



# Digi Connect IT<sup>®</sup> 4

User Guide

---

User Guide

## Revision history—90002355

Revision	Date	Description
A	July 2019	Initial release.

## Trademarks and copyright

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

© 2019 Digi International Inc. All rights reserved.

## Disclaimers

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

## Warranty

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

[www.digi.com/howtobuy/terms](http://www.digi.com/howtobuy/terms)

## Send comments

**Documentation feedback:** To provide feedback on this document, send your comments to [techcomm@digi.com](mailto:techcomm@digi.com).

## Customer support

**Digi Technical Support:** Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at +1 952.912.3444 or visit us at [www.digi.com/support](http://www.digi.com/support).

# Contents

---

## Digi Connect IT® 4 User Guide

### Get started with Connect IT 4

Verify product components .....	8
Included equipment .....	8
Required additional equipment .....	9
Cellular ONLY: Insert the CORE module .....	10
Prerequisites .....	10
Connect the hardware to a network .....	10
Connect hardware and connect to a cellular network .....	11
Connect hardware and connect to site network using an Ethernet LAN .....	11

### Connect equipment to the Connect IT serial ports

Serial port pinout and use .....	13
----------------------------------	----

### Configure Connect IT using Remote Manager

Before you begin .....	15
Enable local management for Connect IT 4 .....	16
Create a Remote Manager account and add devices .....	16
Create a Remote Manager account .....	16
Log in to Remote Manager .....	17
Add a Connect IT to your inventory .....	17
Update the firmware on Connect IT from Remote Manager .....	18
View identifying information about the Connect IT on the Home page .....	19
Access the Remote Manager configuration page .....	19
Schedule system maintenance from Remote Manager .....	20
Configure FIPS mode from Remote Manager .....	22
Configure VPN using Remote Manager .....	23
Configure an IPsec tunnel for a VPN from Remote Manager .....	23
Configure an OpenVPN server from Remote Manager .....	23
Configure an IP tunnel for a VPN from Remote Manager .....	24
View system status information from Remote Manager .....	25
View Connect IT summary dashboard .....	25
View Connect IT connection history .....	25

## Configure Connect IT using the web user interface

Log in to the Connect IT web UI .....	27
Manage users, groups, password, and two-factor authentication from the web UI .....	27
Configure idle timeout from the web UI .....	27
Add a new user from the web UI .....	28
Add a user group from the web UI .....	28
Configure the user groups from the web UI .....	28
Change a Connect IT password from the web UI .....	30
Configure the user groups from the web UI .....	30
Configure two-factor authentication from the web UI .....	31
Configure authentication methods from the web UI .....	32
Update Connect IT firmware .....	33
Download the Connect IT firmware to your PC .....	33
Configure connection to Remote Manager from the web UI .....	33
Update modem firmware .....	34
Configure a serial port .....	34
Configure the connection settings for a serial port .....	34
Monitor serial port changes .....	35
Enable a Telnet connection on the serial port .....	36
Enable a TCP connection on the serial port .....	37
Enable an SSH connection on the serial port .....	38
Configure the modem in the Connect IT .....	39
Configure the modem .....	39
Define a custom APN .....	42
Configure an IP passthrough for the modem .....	42
Configure a custom gateway for the modem .....	44
Configure an IPv4 network interface for the modem .....	44
Configure an IPv6 network interface for the modem .....	45
Configure the network from the web UI .....	47
Configure FIPS mode from the web UI .....	47
Configure VPN from the web UI .....	48
Configure an IPsec tunnel for a VPN from the web UI .....	48
Configure an OpenVPN server from the web UI .....	49
Configure an IP tunnel for a VPN from the web UI .....	49
Back up, restore, and delete the configuration .....	50
Back up the Connect IT configuration .....	50
Restore the Connect IT configuration .....	50
Delete the Connect IT configuration .....	50
Configure the firewall from the web UI .....	50
Configure services from the web UI .....	51
Monitor the data from the Connect IT .....	52
Reboot from the web UI .....	53
Immediately reboot the Connect IT .....	53
Schedule a reboot from the web UI .....	53
Schedule system maintenance from the web UI .....	53
Synchronize system time from the web UI .....	55
View Connect IT status information .....	55
Download an archive of the supported MIBs .....	55
Download a support report file .....	56
Configure and view events and logs in the web UI .....	56
View events information .....	56
Configure log messages from the web UI .....	56
View system log information .....	57

