifications. Dejero recommends a 10A fuse for V+ (from the vehicle battery) and a 1A fuse for the IGN signal.
4. Plug the power connector into the front of the Titan device or attach the POE++ enabled ethernet cable to Ethernet Port 4 on the left-hand side of the Ethernet ports.
5. If used, tighten the DC Power Input Connector screws with a flat head screwdriver to secure the connection to the Titan device. Take care to not over tighten.
6. Plug the power cable into a power source.
7. If necessary, perform the following actions:
 - To connect to a WAN, connect an Ethernet cable to Port 1, 2, or 3 on the front of the Titan device. Add a label to indicate that the cable is for the WAN connection.
 - To connect to a LAN, connect an Ethernet cable to the Ethernet 4 port on the front of the Titan device. Add a label to indicate that the cable is for the LAN connection.
 - If you want to configure the device using the Titan User Interface and you want to use a monitor with this tool, connect a monitor, keyboard and mouse to the USB-C port on the front of the device with a USB-C adapter. If the unit is operating, a reboot may be required to recognize the USB adapter.
 - To use the DIO, insert a wire (with ferrule) into the mating connector using a small flat-blade screwdriver to depress the orange plunger. Note that the plunger spring is strong and requires some force. Depressing the plunger opens the contacts and allows the wire to be inserted. Hold the wire in place and release the orange plunger to lock it in position. Note that the plunger will remain "low" with the wire in place. To release a wire, use a small flat-blade screwdriver to depress the orange plunger, then pull the wire out.



Note: Ferrules should always be installed on any wiring before inserting into the DIO connector.

Using the Titan device

Upon applying power, the Titan device turns on automatically and runs through the startup process and establishes its connections.

- To power on the device, press and hold the Power Button for a minimum of 2 seconds
- To power off the device, press and hold the Power Button for a minimum of 2 seconds
- To reboot the device, press and hold the Power Button for a minimum of 10 seconds

When controlled by the optional IGN input, Titan has a default auto-on delay of 5 seconds and a default power-off delay of 30 minutes.



Insert SIM cards

To take advantage of the integrated cellular modems, you need to insert SIM cards into the Titan device.

1. Power off the Titan device using the power button on the front of the Titan device.
2. On the back of the Titan device, remove the SIM card cover.



Note: The SIM card cover end is a tool to insert and remove the SIM cards.



Note: Use industrial-grade nano SIMs to ensure reliable operation within the device's operating temperature range.

3. Insert nano SIM cards into the slots.
4. Reattach the SIM card cover.
5. Reconnect the power connector to the front of the Titan device.

Connecting Titan with other devices

After you set up Titan, connect other devices to it to access the Internet or your private network.

You can also configure the Titan device as a Wi-Fi access point to allow your laptop, tablet, or smartphone to connect to the Internet. Alternatively, you can connect other Wi-Fi routers or a network switch to the LAN port and then connect your devices to the network provided by the router or switch.

Configuring Titan with Control

To configure a Titan device using Control, you must be an administrator with the appropriate permissions. For more information on using Control, visit support.dejero.com to read the *Dejero Control User Guide*.

Log in to Control

Prerequisite: Verify that you have login information, sent to you in an email from Dejero. Create a password for the site.

1. In a browser, type control.dejero.com.
2. Type your email address.
3. Type your password.
4. Click **Sign in**.

Configure a Titan device

1. In Control, click **Manage** > GateWay.

2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, serial number, status, station name, or software version.
3. Click a device name.
4. On the right side of the screen, click .
5. Click  **CONFIGURE GATEWAY**.
6. On the **Configure Titan** screen, if necessary, change the name of the device.
7. If you want to use one or more of the WAN Ethernet connections, in the **WAN Port** section, perform one of the following actions:
 - To blend the Ethernet connection using DHCP, select **Using DHCP**.
 - To set the IP address manually, select **Manually**. Set the **IP Address**, **Network Prefix Length**, **Default Titan**, **Primary DNS**, and **Secondary DNS** fields.
8. Click .

Configure the Titan device as a Wi-Fi access point

You can configure the Titan device as a Wi-Fi access point to hotspot to the Internet. The Titan device has one Wi-Fi access point, which can support 2.4 GHz, 5.0 GHz or 6.0GHz (802.11 a/b/g/n/ac/ax) network configurations.

By default, when you enable the device as a hotspot, the device broadcasts the hotspot so other users can access it.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. On the right side of the screen, click  **CONFIGURE GATEWAY**.
5. On the **Configure Titan** screen, in the **Wi-Fi Hotspot** section, click **ON**.
6. Perform one or more of the following actions:
 - Change the name for the access point.
 - If you do not want to broadcast the hotspot, click **NO**.
 - Select the type of security for the access point.

- Set the access point password.
- Set the radio mode to **2.4 GHz**, **5.0 GHz** or **6.0GHz**.

7. Using WPA3 Enterprise as a security type

- Support has been added to all Titan models for WPA3 Enterprise security. When configuring a Wi-Fi Hotspot with this security type the user will need to input the IP address, port, and shared secret of the RADIUS server. The user will need to be able to provide these details.
- The Titan Command also supports WPA3 Enterprise 192 bit encryption as an option.

Configure GateWay

☐ WPA

☐ WPA2 Personal

☐ WPA3 Personal (Recommended)

☐ WPA3 Enterprise

☒ WPA3 Enterprise 192 bit

Authentication Server Address*

1.2.3.4

Authentication Server Port*

1812

Authentication Server Shared Secret*

password

Radio Mode

☒ 2.4 GHz (802.11 b/g/n)

☐ 5.0 GHz (802.11 a/n/ac)

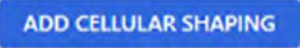
8. Click .

Configure cellular data shaping

If you want to manage your cellular data costs, you can configure cellular data shaping for your Titan device. When cellular data shaping is turned on, Control monitors the amount of data transmitted during the billing period. If the amount of data transmitted reaches a specified threshold, the device starts transferring at the defined lower shaped speed. On the first day of the next calendar month, the data transfer speed returns to normal.



Note: Cellular data shaping applies when the device meets the threshold for cellular data transfers only. Any data transferred over the WAN Ethernet connection is not shaped.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. In the **Cellular Shaping** section, click .
5. Perform the following actions:
 - In the **Threshold** field, set the data usage level that the device must reach before starting to shape the transfer speed.
 - In the **Shaping Speed** field, set the data transfer speed that the device uses after it reaches the threshold. The speed cannot be lower than 128 kb/s.
6. Click .

If you configure shaping, Control updates the **Cellular Usage This Month** graph that appears on the **Usage** tab. A red line appears to indicate the threshold that you specified. On the Titan device, **Cellular Shaping Active** appears on the Main screen.

Change the cellular data shaping configuration

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.

3. Click a device name.
4. In the **Cellular Shaping** section, click .
5. Change the **Threshold** and **Shaping Speed** fields.
6. Click .

Remove cellular data shaping

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click . Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. In the **Cellular Shaping** section, click .
5. Click **REMOVE CELLULAR SHAPING**.

Configure connection priority

If you have additional WAN connections to transmit data (beyond the embedded cellular modems), you can set the usage priority for each connection. The Titan device uses the primary connections as long as it can maintain a specified upload and download speed. If it can't maintain that speed, it starts using all of the connections set with a secondary priority.

In addition to setting the priority for the WAN connections connected to the device, you can also set the priority for the cellular modems embedded in the device.

You might want to configure this feature to control costs, using the more expensive connection types only when necessary to maintain the desired performance.



Note: You must set a priority for any ports that are available, even if there isn't a connection to that port. If a port is available but you are unsure of the connection or its priority, configure the port with secondary priority.

If you assign the same priority to more than one connection, the connections form a pool. They work together to maintain the desired performance speed.



Note: Because the device might need to start using a connection if the data transfer rates fall below the desired level, the device must keep all connections open. To do that, a small amount of data is sent over every connection.



Note: If you need any help configuring connection priority, contact Dejero Support.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Connection Priority** tab.
5. Click **Set Up**.
6. Select the priority for each connection.
7. If necessary, for any of the ports, add a friendly name for the port.
8. In the **Activation Threshold** section, set the download and upload speeds that you want the primary connections to maintain before using secondary connections.
9. Click .



Note: If you want to configure connection priority, but don't want to enable it right away, clear the **Apply settings automatically** check box. Click **Save**. Control saves the configuration but does not enable it on the Titan. To start using connection priority, on the **Connection Priority** tab, click the toggle into the **On** position.

Change connection priority settings

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Connection Priority** tab.
5. Click .
6. Perform one or more of the following actions:
 - Add, change, or remove the friendly name for each port.

- Select a different priority for a connection.
- Change the upload or download speed for primary or primary and secondary connections.

7. Click .

Turn off connection priority

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Connection Priority** tab.
5. Click .

Configure port forwarding

To set up port forwarding, you must have a static IP address configured for your Titan device. For more information, contact Dejero Support.



Note: Port forwarding configuration requires GateWay Edit permissions in Dejero Control. This feature will only be visible to those users with that permission level.

Forwarding options

Setting	Description
Port Forwarding	Use this option to enable inbound communication from the internet to multiple Redirect IP addresses on configured ports. Traffic from Redirect IP addresses use the static public IP address.
1:1 NAT	Use this option to enable inbound communication from the internet to a single Redirect IP address. Traffic from the Redirect IP address uses the static public IP address. All other clients use the ephemeral IP address.

Disabled	Use this option to turn off 1:1 NAT and port forwarding. All traffic appears from the static IP address.
----------	--

Enable port forwarding

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Routing** tab.
5. In the upper-right corner of the tab, click .
6. In the **Forwarding Mode** drop-down list, select **Port Forwarding**.
7. Perform the following actions:
 - a. In the **Protocol** drop-down list, select the transfer protocol to use.
 - b. Set the **Redirect IP** field.
 - c. Specify the **Port Range** and the **Redirect Port Range** fields. The difference specified in each range must be the same. For example, if you set the **Port Range** fields to **5001** and **5006** (a difference of 6 ports), you must specify a difference of 6 ports for the **Redirect Port Range** field (such as 6001 and 6006).
8. To add another forwarding rule, click . Repeat step 7 to configure any additional rules.
9. Click .

Remove a port forwarding rule

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Routing** tab.
5. In the upper-right corner of the tab, click .

6. Beside the rule that you want to remove, click  **REMOVE**.
7. Click .



Note: If you remove all port forwarding rules, **Save** changes to **Save & Disable**. When you click **Save & Disable**, port forwarding is turned off.

Enable 1:1 NAT forwarding

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Routing** tab.
5. In the upper-right corner of the tab, click .
6. In the **Forwarding Mode** drop-down list, select **1:1 NAT**.
7. Set the **Redirect IP** field.
8. Click .

Turn off forwarding

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Routing** tab.
5. In the upper-right corner of the tab, click .
6. In the **Forwarding Mode** drop-down list, select **Disabled**.
7. Click .

Configure DHCP and reserved static IP settings



Note: These network settings are advanced. You must ensure that any modifications to values do not cause any network conflicts that could result in devices becoming unavailable. Please contact Dejero Support to enable. If using Routed Mode on the Titan, the DHCP settings are available in the Titan Web UI configuration screen.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Routing** tab.
5. In the upper-right corner of the tab, click .
6. In the **DHCP Settings** section, set the network, Titan, and DNS fields.
7. If necessary, perform one of the following actions:
 - To add a reserved IP, Click . Set the **Static Address**, **Static MAC**, and **Static Hostname** fields.
 - To change a reserved IP, change the **Static Address**, **Static MAC**, or **Static Hostname** fields.
 - To remove a reserved IP, for the reserved IP you want to delete, click .
8. Click .

Add tags to Titan devices

You can add tags to Titan devices to make searching easier. Tags can be added on the Manage > GateWay page or on the Information tab for a Titan device. Tags must not be more than 45 characters long.



Note: To add tags, you must have permissions to manage devices and your home station must have an enhanced license.

Add tags to Titan devices on the Manage > GateWay page

1. Click **Manage** > GateWay.
2. Perform one or more of the following actions:

- Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Select the check box for one or more Titan devices.
 4. Click  **Tags**.
 5. In the list, perform one of the following actions:
 - Type the name of the tag.
 - If you want to use a tag that was added to the device's station by another user, start typing the name of the tag. Select the tag.
 6. Click .

Add tags to a Titan device on its Information tab

1. Click **Manage > GateWay**.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click the Titan device.
4. Click the **Information** tab.
5. Click .
6. In the **Tags** field, perform one of the following actions:
 - Type the name of the tag.
 - If you want to use a tag that was added to the device's station by another user, start typing the name of the tag. Select the tag.
7. Click .

Managing device profiles

Device profiles allow you to store a collection of configuration settings that can be applied to other devices with the same model type and software version. You can apply a device profile to multiple devices at one time.

Any device configuration changes that are applied via device profiles are captured as Titan Configuration entries in the Device Activity Log in Dejero Control. If a device profile is applied to

more than one device, the additional details for the entry includes a list of the devices that the profile was applied to.



Note: Device profiles require Titan software version 3.4.0 or later.

Create a device profile

When you export the configuration settings of an existing Titan Device to create a device profile, you can choose the types of settings to export.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. On the right side of the screen, click .
5. Click  **EXPORT SETTINGS**.
6. Type a name for the device profile.
7. If necessary, type a description for the device profile.
8. Select the settings to include in the exported device profile.
9. Click .

The created device profile is stored in Control and can be viewed on the **Manage > Device Profiles** page.

Device profile export options

When exporting settings to create a device profile, you can include on-device settings (configured using the local user interface or Titan Web UI) and settings configured via Dejero Control.

Configured: On-device	
Group	Settings
Blending	Interfaces included in blending (Titan Web UI)

Configured: On-device

	Flow rules (Titan Web UI)
Network	IP configuration of WAN interfaces (Titan Web UI) Connection priority local override (Titan Web UI) Interface friendly names NTP servers Wi-Fi country and channel
Routers	Router configuration (Titan Web UI) Bridged vs Routed mode (Titan Web UI)

Configured: Via Dejero Control

Group	Settings
Interface and Connection Priority Configurations	Interface configuration, including WAN/LAN setting, IP address source (DHCP / Static IP), and DNS addresses Connection priority group assignment Connection priority threshold definition
Connection Priority Enabled Status	Status of the Connection Priority Enabled setting
Hotspot	Hotspot configuration, including SSID, passphrase, authentication type, and Wi-Fi band

Apply a device profile

You can apply a device profile to one or more devices that are similar (same hardware type and software version) to the device that was used to create the device profile.



Note: Unique settings, such as the Hotspot SSID and passphrase may not apply to all selected devices. By default, a generated SSID or passphrase is applied instead; however, you may choose to use the settings in the profile instead, although this is a potential security risk across multiple devices and is not recommended.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Select the check box for one or more Titan devices.
4. Click  **Profiles**.
5. Select the device profile to apply.
6. Review the profile details to confirm it contains the settings you want to apply and to confirm that all selected devices support the profile.
7. If the profile contains values, such as the Wi-Fi Hotspot Network SSID or Hotspot passphrase, that may not apply, review the settings and select the appropriate option.
8. Click .
9. If necessary, to avoid networking conflicts, adjust any settings, such as the Wi-Fi Hotspot Network SSID or Hotspot passphrase, that should have unique values. For more information, see "Configure the Titan device as a Wi-Fi access point" on page .

Before deploying the devices, verify the updated device settings using the device activity log or by checking the individual settings sections in Dejero Control, the Titan Web UI, or the Titan local user interface.

View saved device profiles

You can view the saved device profiles, including the associated product model, software version, and settings.

1. In Control, click **Manage** > **Device Profiles**.
2. To review the settings included in the device profile, click on the name of the profile.

Delete a saved device profile

You can view the saved device profiles, including the associated product model, software version, and settings.

1. In Control, click **Manage** > **Device Profiles**.
2. For the device profile you want to delete, click  **DELETE**.

Using the Titan Web User Interface

The Titan Web User Interface (UI) allows a user to view realtime connection metrics and manage local configurations for the device

Remotely access the Titan Web User Interface

You can remotely access the Titan Web User Interface (UI) as if you were connected directly to the device. The Titan Web UI includes performance details, network interface status, and additional Titan configuration settings, including flow rules, connection priority and Titan mode (bridged or routed).

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click . Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. On the right side of the screen, click .
5. Click  **REMOTE ACCESS**.
6. Click .

About the Titan Web UI screen

The Titan Web UI screen contains several sections:

- The header displays the Titan Serial Number and the Dejerian OS version.
- The **Overview** section provides the throughput for each known connection and the blended connection. It also displays the latency and connections status for each known connection.
- The **Individual Connections** section displays the throughput and latency metrics for each of the known connections.



Navigate the Titan Web UI

- Use the icons at the bottom right of each graph to pan left, reset a chart, pan right, zoom in, and zoom out.

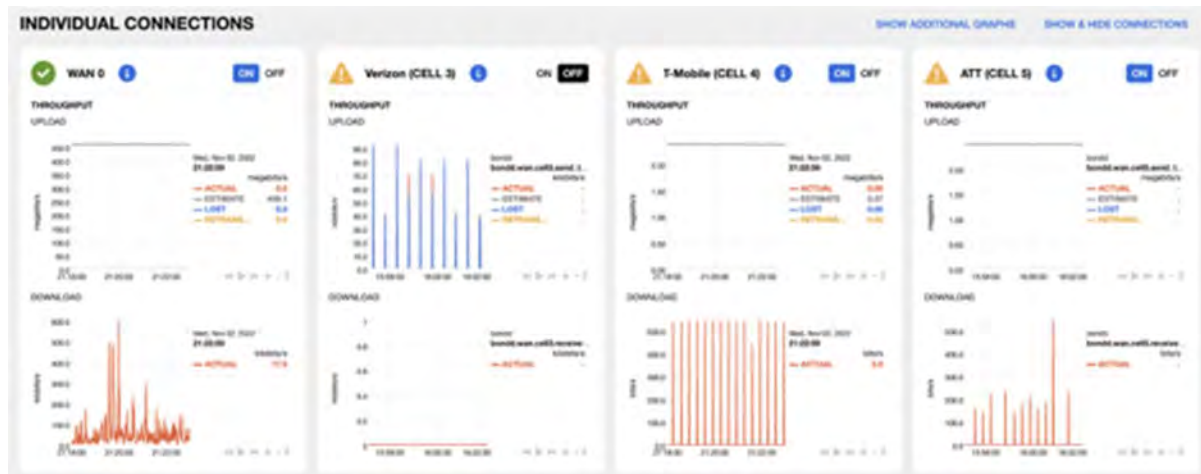


- To pan left or right using your mouse, click on the graph and drag it left and right.
- To zoom in or out using your mouse, click on the graph and hold the Shift key while scrolling the mouse wheel up or down.
- To zoom in on a specific section, hold the Shift key and click on the area, and drag until the area to view is highlighted.
- To reset a chart, double click on an area inside the chart.

View information about individual connections

The Individual Connections section displays the Throughput graphs. Each graph is interactive.

- To display the Latency graph for each connection, click **Show Additional Graphs**.
- To filter a graph to show only specific information, click the item in the legend.

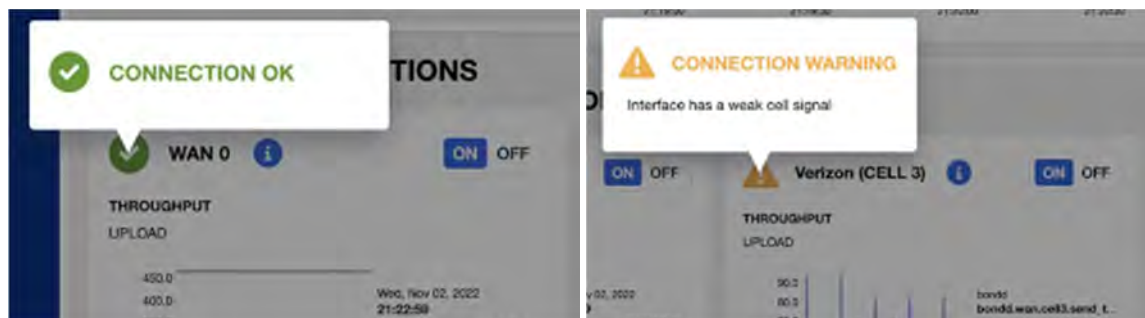


About connection status icons

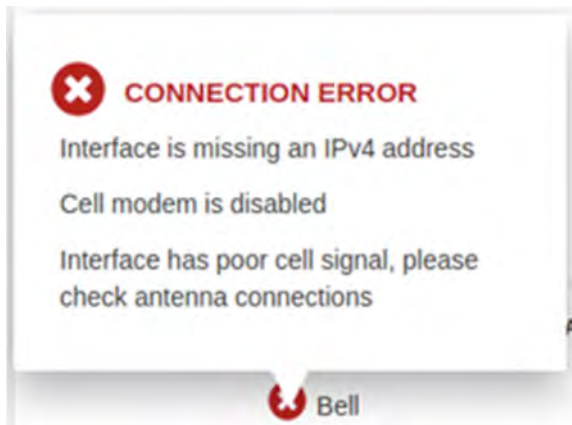
The connection status icons show the connection state and appear as a red, yellow, or green icon.

To see more information about the state, click on the icon. You may see different information, depending on the connection type.

For example, the wan0 connection has a green status icon and the additional information indicates the interface and connection are good. The yellow cellular connection indicates a poor cell signal.



If the connection was dropped or the modem was disabled, the additional information may include details to help troubleshoot the connection state.



For Ethernet connections, a green status indicates the connection is connected and has an IPv4 address.



The connection shows an ERROR status if any of the following conditions are met:

- One or more IPv4 fields are not populated
- The Ethernet link state is DOWN
- The cellular modem is disabled, powered off, has no carrier, or is in emergency mode
- The Received Signal Strength Indicator (RSSI), Received Signal Code Power (RSCP), or Reference Signals Received Power (RSRP) measurements on the main cellular antenna are in “poor” or worse state, or the diversity strength is more than one quality bucket a part

For more information about the quality bucket definitions, visit the following pages:

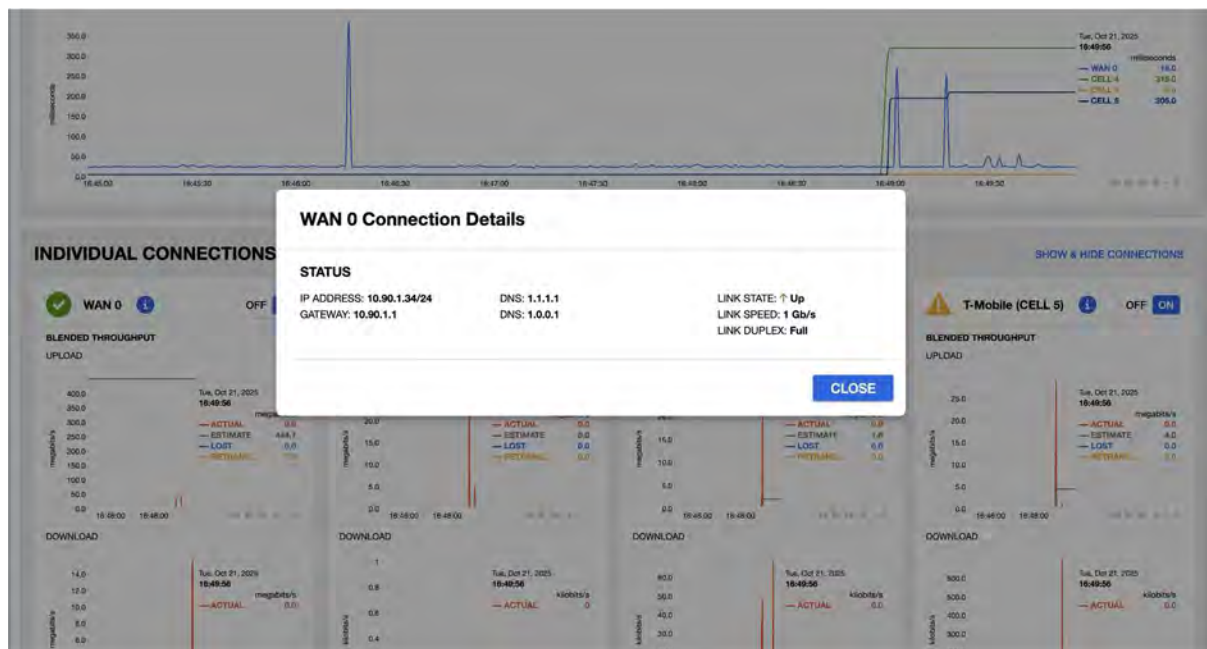
<https://wiki.teltonika-networks.com/view/RSSI>