## Troubleshooting

Cellular network fallback .....	59
Reset your device to the factory defaults .....	59
Tips for improving cellular signal strength .....	59
Download a support report .....	59

## Hardware

Connect IT 4 hardware and LEDs .....	60
Front panel and LEDs .....	60
Back panel .....	61
Signal strength .....	62
Exchange power tips .....	62
Select SIM card .....	63

## Regulatory and safety information

FCC certifications .....	64
USA .....	64
INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A) .....	64
European Union .....	64
Safety warnings .....	64

## **Digi Connect IT® 4 User Guide**

---

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

The 4 provides out-of-band management for remote network or infrastructure devices. Cellular connectivity, available as standard in some models and as an option in other models, provides fast reliable cellular connections without additional equipment. All connections are encrypted for security.

## Get started with Connect IT 4

---




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

1. [Verify product components.](#)
2. [Cellular ONLY: Insert the CORE module.](#)
3. [Connect the hardware to a network.](#)
4. Access the device from the [web UI](#).
5. Update the firmware on the Connect IT from the [web UI](#).
6. [Change the password from the web UI.](#)
7. Administrators only: Additional configuration to the Connect IT can be done in Remote Manager or in the Connect IT's web user interface.
  - [Configure Connect IT using Remote Manager](#)
  - [Configure Connect IT using the web user interface](#)
8. [Connect equipment to the Connect IT serial ports.](#)




## Verify product components

Verify that you have the following included equipment.

### Included equipment

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



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

## Required additional equipment

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

## Cellular ONLY: Insert the CORE module

---

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

---

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

### Prerequisites

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

To connect the hardware and connect to the cellular network:

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

---

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

---

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

---

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

---

## Connect the hardware to a network

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

---

**Note** This is required if you want to automatically connect the Connect IT to Digi® Remote Manager. For more information, see [Configure Connect IT using Remote Manager](#).

---

- [Connect hardware and connect to a cellular network](#)
- [Connect hardware and connect to site network using an Ethernet LAN](#)

## Connect hardware and connect to a cellular network

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

---

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

---

To connect the hardware and connect to the cellular network:

1. Insert a CORE module with an activated SIM card. See [Cellular ONLY: Insert the CORE module](#).
2. Connect the power supply unit to the device.
3. Verify the cellular network signal strength indicator on the front of the 4 shows two or more bars for proper operation. See [Signal strength](#).



## Connect hardware and connect to site network using an Ethernet LAN

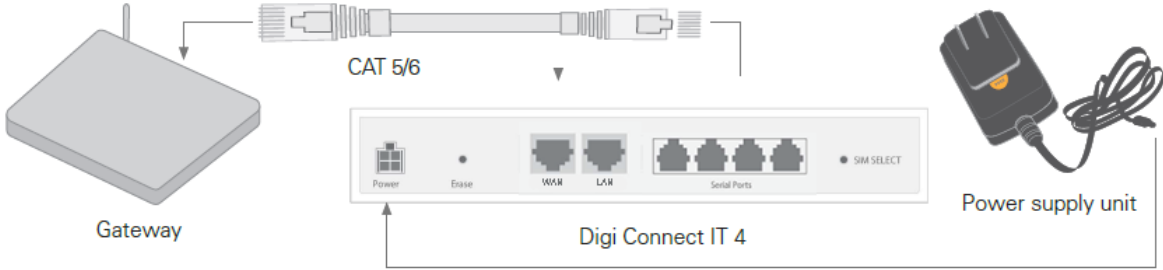
This section explains how to connect the Connect IT hardware and then connect to a site network, using an Ethernet cable.

### Prerequisites

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

To connect the hardware and connect to a site network:

1. Plug the power supply unit into an AC power outlet and connect the other end to the **Power** plug on the 4.
2. Connect one end of an Ethernet cable to your site gateway.
3. Connect the other end of the Ethernet cable to the Ethernet LAN port on the 4.