[https://wiki.teltonika-networks.com/view/RSRP and RSRQ](https://wiki.teltonika-networks.com/view/RSRP_and_RSRQ)

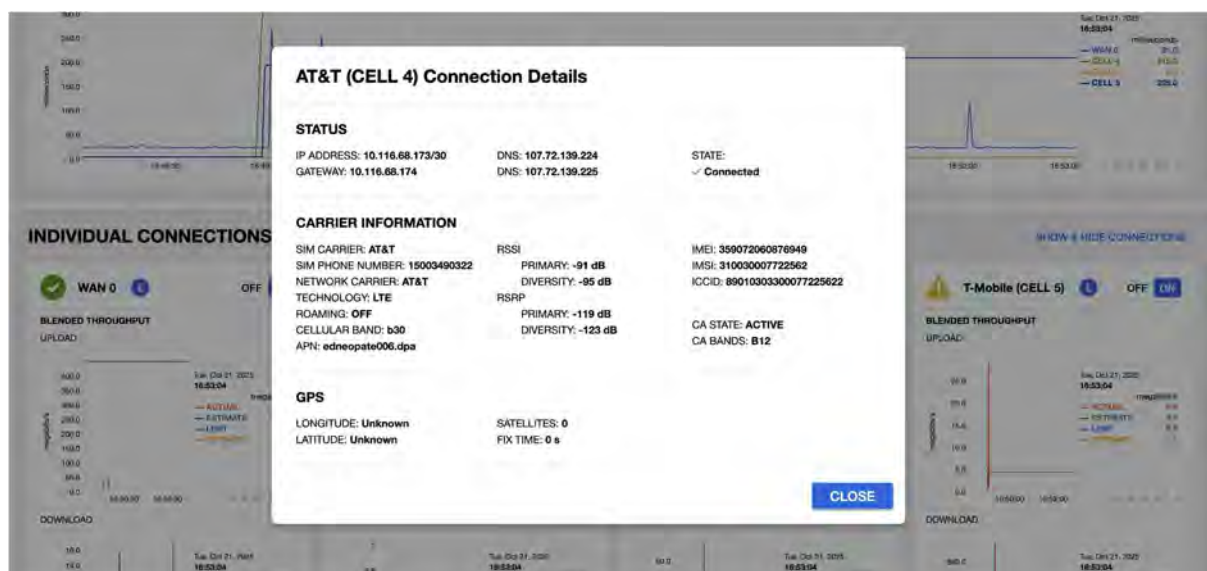
<https://wiki.teltonika-networks.com/view/RSCP>

About the information icon

To see the detailed status of each connection, click the information icon to the right of the connection name.



For cellular connections, the detailed information includes the carrier details and current signal metrics.



Change which connections are included in the Blended throughput pool

In upper right corner of each connection column is an option to set whether the connection is included in the pool of connections shown in the Blended Throughput graph.

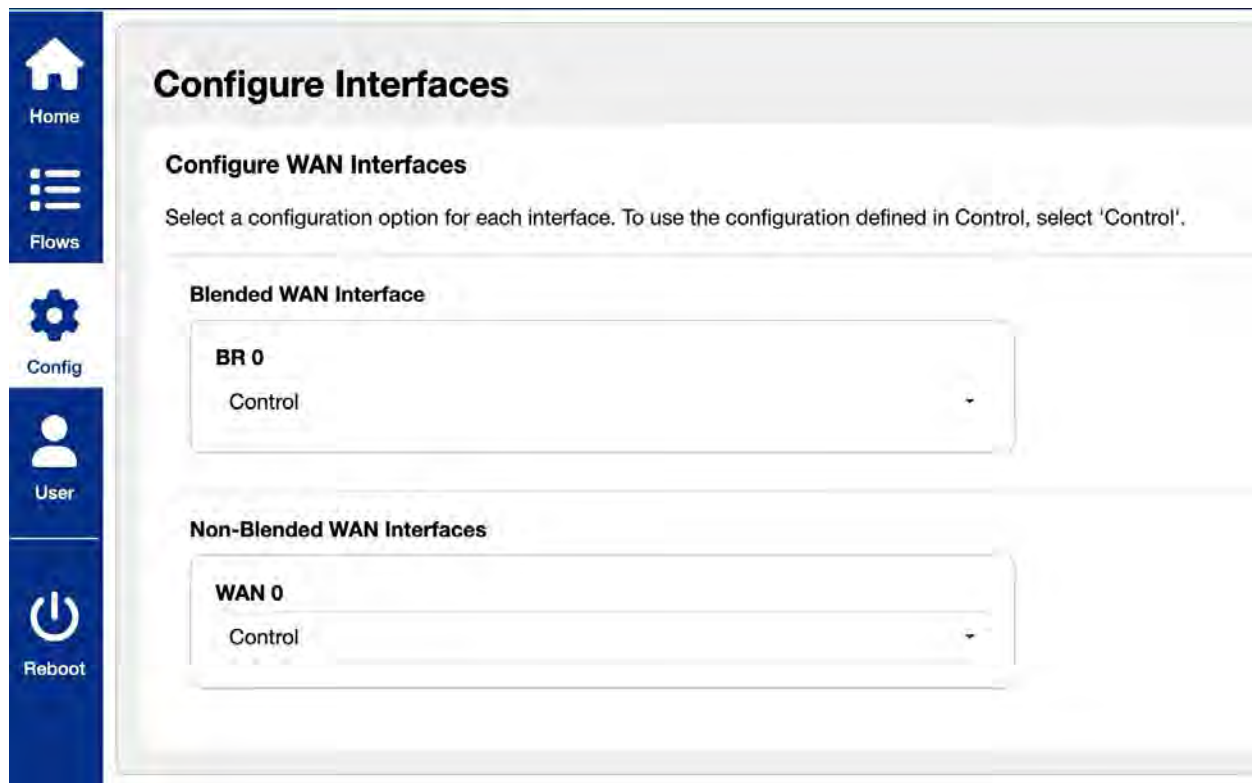


Note: Changing the toggle does not affect the connected state of any of the connections.

1. To change whether a connection is included in the blending pool, perform one of the following actions:
 - To include the connection in the blending pool, set the option to **ON**.
 - To exclude the connection from the blending pool, set the option to **OFF**.

Configuring Interfaces

Using the Titan Web UI you can configure options for each interface.



These configuration options are alternatively available in Dejero Control.

Configure the management interface

1. In the Titan Web UI, navigate to **Config > Interfaces**.
2. Select **br0**.
3. Perform one of the following options:
 - To use the settings in Control, navigate in the drop down list to **Control**.
 - To override the setting in Control and use DHCP, navigate in the drop down list to **DHCP**.

- To override the setting in Control and use a static IP, navigate to **Static IP**. Set the **IP**, **Netmask and DNS** fields.

4. Click 

5. Restart the Titan device.

Configure the WAN interface

4. In the Titan Web UI, navigate to **Config > Interfaces**.

5. Select **WAN (x)** that want to configure.

6. Perform one of the following options:

- To use the settings in Control, navigate in the drop down list to **Control**.
- To override the setting in Control and use DHCP, navigate in the drop down list to **DHCP**.
- To override the setting in Control and use a static IP, navigate to **Static IP**. Set the **IP**, **Netmask and DNS** fields.

6. Click 

7. Restart the Titan device.

Using routed mode and multi-WAN routing

Within the Titan Web UI you can configure multiple routers, each with its own subnet and independent configuration.



Note: A router must have at least one LAN interface assigned to it, and each LAN interface can be used by only one router.

LAN and WAN settings are configured independently for each router. LAN settings control the configuration that is pushed to the client connected to this router. WAN settings control how the router provides connectivity. You can configure multiple WAN interfaces for each router. For example, you might want to configure a router to send traffic using multiple WAN interfaces to ensure there is a backup if one interface loses connectivity.

Manage routers

1. In the Titan Web UI, navigate to **Config > Routers**.

2. Click 

3. Perform one of the following actions:
 - To add a new router, click . Type a name and description for the router.
 - To change the settings for an existing router, click .
4. Configure the LAN and WAN settings for the routers.
5. Click  or .

Manage LAN settings for a router

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **LAN Settings** section, perform the following actions:
 - In the **Router Address** field, type the default Titan of the router.
 - If necessary, in the **Prefix Length** field, change the length of the DHCP subnet.
 - In the **Management Address** field, type the address used to access the Titan Web UI.
 - If necessary, in the **Management Hostname** field, change the user-friendly name used to access the Titan Web UI.
5. In the **LAN Interfaces** sub-section, select which interfaces will be part of this router. A router must have at least one LAN interface, but LAN interfaces cannot be shared across different routers.

Configure DHCP settings for a router

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **WAN Settings** section, set the **DHCP Settings** option to **ON**.
5. Perform the following actions:
 - Set the start and end points of the subnet of the router. The range of the subnet cannot be greater than the value of the **Prefix Length** field. Do not include the default Titan and management address IP in the DHCP range.
 - Set the lease time for the IP address.
6. If necessary, set up one or more custom DHCP options to push to the client when the DHCP lease is negotiated.

7. If necessary, set up one or more IP reservations.
8. Click .

Enable firewall rules for a router

When you add firewall rules for a router, traffic is matched to rules as defined in the modal starting from top to bottom. For example, if a rule defines a DROP action for a certain 3 or 5 tuple, and a later rule defines an ACCEPT action, the rule specifying the DROP action is applied before the rule specifying the ACCEPT action for the same traffic.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **LAN Settings** section, set the **Firewall Rules** option to **ON**.
5. Click .
6. Perform the following actions:
 - a. In the **Action** drop-down list, select the action to apply.
 - b. In the **Protocol** drop-down list, select the transfer protocol to use.
 - c. In the **Source IP Addresses** field, add one or more IP addresses.
 - d. In the **Destination IP Addresses** field, add one or more IP addresses.
 - e. In the **Source Port Ranges** field, add on or more ports or port range.
 - f. In the **Destination Port Ranges** field, add on or more ports or port range.
 - g. In the **Source MAC Addresses** level filtering, add one or more MAC addresses.
 - h. In the **Destination MAC Addresses** level filtering, add one or more MAC addresses.



Note: Destination MAC filtering is an advanced feature, please use with caution or contact Dejero support with questions.

7. To add another firewall rule, repeat steps 5 and 6.
8. To set the order of rules, use the arrows.
9. Click .

Remove a firewall rule from router

1. In the Titan Web UI, navigate to **Config > Routers**.

2. Click .
3. For the router you want to manage settings for, click .
4. In the **Firewall Rules** sub-section of the **LAN Settings** section, beside the rule that you want to remove, click .
5. Click .

Enable Static Routing for a router

You can add static routes to support IP subnets that are reachable via the Titan LAN but are not directly connected.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **LAN Settings** section, set the **Static Routes** option to **ON**.
5. Click .
6. Perform the following actions:
 - a. In the **Description** field, enter a text description of the new route.
 - b. Set the **Destination Address** field. This can be a single host or a network address.
 - c. In the **Prefix Length** drop-down list, set the appropriate prefix length.
 - d. Set the **Titan Address** field. This is the default IP Titan behind which the Destination Address or Subnet can be reached.
7. To add another forwarding rule, repeat steps 5 and 6.

Configure DNS Forwarding settings for a router

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **WAN Settings** section, set the **DNS** option to **ON**.
5. Perform the following actions:
 - Configure one or more Nameservers by entering the IP address of each server

6. Click .

Manage WAN settings for a router

You can configure each router to use one or more WAN interfaces. To configure a router to provide connectivity over a non-blended connection, configure the WAN interface that is not br0. To configure a router to provide blended connectivity, configure br0 as the WAN interface.

For configurations using a non-blended connection with a static IP address, you can set up port forwarding or 1:1 NAT. Typically, you would configure 1:1 NAT for wired WAN interfaces only as carriers already configure this for cell interfaces.

For both blended and non-blended connections, you can configure policy rules to steer traffic matching the specific criteria to follow the blended or non-blended paths, and you can also configure failover and monitoring capabilities independently for each WAN interface.

If you select more than one WAN interface, set up a health monitor for each interface that you select to help the Titan determine the priority of each connection when sending traffic.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **WAN Settings** section, select one or more WAN interfaces to use to provide connectivity to the LAN devices. For blended connectivity, choose the **br0** interface. For non-blended connectivity choose another interface.
5. Click .

Enable Port Forwarding for a WAN interface

If you have configured a router to provide connectivity over a non-blended connection, you can configure port forwarding rules for that connection.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **DNAT** sub-section of the **WAN Settings** section, in the **Forwarding Mode** drop-down list, select **Port Forwarding**.
5. Click .
6. Perform the following actions:
 - a. In the **Protocol** drop-down list, select the transfer protocol to use.
 - b. Set the **Redirect IP** field.

- c. Specify the **Port Range** and the **Redirect Port Range** fields. The difference specified in each range must be the same. For example, if you set the **Port Range** fields to **5001** and **5006** (a difference of 6 ports), you must specify a difference of 6 ports for the **Redirect Port Range** field (such as 6001 and 6006).
7. To add another forwarding rule, repeat steps 5 and 6.
8. Click .

Remove a port forwarding rule from a WAN interface

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **DNAT** sub-section of the **WAN Settings** section, beside the rule that you want to remove, click .
5. Click .

Enable 1:1 NAT forwarding

If you have configured a router to provide connectivity over a non-blended connection, you can configure 1:1 NAT rules for that connection.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **DNAT** sub-section of the **WAN Settings** section, in the **Forwarding Mode** drop-down list, select **1:1 NAT**.
5. Set the **Redirect IP** field.
6. Click .

Turn off forwarding for a WAN interface

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **DNAT** sub-section of the **WAN Settings** section, in the **Forwarding Mode** drop-down list, select **Disabled**.

5. Click .

Enable health monitors for a WAN interface

You can configure one or more health monitors for each WAN interface. Health monitors detect the current state of the interface and are used to determine whether the interface is considered to be a reliable connection.



Tip: Take care when setting the interval. An unnecessarily high interval value will limit how quickly the Titan can detect when a connection transitions between being reliable and unreliable. Ensure that you also consider the latency of the connection type. For example, for fixed line and cell connections, a 200 ms interval may be reasonable. However, a satellite connection with 600 ms RTT will never be considered reliable with an interval set to 200 ms.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **WAN Settings** section, set the **Monitoring** option to **ON**.
5. Click .
6. Perform the following actions:
 - a. In the **Destination IP Address** field, type one or more remote destination IP addresses that can be reached from the Titan IP address using Internet Control Message Protocol (ICMP).
 - b. In the **Interval** field, set how frequently you want the Titan to ping the remote address.
 - c. In the **Consecutive fails for down status** field, set how many pings lost to the destination IP that are required to declare the link un-reliable and trigger the failover condition.
 - d. In the **Consecutive successes for up status** field, set how many successful pings are required before the system deems the link to have returned to a reliable state and resumes normal operation.
7. To add another monitor, repeat steps 5 and 6.
8. Click .

Turn off a health monitor

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .

3. For the router you want to manage settings for, click .
4. In the **Monitoring** subsection of the **WAN Settings** section, for the monitor you want to turn off, set the **Enable Monitor** option to **OFF**.
5. Click .

Remove a health monitor from a WAN interface

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **Monitoring** subsection of the **WAN Settings** section, for the monitor that you want to remove, click .
5. Click .

Enable policy routing for a WAN interface

If you have configured a router with two or more WAN interfaces, you can configure one or more policies to evaluate traffic and apply a specific forwarding decision based on the matching criteria. For example, you may want to send critical information over the blended connection only. There is a default rule at the end of the sequence that will forward traffic over the blended connection.

Policies are evaluated and applied in the order they appear.

1. In the Titan Web UI, navigate to **Config > Routers**.
2. Click .
3. For the router you want to manage settings for, click .
4. In the **WAN Settings** section, in the **Routing** subsection, click .
5. In the **Description** field, type the description for the policy.
6. To set the matching criteria, perform one or more of the following actions:
 - In the **IP Protocol** drop-down list, select a protocol.
 - In the **DSCP** field, type a Differentiated Services Code Point (DSCP) value.
 - In the **Source IP** or **Destination IP** fields, type an IP address.
 - In the **Source Port Range** or **Destination Port Range** fields, specify a start or end port range.
7. In the **Route** list, set a metric for each interface. A lower metric indicates that interface is preferred over an interface with a higher number. For example, if both metrics are identical,

traffic will be sent over both connections. If one interface has a metric of 10 and another has a metric of 100, traffic is sent over the interface that has a metric of 10 even when both connections are reliable.

8. To add another policy, repeat steps 4 to 7.

9. Click .

Configuring the VPN Client

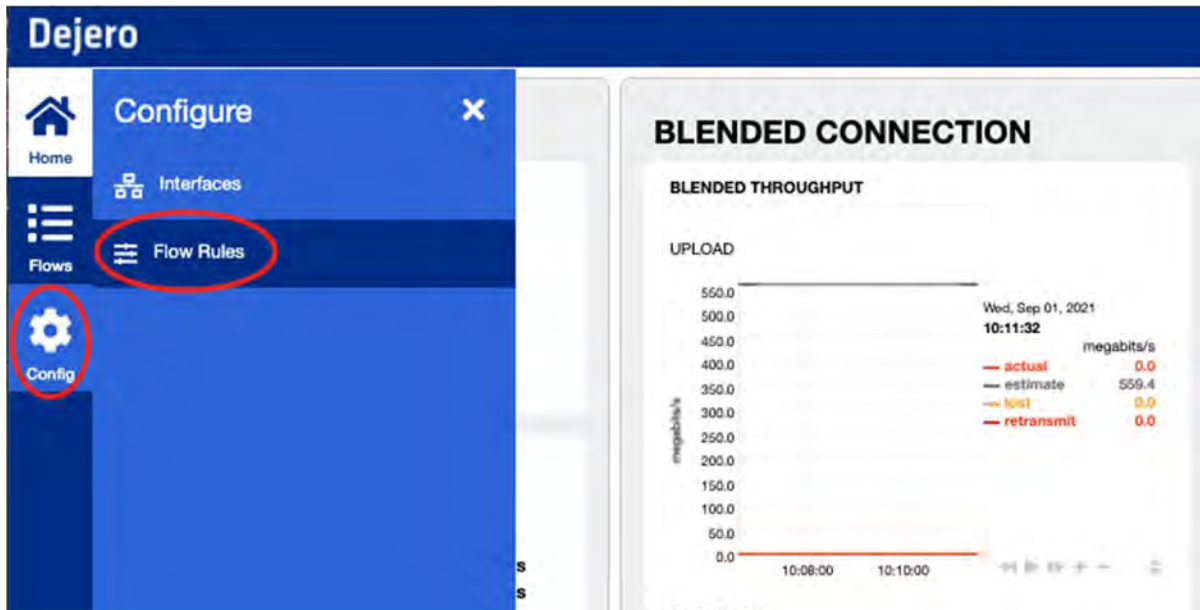
You can use the Titan to connect to a remote destination using an encrypted IPSec VPN.

1. In the Titan Web UI, navigate to **Config > VPN** .
2. Click .
3. In the **VPN Settings** section, click .
4. In the **Description** field, type a description for the VPN connection.
7. Configure the Remote Endpoint IP address
8. Configure the Remote ID from the remote VPN server
9. Configure local router configuration to which this VPN applies.
10. Configure a Local ID for this Titan
11. In the **Traffic Routing** section, specify destination subnets to route specific traffic over the VPN. Default is all traffic will be forwarded through the VPN.
12. **Configure the Mutual Pre-Shared Key**
13. **Advanced Setting allow the selection of NAT traversal mode. Default is On.**
14. To complete the VPN connection, click on the .
15. Click .

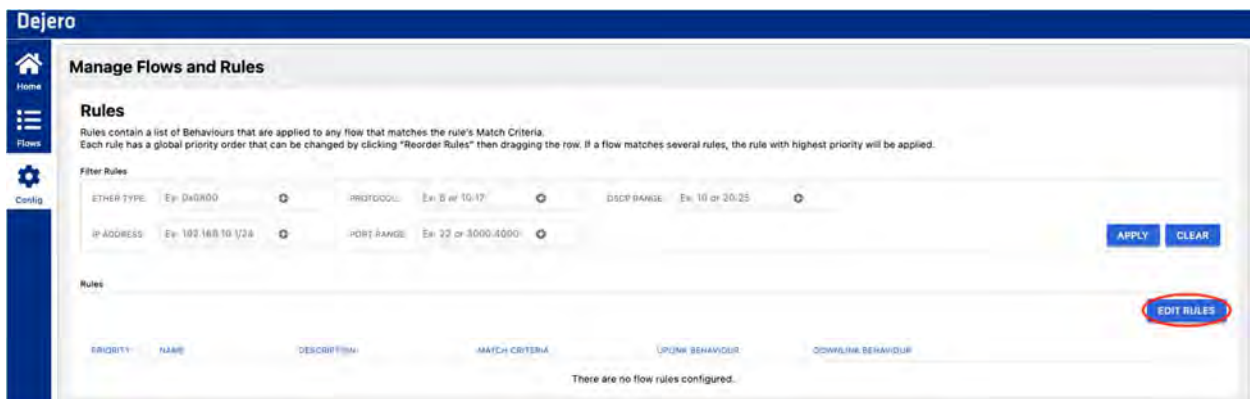
Configuring Flow Rules

The following screen shows how to access the Rule configuration screen.

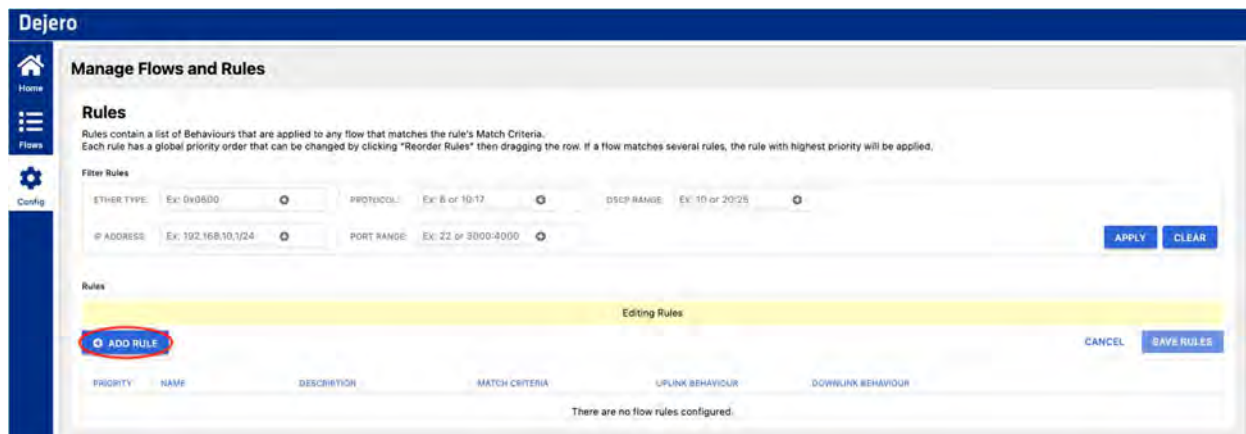
1. Select the “*Config*” icon on the Web UI navigation bar
2. Then select “*Flow Rules*”.



The current set of Rules will be displayed. This screen has two modes of operation: viewing and editing. In order to add or change rules, enter edit mode by clicking the “*Edit Rules*” button.



To add a new rule, hit the “*Add Rule*” button.



Add/edit rule modal

The following screen shows the modal dialog for adding a new rule or editing an existing one.

Add Rule

Name
My First Rule

Description
Description for my first rule

Match Criteria ⌵ Collapse

Ether Type
IPv4 (0x0800)

Protocol
TCP (6)

Local IP(s)
Tip: press enter, tab, or comma to add ports
100.64.0.12 Ex: 192.168.10.1/24

Remote IP(s)
Tip: press enter, tab, or comma to add ports
Ex: 192.168.10.1/24

Local Port(s)
Tip: press enter, tab, or comma to add ports
Ex: 22 or 3000:4000

Remote Port(s)
Tip: press enter, tab, or comma to add ports
80 443 Ex: 22 or 3000:4000

Enable Rule
ON **OFF**

The first section includes the “*Name*” and “*Description*” fields, which can be used to provide a friendly display name for the Rule.

The next section allows configuring the **Match Criteria** for the Rule, which is specified in terms of the tuples that can be parsed from the Ethernet frame headers:

- EtherType
- If EtherType is IPv4:
 - a. Protocol
 - b. Local IP
 - c. Remote IP
- If Protocol is TCP or UDP:

- a. Local port
- b. Remote port

The next section allows configuring the resulting **Behaviour** to be applied when a flow matches the specified **Match Criteria**. The available **Behaviour** options can change based on the selected protocol. The following screen shows how when the Protocol “TCP (6)” is specified for the **Match Criteria**, a **Behaviour** is available that allows enabling or disabling TCP Acceleration.

The screenshot displays the configuration interface for Match Criteria and Behavior. In the Match Criteria section, the Protocol is set to TCP (6), which is circled in red. The Local IP(s) is 100.64.0.12, Remote IP(s) is 192.168.10.1/24, Local Port(s) is 22 or 3000:4000, and Remote Port(s) is 80, 443, and 22 or 3000:4000. In the Behavior section, the text 'TCP Acceleration does not apply to connections initiated from WAN.' is displayed above two buttons, 'ON' and 'OFF', both of which are circled in red, with the text 'TCP Acceleration' next to them.

Note that when TCP acceleration is enabled, it only applies to outbound TCP flows initiated from behind the GateWay. Inbound TCP flows that are initiated from beyond the Concentrator (which require configuring Port Forwarding in Control), will never match any rules that enable TCP acceleration, regardless of the Match Criteria.

If desired, rules can still be added to match these inbound TCP flows. This is typically not necessary because the default SBT behaviour when there are no matching rules is generally as expected for TCP flows.

However, just as a contrived example, consider a scenario where there is a web server plugged into the GateWay with IP address 100.64.0.254, listening on port 443. Port forwards have been set up in Control such that this web server is reachable from the Internet.

In addition to accepting inbound web server connections, imagine that the web server also makes outbound TCP connections to download OS and application updates.

Normally no rules would need to be added to achieve optimal behaviour. By default the outbound TCP connections are TCP accelerated, and the inbound connections use the Controlled Delay (CoDel) input queue.

For the sake of argument, say the End User does not want the outbound TCP connections to be accelerated. They would add the following rule to achieve this:

Rule #1: Disable TCP acceleration for outgoing connections from the web server to retrieve OS/application updates

- **Match Criteria**

- Ether Type: IPv4 (0x0800)
- Protocol: TCP (6)
- Local IP: 100.64.0.254
- Local Port: <any>
- Remote IP: <any>
- Remote Port: <any>

- **Behaviour**

- TCP Acceleration: OFF
- Input Queue Type: CoDel
- Interval (ms): 100
- Target (ms): 5

Sometime later, say the End User now wants the inbound TCP connections to the web server to use the MaxAgeFIFO input queue rather than the default Controlled Delay (CoDel). To achieve this, they must insert a new rule before the previous one, since the new rule has more specific Match Criteria (recall that “first match wins”).

Note how the local information in the Match Criteria of this new rule is still from the perspective of the web server, even though the rule is intended to match inbound connections. Specifically, the web server IP and listening port are listed as the “Local IP” and “Local Port” in this rule, not the remote.

Rule #1: Use the MaxAgeFIFO input queue for inbound connections to the web server

- **Match Criteria**

- Ether Type: IPv4 (0x0800)
- Protocol: TCP (6)
- Local IP: 100.64.0.254
- Local Port: 443
- Remote IP: <any>
- Remote Port: <any>

- **Behaviour**

- TCP Acceleration: OFF
- Input Queue Type: MaxAgeFIFO
- Max Age: 150 ms

Rule #2: Disable TCP acceleration for outbound connections from the web server to retrieve OS/application updates

- **Match Criteria**

- Ether Type: IPv4 (0x0800)
- Protocol: TCP (6)
- Local IP: 100.64.0.254
- Local Port: <any>
- Remote IP: <any>
- Remote Port: <any>

- **Behaviour**

- TCP Acceleration: OFF
- Input Queue Type: CoDel
- Interval (ms): 100
- Target (ms): 5

The following screen shows how the available Behaviours can change in response to the settings for the Behaviours themselves.

Behavior ⌵ Collapse

TCP Acceleration does not apply to connections initiated from WAN.

☒ ON ☐ OFF TCP Acceleration

☒ ON ☐ OFF Same Behavior for Uplink & Downlink

Uplink & Downlink Behavior

Input Queue Type

CoDel

Interval (ms) *

100

Target (ms) *

5

When TCP Acceleration is disabled, additional Behaviours are shown that allow configuring the Input Queue. The supported options are:

- CoDel (Controlled Delay) - This AQM algorithm is described by [RFC 8289](#). Under contention, it adaptively drops packets from the input queue based on the packet sojourn time (Queueing + Round-trip Transmission delay), dropping them in a way that is intended to make a typical TCP sender reduce its transmission rate. See the RFC for more details on how the algorithm works, and the meaning of its two parameters (Interval and Target).
- MaxAgeFIFO - Under contention, this AQM algorithm drops packets in a FIFO manner, based purely on the age of the packets. If the age exceeds the configured threshold at the time of dequeue, the packet is dropped. It is intended for real-time flows that have a hard

deadline. For example, if a live video stream has a target playback latency of 500ms, packets with an age that exceed this latency will not be useful to transmit since they will be too late for playback by the time they reach the receiver.

The following screen shows similar Input Queue configuration capabilities for non-TCP protocols (Protocol==UDP (17)). Also note how the “TCP Acceleration” option is not shown for this protocol.

The screenshot displays the configuration interface for a Dejero Titan Command. It is divided into two main sections: "Match Criteria" and "Behavior".

Match Criteria: This section contains fields for "Ether Type" (set to IPv4 (0x0800)), "Protocol" (set to UDP (17), which is circled in red), "Local IP(s)", "Remote IP(s)", "Local Port(s)", and "Remote Port(s)". Each IP and port field includes a tip: "Tip: press enter, tab, or comma to add ports".

Behavior: This section includes a toggle for "Same Behavior for Uplink & Downlink" (currently set to "ON"). Below this is a section titled "Uplink & Downlink Behavior" which is circled in red. It contains three fields: "Input Queue Type" (set to CoDel), "Interval (ms)" (set to 100), and "Target (ms)" (set to 5).

The following screen shows the option to configure different behaviours for the uplink and downlink directions. Typically, applications would expect a symmetric configuration, so the default is to use the same settings on both sides. However, the default can be disabled if desired.

The screenshot shows the 'Behavior' configuration page. At the top, there are two buttons: 'ON' (highlighted with a red circle) and 'OFF'. To the right of these buttons is the text 'Same Behavior for Uplink & Downlink'. Below this, there are two columns of settings. The left column is titled 'Uplink Behavior' and contains three fields: 'Input Queue Type' (set to 'CoDel'), 'Interval (ms) *' (set to '100'), and 'Target (ms) *' (set to '5'). The right column is titled 'Downlink Behavior' and contains two fields: 'Input Queue Type' (set to 'MaxAgeFIFO') and 'Max Age (ms) *' (set to '3000'). A red circle highlights the 'Downlink Behavior' section.

The following screen shows how to customize behaviour for packets within a flow that is DSCP tagged.

The screenshot shows the 'Behavior' configuration page. At the top, there are two buttons: 'ON' (highlighted with a red circle) and 'OFF'. To the right of these buttons is the text 'Same Behavior for Uplink & Downlink'. Below this, there is a section titled 'Uplink & Downlink Behavior' which contains three fields: 'Input Queue Type' (set to 'CoDel'), 'Interval (ms) *' (set to '100'), and 'Target (ms) *' (set to '5'). Below this section, there is a section titled 'DSCP' which contains a button labeled 'ADD SUB RULE' (highlighted with a red circle).

For example, a parent flow (identified by EtherType, Protocol, IPs, or Ports) might match VPN traffic. Within that VPN, there may be independent flows generated by several applications that have different requirements such as a VoIP flow in the VPN at the same time as a TCP file transfer, both with their own unique DSCP tags.

Clicking the “Add Sub Rule” button allows adding additional Match Criteria and Behaviours that will only be applied to packets that match the parent Match Criteria and the Sub Rule Match Criteria.

The following screen shows a Sub Rule configured to match DSCP tag 13, for which the MaxAgeFIFO input queue AQM algorithm will be applied.

DSCP Collapse

☒ Live video inside VPN tunnel ✕

Name

Live video inside VPN tunnel

Match Criteria

DSCP Ranges(s) *

13 ✕ Ex: 5 of 5:15 +

☒ **ON** ☐ **OFF** Same Behavior for Uplink & Downlink

Uplink & Downlink Behavior

Input Queue Type	Max Age (ms) *
MaxAgeFIFO	1000

+ **ADD SUB RULE**

As more Behaviours are added in the future, only some of them will be configurable for Sub Rules. Sub Rules are constrained by requirements of their parent flow. For example, VPNs generally require packets to be delivered in order (to prevent replay attacks). Therefore, the only Behaviours on Sub Rules that will be exposed are those that cannot result in packets being delivered out of order.

The following screen shows how it is possible to add multiple DSCP Sub Rules and manage them using the icons in top right.

The screenshot displays the DSCP configuration page. At the top left is the 'DSCP' header, and at the top right is a 'Collapse' button. Below the header, there are two rule configurations. The first rule is 'Live video inside VPN tunnel'. It has a name field with the text 'Live video inside VPN tunnel'. Under 'Match Criteria', there is a 'DSCP Ranges(s)' field with the value '13' and an example 'Ex: 5 or 5:15'. Below this are 'ON' and 'OFF' buttons, with 'ON' being selected. A label 'Same Behavior for Uplink & Downlink' is next to the buttons. Under 'Uplink & Downlink Behavior', there is an 'Input Queue Type' field with 'MaxAgeFIFO' and a 'Max Age (ms)' field with '1000'. The second rule is 'TCP inside VPN tunnel'. It has a name field with the text 'TCP inside VPN tunnel'. Under 'Match Criteria', there is a 'DSCP Ranges(s)' field with the value '42' and an example 'Ex: 5 or 5:15'. Below this are 'ON' and 'OFF' buttons, with 'ON' being selected. A label 'Same Behavior for Uplink & Downlink' is next to the buttons. Under 'Uplink & Downlink Behavior', there is an 'Input Queue Type' field with 'MaxAgeFIFO' and a 'Max Age (ms)' field with '1000'. Red circles highlight the up/down arrows and trash can icons for each rule.

Management includes:

- Changing their order using the up/down arrows (just like parent rules, first match “wins” for Sub Rules)
- Deleting them using the trash can icon

The following screen shows how the Add/Edit modal can be dismissed by clicking one of the two buttons at the bottom of the dialog, “Cancel” or “Add”.

Add Rule

Name

My First Rule

Enable Rule

ON OFF

Description

Description for my first rule

Match Criteria

Collapse

Ether Type

IPv4 (0x0800)

Protocol

TCP (6)

Local IP(s)

Tip: press enter, tab, or comma to add ports

100.64.0.12 Ex: 192.168.10.1/24

Remote IP(s)

Tip: press enter, tab, or comma to add ports

Ex: 192.168.10.1/24

Local Port(s)

Tip: press enter, tab, or comma to add ports

Ex: 22 or 3000:4000

Remote Port(s)

Tip: press enter, tab, or comma to add ports

80 443 Ex: 22 or 3000:4000

Behavior

Collapse

TCP Acceleration does not apply to connections initiated from WAN.

ON OFF

TCP Acceleration

ON OFF

Same Behavior for Uplink & Downlink

Uplink & Downlink Behavior

Input Queue Type

CoDel

Interval (ms) *

100

Target (ms) *

5

CANCEL

ADD

Clicking either will return to the “Managed Flows and Rules” screen, still in edit mode.

“Add” will add a draft of the new Rule to the edit mode screen.

Manage rules

The following screen shows the “*Manage Flows and Rules*” screen in edit mode, with draft rules that are in progress.

Dejero

Manage Flows and Rules

Rules

Rules contain a list of Behaviours that are applied to any flow that matches the rule's Match Criteria. Each rule has a global priority order that can be changed by clicking "Reorder Rules" then dragging the row. If a flow matches several rules, the rule with highest priority will be applied.

Filter Rules

ETHER TYPE: Ex: 0x0800 PROTOCOL: Ex: 6 or 10/17 DSCP RANGE: Ex: 10 or 20/25
 IP ADDRESS: Ex: 192.168.10.1/24 PORT RANGE: Ex: 22 or 3000-4000

Rules

Editing Rules

ADD RULE **CANCEL** **SAVE RULES**

PRIORITY	NAME	DESCRIPTION	MATCH CRITERIA	UPLINK BEHAVIOUR	DOWNLINK BEHAVIOUR
1	> My First Rule Includes DSCP Sub Rules	Description for my first rule	ETHER TYPE: IPv4 (0x0800) PROTOCOL: TCP (6)	QUEUE TYPE: CoDel INTERVAL (ms): 100 TARGET (ms): 5	QUEUE TYPE: CoDel INTERVAL (ms): 100 TARGET (ms): 5...
2	> Default UDP	Apply default behaviour for UDP traffic	ETHER TYPE: IPv4 (0x0800) PROTOCOL: UDP (17)	QUEUE TYPE: MaxAgeFIFO MAX AGE (ms): 500	QUEUE TYPE: MaxAgeFIFO MAX AGE (ms): 500

While in this mode, additional changes can be made including the ability to re-order the rules. Similar to firewall rules, per-flow Rules are matched in the order that they appear, and the first match "wins".

The rules can be re-ordered by clicking and holding the handle on the left-side of the rule and dragging the rule up or down within the list. Releasing the handle completes the reordering.

The following screen shows that while in edit mode, the other options are to edit or delete the individual rules, using either of the two buttons to the right of the rule.

Dejero

Manage Flows and Rules

Rules

Rules contain a list of Behaviours that are applied to any flow that matches the rule's Match Criteria. Each rule has a global priority order that can be changed by clicking "Reorder Rules" then dragging the row. If a flow matches several rules, the rule with highest priority will be applied.

Filter Rules

ETHER TYPE: Ex: 0x0800 PROTOCOL: Ex: 6 or 10/17 DSCP RANGE: Ex: 10 or 20/25
 IP ADDRESS: Ex: 192.168.10.1/24 PORT RANGE: Ex: 22 or 3000-4000

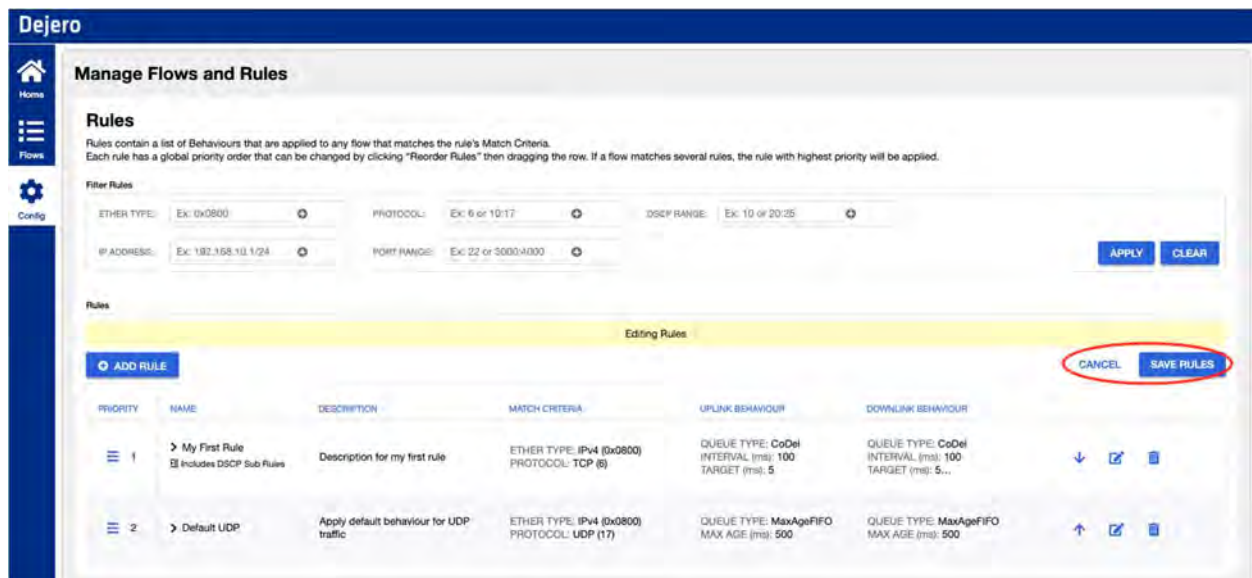
Rules

Editing Rules

ADD RULE **CANCEL** **SAVE RULES**

PRIORITY	NAME	DESCRIPTION	MATCH CRITERIA	UPLINK BEHAVIOUR	DOWNLINK BEHAVIOUR
1	> My First Rule Includes DSCP Sub Rules	Description for my first rule	ETHER TYPE: IPv4 (0x0800) PROTOCOL: TCP (6)	QUEUE TYPE: CoDel INTERVAL (ms): 100 TARGET (ms): 5	QUEUE TYPE: CoDel INTERVAL (ms): 100 TARGET (ms): 5...
2	> Default UDP	Apply default behaviour for UDP traffic	ETHER TYPE: IPv4 (0x0800) PROTOCOL: UDP (17)	QUEUE TYPE: MaxAgeFIFO MAX AGE (ms): 500	QUEUE TYPE: MaxAgeFIFO MAX AGE (ms): 500

The following screen shows that once all of the desired changes have been completed, edit mode can be exited by clicking either of the two buttons in the top right corner.

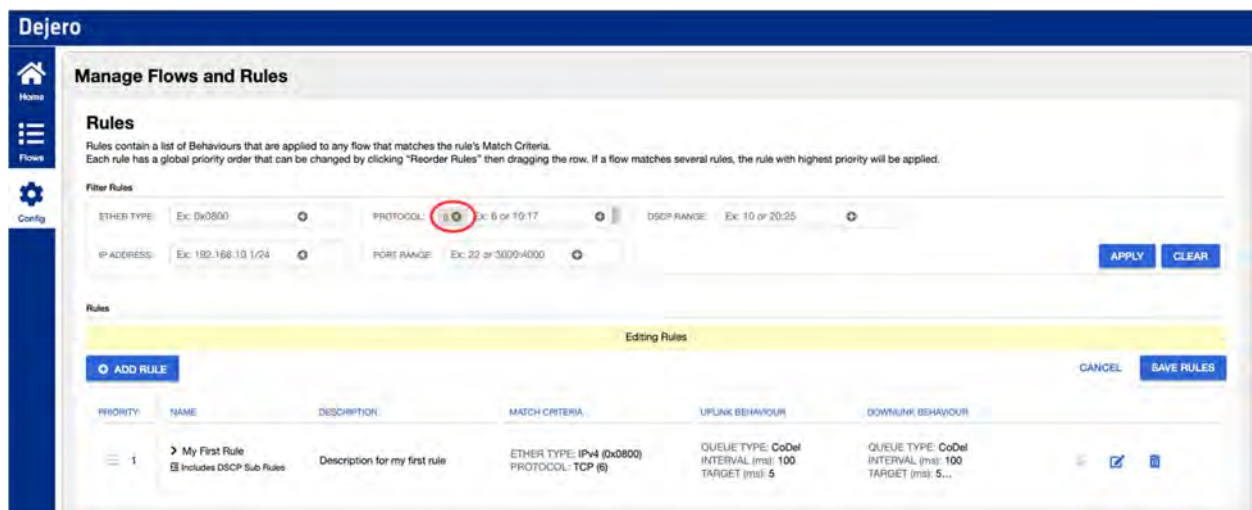


“Cancel” discards any changes made to the rules, and “Save Rules” makes the changes active so that they will immediately start to be applied to flows moving through the system.

Attempting to navigate away from the page while still in edit mode with unsaved changes will display a warning.

Searching or filtering rules

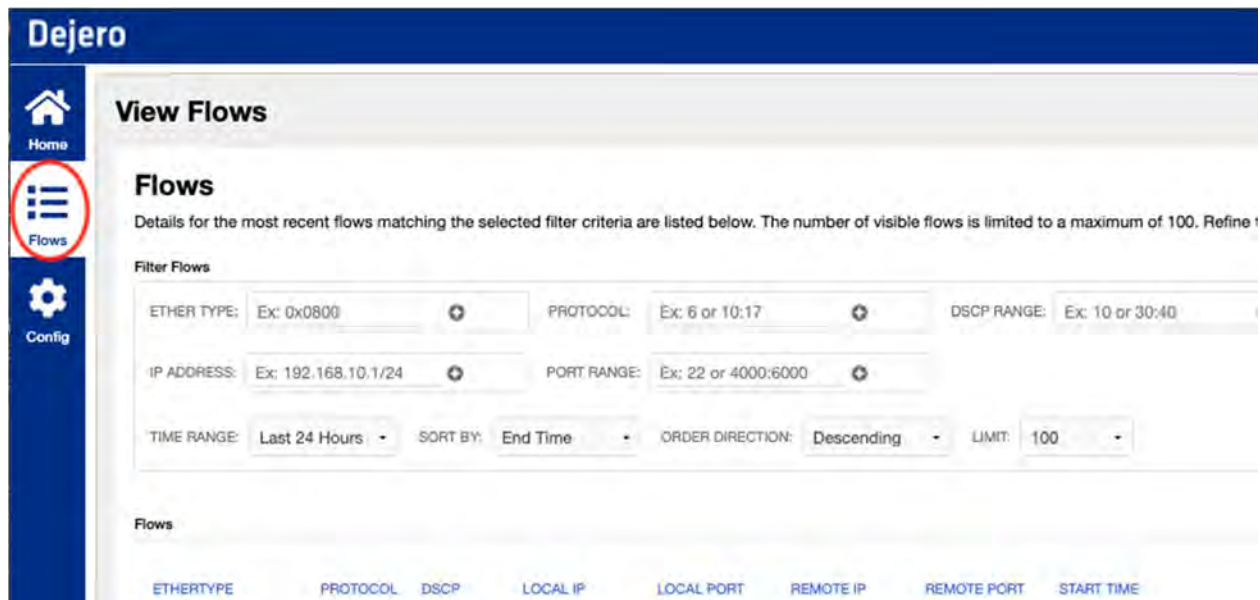
The Rules on the “Manage Flows and Rules” screen can also be searched or filtered, which can be useful if the rule set is especially large. The following screen shows how the rule list has been filtered by the TCP protocol.



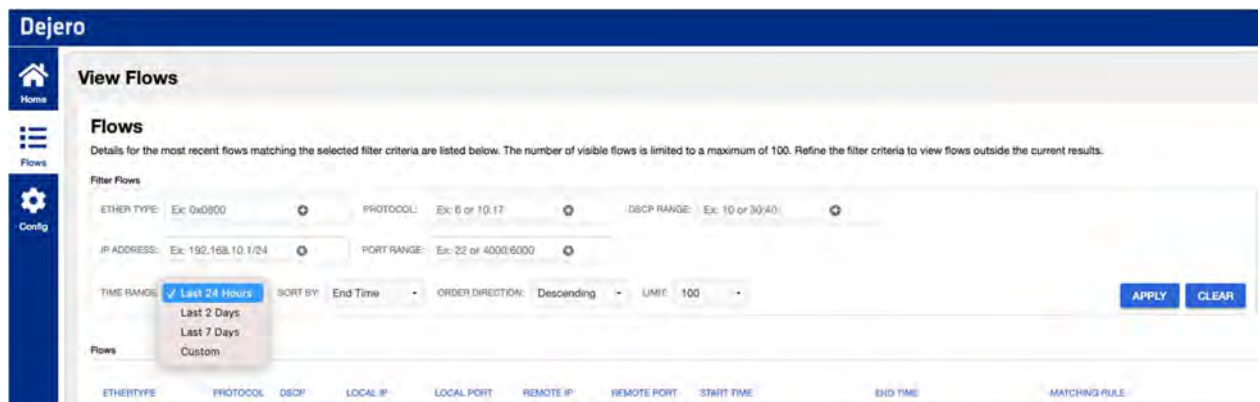
At any time, the applied filter can be cleared by clicking the “Clear” button.

View flows

As application flows traverse through the GateWay and Concentrator, metadata about each of the flows is recorded. The “View Flows” screen allows inspection of metadata for both current and historical flows. The following screen shows how to access this screen, by clicking on the “Flows” button in the navigation bar.



Since a typical GateWay device will have many application flows, the first step is typically to filter and sort them based on criteria. The following screen shows the filters that are available:

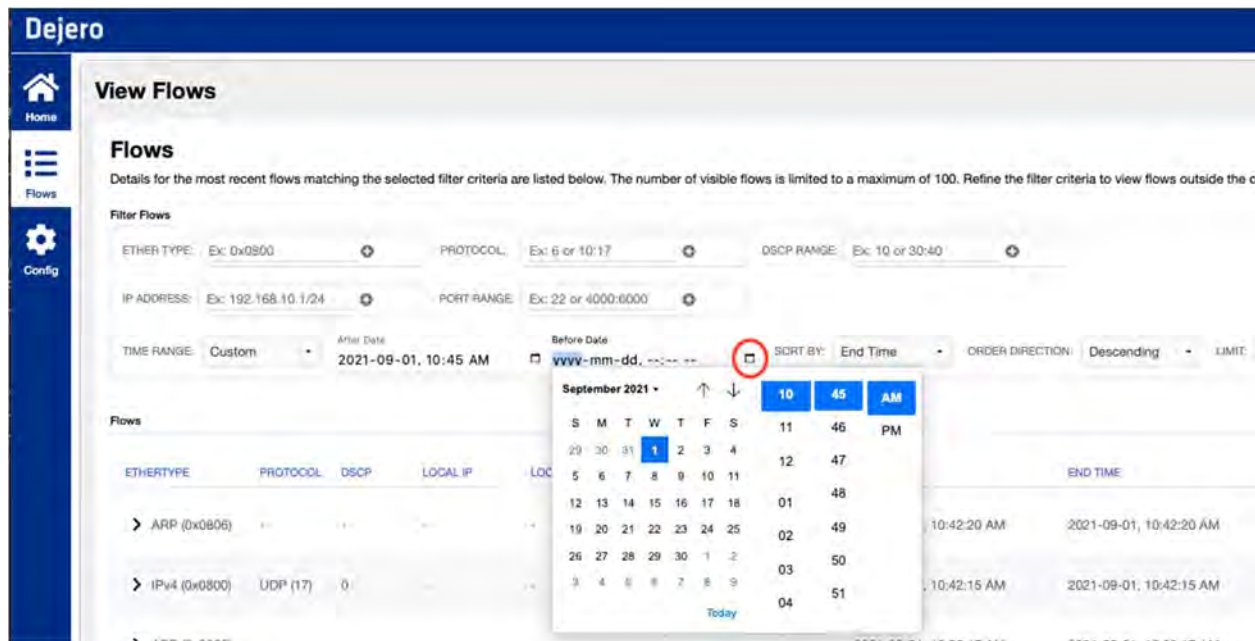


- Ether Type
- Protocol
- DSCP Range
- IP Address
- Port Range
- Time Range
 - Last 24 hours
 - Last 2 days
 - Last 7 days
 - Custom

As well as sort and limit operations:

- Sort by
 - End Time
 - Start Time
 - Usage (sum of upload and download bytes)
- Order Direction
 - Descending
 - Ascending
- Limit (10, 25, 50, 100, 250, no limit)

The following screen shows the date pickers for selecting the start and end times for the Custom range.



The following screen shows the resulting table of flows that is displayed for the given filter.

View Flows

Flows
Details for the most recent flows matching the selected filter criteria are listed below. The number of visible flows is limited to a maximum of 100. Refine the filter criteria to view flows outside the current results.

Filter Flows

ETHER TYPE: Ex: 0x0800 PROTOCOL: Ex: 6 or 10,17 DSCP RANGE: Ex: 10 or 30:40

IP ADDRESS: Ex: 192.168.10.1/24 PORT RANGE: Ex: 22 or 4000:8000

TIME RANGE: Last 24 Hours SORT BY: End Time ORDER DIRECTION: Descending LIMIT: 100

Flows

ETHERTYPE	PROTOCOL	DSCP	LOCAL IP	LOCAL PORT	REMOTE IP	REMOTE PORT	START TIME	END TIME	MATCHING RULE
IPv4 (0x0800)	TCP (6)	0	10.200.1.2	41338	172.217.165.14	443	2021-09-01, 11:10:00 AM	-	RULE #1: My First Rule
IPv4 (0x0800)	ICMP (1)	48	10.200.1.2	-	8.8.8.8	-	2021-09-01, 11:10:00 AM	-	NO MATCH
IPv4 (0x0800)	ICMP (1)	48	10.200.1.2	-	8.8.4.4	-	2021-09-01, 11:10:00 AM	-	NO MATCH
IPv4 (0x0800)	UDP (17)	0	10.200.1.2	52395	8.8.8.8	53	2021-09-01, 11:10:00 AM	-	RULE #2: Default UDP
IPv4 (0x0800)	UDP (17)	0	10.200.1.2	52395	8.8.4.4	53	2021-09-01, 11:10:00 AM	-	RULE #2: Default UDP
IPv4 (0x0800)	UDP (17)	0	10.200.1.2	12483	8.8.8.8	53	2021-09-01, 11:10:00 AM	-	RULE #2: Default UDP
IPv4 (0x0800)	UDP (17)	0	10.200.1.2	12483	8.8.4.4	53	2021-09-01, 11:10:00 AM	-	RULE #2: Default UDP

The displayed columns are:

- The Ethernet frame header information that identifies the flow (same fields as the Match Criteria in the Rules).
- The start and end times for the flow. The end time can be blank if the flow is still active.
 - The start and end times for TCP accelerated flows reflect the TCP state machine (i.e. from TCP SYN to TCP FIN).
 - For non-TCP accelerated flows, the end time is based on an activity timer. If a flow has not generated any traffic for 1 minute (in either direction), its last activity time is counted as the flow end time. These flows also end when the Rules are updated (ongoing flows will be logged again as new entries) or when the GateWay is powered down.
- The name of the Rule (and Sub Rule) that was matched and applied to the flow, if any.

The “*Refresh*” button can be used to update the list of flows matching the selected filter criteria. The “*Clear*” button resets the filter to its default state and updates the list of flows accordingly.

The following screen shows how it is possible to click on a flow and expand its details. Detailed metadata including aggregate and per-WAN byte and packet counts are displayed.

 V4 (0x0800)	UDP (17)	0	100.64.0.4	51451	172.217.13.105	443	2021-09-03, 11:53:08 AM	NO MATCH
---	----------	---	------------	-------	----------------	-----	-------------------------	----------

FLOW TIMES	
START TIME	LAST ACTIVE
2021-09-03, 11:53:08 AM	-

BLENDED UPLOAD			BLENDED DOWNLOAD		
	DATA	PACKETS		DATA	PACKETS
ACTUAL	1.171 MB	3913	ACTUAL	350.176 KB	1734
RETRANSMITTED	936.476 KB	2661	LATE	0	0
DROPPED	0	0	DROPPED	48.303 KB	435

UPLOAD BY CONNECTION			DOWNLOAD BY CONNECTION		
	DATA	PACKETS		DATA	PACKETS
WAN0	713.66 KB	2046	WAN0	262.723 KB	1299
CELL2	116.633 KB	419	CELL2	32.959 KB	175
CELL1	210.883 KB	1086	CELL1	11.504 KB	31
CELL0	130.076 KB	362	CELL0	42.99 KB	229

Configuring the device with the Titan local user interface

You can use the Titan local user interface to configure the device.



Note: To access the Titan local user interface, you must have a monitor and keyboard attached to the Titan device. You must use a USB-C adapter with an HDMI or Display Port port as well as an available USB port for the keyboard attachment..

Configure the management interface

4. In the Titan local user interface, navigate to **Configure Interfaces** and press **Enter**.
5. Navigate to **br0** and press **Enter**.
6. Perform one of the following options:
 - To use the settings in Control, navigate to **Control** and press **Enter**.
 - To use a static IP, navigate to **Static IP** and press **Enter**. Set the **IP** and **Netmask** fields.
7. Navigate to **OK** and press **Enter**.
8. Restart the Titan device.

Configure the WAN interface

1. In the Titan local user interface, navigate to **Configure Interfaces** and press **Enter**.
2. Navigate to **wan0** and press **Enter**.
3. Perform one of the following options:
 - To use the settings in Control, navigate to **Control** and press **Enter**.

- To use a DHCP server, navigate to **DHCP** and press **Enter**.
 - To use a static IP, navigate to **Static IP** and press **Enter**. Set the **IP**, **Netmask**, **Titan**, and **DNS Servers** fields.
8. Navigate to **OK** and press **Enter**.
 9. Restart the Titan device.

Set a friendly name for interfaces

1. In the Titan local user interface, navigate to **Interface Names** and press **Enter**.
2. Navigate to **Add Name** and press **Enter**.

Remove friendly name for interfaces

1. In the Titan local user interface, navigate to **Interface Names** and press **Enter**.
2. Navigate to **Remove Names** and press **Enter**.

Add custom NTP servers

You can add up to two custom NTP servers for each WAN interface.

1. In the Titan local user interface, navigate to **NTP Configuration** and press **Enter**.
2. Navigate to **Set servers** and press **Enter**.
3. In the **WAN interface name** field, type the name of the interface.
4. In the **NTP server(s)** field, type the IP addresses for the NTP servers.
5. Navigate to **Set** and press **Enter**.
6. Restart the Titan device.

Change the details for custom NTP servers

You can change the details for the custom NTP servers that you configure for your WAN interfaces.

1. In the Titan local user interface, navigate to **NTP Configuration** and press **Enter**.
2. Navigate to **Edit server** and press **Enter**. Perform one of the following actions:
3. Navigate to an interface and press **Enter**.
4. Change the details for the configuration.
5. Navigate to **Save** and press **Enter**.
6. Restart the Titan device.

Remove a custom NTP server from a WAN interface

You can remove a custom server from a WAN interface.

1. In the Titan local user interface, navigate to **NTP Configuration** and press **Enter**.
2. Navigate to **Clear server** and press **Enter**.
3. Navigate to an interface and press **Enter**.
4. Navigate to **Clear** and press **Enter**.
5. Restart the Titan device.

Configure Wi-Fi overrides

By default, the Titan device attempts to configure the Wi-Fi network based on the location of the Titan device. However, if the device cannot determine the location, you can configure a specific country code so your Wi-Fi network uses only the network bands allowed as part of the country's regulations.



Tip: For a list of the country codes that you can use, visit <https://www.iso.org/iso-3166-country-codes.html>.

1. In the Titan local user interface, navigate to **Wi-Fi Overrides** and press **Enter**.
2. In the **Country code** field, type the country code.
3. Navigate to **OK** and press **Enter**.
4. Restart the Titan device.



Note: To clear the Wi-Fi override, clear the **Country code** field.

Monitoring the Titan device

You can also use Control to monitor the Titan device, including reviewing the device's speed and data usage. You can also run reports on the device.

View device status and upload and download speed

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.

The **Manage > GateWay** page shows the status of the device and its upload and download speed.

View the status of network interfaces

This feature is available for Titan devices with version 3.6.0 or later.

1. In Control, click **Manage > GateWay**.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. View the interface information beside the device name.



Tip: To view more detailed information about the network interfaces, for example, if they are not connected and should be or are in an error state, you can view more detailed information for the individual connections on the Home page of the Titan Web UI. For more information on accessing the Titan Web UI, see "Remotely access the Titan Web User Interface" on page .

Monitor data usage

1. In Control, click **Manage > GateWay**.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.

On the **Usage** tab, the **Data Usage** section shows specific details about the data used by all connections and the transfer rate. The **Cellular Usage This Month** section includes a graph with only the cellular data used in the past month.

Monitor data transfer speed

1. In Control, click **Manage > GateWay**.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.

3. Click a device name.
4. In the **Data Usage** section, perform one or more of the following actions:
 - Review the data in the **Download by Connection** and **Upload by Connection** graphs.
 - In the **Transfer Rate** graph, click **Last Hour**, **Last 6 Hours**, or **Last 24 Hours**.



Tip: To view more information about the upload or download speed at a given point in time, hover over the **Transfer Rate** graph at that point. To view only the upload or download speed, click **Upload** or **Download** in the graph's legend.

Geolocate the Titan device

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.

On the **Usage** tab, the map shows the last known location of the Titan device.



Tip: To update the map, refresh the page.

Run a speed test

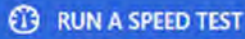
You can run a speed test on a Titan device to measure its performance. You can only run a speed test when a Titan device is connected.



Note: If you turn on connection priority and then run a speed test, the test follows the connection priority rules that you configured. If you enable cellular shaping, and the amount of data transferred reaches the specified threshold, the test reports the lower data transfer speed.

1. In Control, click **Manage** > GateWay.
2. Beside the **Quick Filter** field, click ▼.
3. Select **Connected**.
4. Click a device name.
5. Click the **Speed Test** tab.

6. Click



During the speed test, Control checks the latency for the blended connection, as well as its download and upload speeds. It also checks the latency, download, and upload speed for each individual connection.



Note: Running a speed test uses data from your monthly data allocation.

View information on support sessions

If you need to contact Dejero Support, they use a support session to access your Titan device. During a support session, the status of the Titan device can appear as **Disconnected** in Control and on the Titan device's Main screen.

1. In Control, click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Click a device name.
4. Click the **Support Sessions** tab.

On this tab, you can view the user who accessed the Titan and the start and end times of each support session.



Note: By default, a support session lasts a maximum of one hour. If you view the information for a support session while the session is active, the **End Time** column might show a time in the future.

Run a Titan usage report

You can run a usage report for the Titan to view statistics on the Titan solution for your selected stations. You can also narrow the report to view statistics for specific devices.

1. In Control, click **Reports** > **GateWay Usage Report**.
2. Beside the **Report Options** field, click ▼.
3. Perform one or more of the following actions:
 - In the **Date span** drop-down list, set the time period for the report. By default, the time period is set to **This Month**.

- To set a custom time period for the report, in the **Date Span** drop-down list, select **Custom**. Set the date range.
- To narrow the Titan devices included in the report, in the **Filter by Titan** field, type the device name, asset tag, or serial number. Select a device. Repeat this step to include additional devices in the report.
- In the **Connection Types** section, select **All** or **Cellular-only**.

4. Click .

The report refreshes to show the total amount of data used, the number of Titan devices in the solution, and the data used over time. The report also shows the name of each Titan device in the solution during the selected period, and the amount of data used per device.



Tip: To view more information about data usage at a given point in time, hover over the **Data Usage Over Time** graph at that point. To view only the cellular data usage or only the other data usage, click the appropriate label in the graph's legend.

Run a Titan usage report quickly for specific devices and the current month

From the Manage Titan screen, you can quickly run a usage report to view statistics for specific devices within your selected stations. By default, the report shows the current month and all connection types.

1. Click **Manage** > GateWay.
2. Perform one or more of the following actions:
 - Beside the **Quick Filter** field, click ▼. Select a status.
 - In the **Enter filter terms** field, select or type the device name, asset tag, serial number, status, station name, or software version.
3. Select the check box for one or more Titan devices.
4. Click  **Usage**.

A new report window opens to show the total amount of data used, the number of Titan devices in the solution, and the data used over time. The report also shows the name of each Titan device in the solution during the selected period, and the amount of data used per device.

5. If necessary, to change any of the report options, beside the **Report Options** field, click ▼.



Tip: To view more information about data usage at a given point in time, hover over the **Data Usage Over Time** graph at that point. To view only the cellular data usage or only the other data usage, click the appropriate label in the graph's legend.

Run a Titan SIM usage report

You can run a SIM usage report for the Titan to view statistics on the SIMs used in your Titan solution for your selected stations.

1. In Control, click **Reports > GateWay SIM Usage Report**.
2. Beside the **Report Options** field, click .
3. Perform one or more of the following actions:
 - In the **Date span** drop-down list, set the time period for the report. By default, the time period is set to **This Month**.
 - To set a custom time period for the report, in the **Date Span** drop-down list, select **Custom**. Set the date range.
4. Click .

The report refreshes to show the SIMs used, their serial number and IMEI, and the name of the wireless network that they roamed onto. The report also shows the total amount of cellular data used for each SIM.



Note: You can only run a SIM usage report back to June 4, 2018. If you select a date earlier than June 4, 2018, blank results appear in the report.

Download a report

1. In Control, after running the Titan Usage Report or the Titan SIM Usage Report, click



Tip: A CSV file is a comma separated value file that you can view as a spreadsheet.

Save a report

1. In Control, after running the Titan Usage Report, click .
2. Add a title.
3. Click .



Tip: When saving a report with a relative date range (such as last week or this month,) the next time that you run the report, it pulls the data as if running a new report. Saving a report with a custom time period runs the saved report with the original date range specified.

Troubleshooting

My device won't connect over VPN.

Verify that your device uses the following settings:

- Enable Support Path MTU Discovery on your VPN. You can also discover the path MTU manually to set the value. The exact value of the MTU will differ based on the wireless network used by the Titan device.
- Use automatic socket buffer tuning. You can also increase the size of the socket buffers (used by the VPN client and server to tunnel traffic.)



Note: When connecting to your corporate system over VPN, for many general applications, you should experience the same reliability and performance that you'd experience with your everyday wired connection.

My data upload or download speed has decreased.

Several factors can affect the speed or reliability of your network connection, including the following:

- **Level of cellular coverage:** Areas with insufficient cellular coverage can affect your data transfer speed. Try moving to an area with a higher level of cellular coverage.
- **Number of devices connected to the Titan device:** If many users are connected to the same Titan device, the data transfer speed for all users decreases. Try connecting to a different Titan device, if one is available.
- **The quality of the cellular connection:** If you are in an area with sufficient cellular coverage, but there are many people accessing the cellular networks at the same time, you might notice a decrease in your data transfer speed.
- **Network connection latency:** The network connection latency time can also be affected by the quality of the cellular connection. If there is a longer latency time, data transfer speeds decrease.

How do I update my software?

Software updates are managed by Dejero. For more information, contact Dejero Support.

Power or connection problems

Problem	Possible solution
The Titan device does not turn on	If the green power light on the front of the Titan does not appear, perform the following actions: 1. Confirm that you connected the power cords securely. 2. Verify that you attached the power connector to the front of the device securely. 3. If there is still no power in a vehicle, check the connections to the vehicle's battery, any relays and switches and verify the ignition switch is on. For more information, see the manual for your vehicle. 4. If the device still does not turn on, contact Dejero Support.
Titan does not connect	If the Titan device does not connect, perform the following actions: 1. Confirm that you connected the power cords securely. 2. If using a wired (Ethernet) connection: confirm that the Ethernet cable is securely connected to both the device and the router or switch. Try a different port on the router or switch. Try a different Ethernet cable. Restart the router or switch. 3. If using a cellular connection: Check that the SIM cards are properly installed. Confirm with the SIM card provider that the SIMs are active and have data service. 4. Restart the device. 5. Use Control to verify the status of the device. If the status shows Offline or Error, contact Dejero Support.

Technical specifications

Network connections

Cellular	3 x 5G with LTE/3G fallback
Cellular Bands	5G Operating Bands: n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41 (PC1.5, PC2), n48, n66, n71, n75, n76, n77 (PC1.5, PC2), n78 (PC1.5, PC2), n79 (PC1.5, PC2) LTE Operating Bands: B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41 (PC2), B42, B43, B46(LAA), B48(CBRS), B66, B71 3G bands: B1, B2, B4, B5, B6, B8, B19 Notes: - PC1.5: Power Class 1.5 - PC2: Power Class 2 - (PC1.5, PC2): the band supports both power classes depending on the carrier/network. - DL: Downlink only
Ethernet	4 x 2.5 Gb/s port
Wi-Fi Hotspot	802.11 a/b/g/n/ac/ax
SIMs	3x Nano SIMs (Industrial SIMs -extended temperature- recommended)

User interface

Indicators	3x LED indicators for power, operational status, pairing status
Control	Setup and monitoring using Control (control.dejero.com)
Titan local user interface	Configuration also available using the Titan local user interface

Titan Web User Interface	Graphical display for metrics for aggregated and individual connections, and configuration of routers
---------------------------------	---

Power

Supply	8 – 36 V with 3-pin terminal block Or POE++ input is available on Ethernet Port 4
Consumption	22W Idle; 40W Typical; 60W Peak

Physical

Dimensions (H x W x D)	6.0 x 32.8 x 25.7 cm (2.36 x 12.91 x 10.12 inches)
Weight	2.6kg (5.73lb)
Operating temperature	-40°C to 70°C (-40°F to 158°F) with 0.6m/s air flow
Operating humidity	Approximately 95% at 40°C (104°F) (non-condensing)
Storage temperature	-40°C to 70°C (-40°F to 158°F)
Vibration	MIL-STD-810G Method 514.6 Categories 12, 13, 14, 20 (Ground Vehicles – Wheeled and Tracked Vehicles), 21, 24
Shock	MIL-STD-810G Method 516.6 Procedure I - Operating 40G, 11ms, terminal peak sawtooth MIL-STD-810G Method 516.6 Procedure V - Crash Hazard 75G, 6ms, terminal peak sawtooth

Active connectors	1 x GPS antenna 4 x RJ-45 2.5 Gigabit Ethernet 1 x USB-C port 1 x Serial (COM) port 1 x DIO 1 DC power port with optional IGN input
Processor	Intel Atom® x7433RE, 3.4 GHz max turbo frequency
Memory	8 GB RAM
Storage capability:	128 GB

Regulatory compliance

Product	Dejero Titan Command
Model	CommandM3E4
Compliance	This product is compliant with international EMC and safety standards.

Additional help

If you still require assistance operating your Dejero Titan solution:

- Visit the Dejero SupportHub online knowledge base at support.dejero.com
- Email the Dejero technical support team at support@dejero.com
- Call the 24-hour technical support number for your region.
 - US & Canada: 1 866 808 3665, ext. 2
 - International: +1 519 772 4824, ext. 2



Note: When you purchase the Titan device, you receive one year of standard support and three years of hardware support for free. Before the end of your first year, contact your Dejero representative for information on the pricing available to continue your support contract.

Document revision history

Version	Date	Changes
001	December 2025	Initial release.



Technical Support:

support@dejero.com

US & Canada (Toll Free): 1 866 808 3665, ext. 2

International: +1 519 772 4824, ext. 2