## Connect equipment to the Connect IT serial ports

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

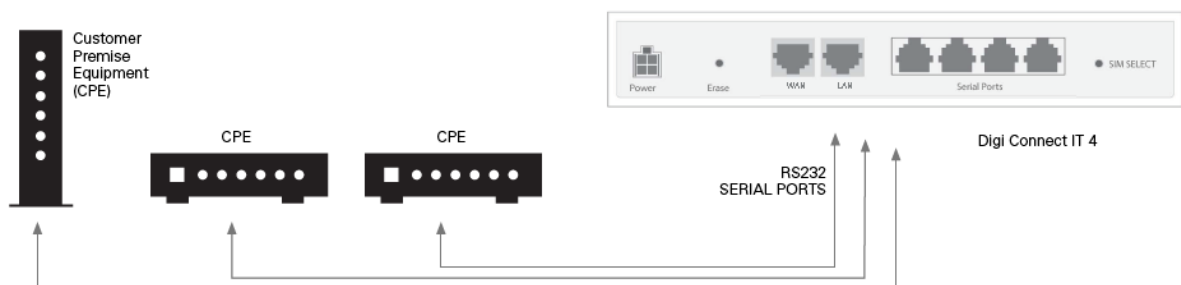
The serial ports on the 4 provide console access to connected critical equipment through the cellular network or a connected Ethernet LAN. You can connect up to 4 network devices to the 4 serial ports. For pinout information, see [Serial port pinout and use](#).

You must use a cable with an RJ45 connector to connect to the 4 with a RJ45, DB9F or DB9M connector, as determined by your device type, to terminate to your device. Consult the user guide for the device you are connecting to the 4 to determine the connector type, cable type, and pinout positions for your specific device.

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

### Serial port pinout and use

The RS232 standard requires support for baud rates up to 9600 baud on shielded multicore cable up to 50 feet (15 meters) long. For the 4, the use of standard CAT 5 cables enables serial communication at all baud rates up to 50 feet. CAT5 unshielded twisted pair cable lengths much longer than 50 feet have been verified at 9600 baud but are non-standard and are not guaranteed.

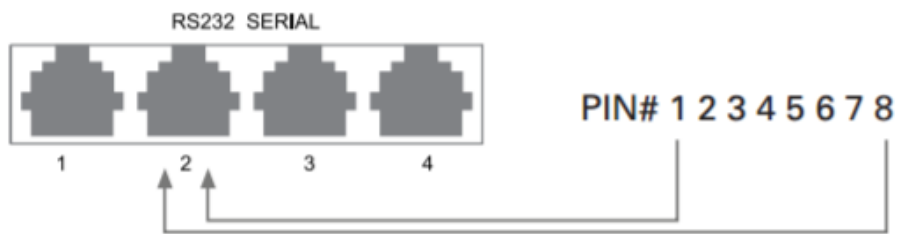


The 4 RS232 serial ports are DTE and have the following pin configuration.

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

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

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



## Configure Connect IT using Remote Manager

---

The following actions are typically only performed by your network administrator.

### Before you begin

#### Connect to Remote Manager

You must configure your computer to connect to the Connect IT, and then enable the Connect IT to connect to Remote Manager. You have the following options:

- **Connect the Connect IT 4 to your network** When the Connect IT 4 has an internet connection, the Connect IT 4 will download its configuration settings from the legacy Digi aView portal by default. This configuration then automatically re-configure the Connect IT 4 to sync with Digi Remote Manager. For instructions, see [Connect the hardware to a network](#).
- If you do not connect the Connect IT 4 to your network, you can configure your computer to connect to the Connect IT 4, and then manually enable the Connect IT 4 to connect to the Digi Remote Manager. For instructions, see [Enable local management for Connect IT 4](#).

#### Create a Remote Manager account

You must [create a Remote Manager account](#) and [add your Connect IT devices](#) to your Remote Manager inventory.

---

**Note** For more detailed information about using Remote Manager, see the [Digi Remote Manager User Guide](#).

---

## Enable local management for Connect IT 4

You can manually enable local management for Connect IT to be able to connect to Remote Manager.

---

**Note** This process should be completed only if you did not connect the Connect IT 4 to your network, which automatically re-configures the Connect IT 4 to sync with Digi Remote Manager. For instructions on connecting the Connect IT to the network, see [Connect the hardware to a network](#).

---

1. [Log in to the Connect IT web UI](#).
2. Select the **Configuration** option in the left pane.
3. Expand the **Central management** section.
4. De-select the **Enable central management** option.
5. In the **Users** section at the bottom of the screen, re-enter the password.
6. Click **Save**.
7. Log out of the Connect IT web UI.
8. Log in to the Connect IT web UI again.
9. Select the **Configuration** option in the left pane.
10. Expand the **Central management** section.
  - a. Select the **Enable central management** option.
  - b. From the **Service** list box, select the **Digi Remote Manager** option.
  - c. In the **Management server** field, enter the URL for Remote Manager.
11. Click **Save**.

## Create a Remote Manager account and add devices

To be able to use Remote Manager, you must create a Remote Manager account and add your Connect IT devices to the device list. You should also verify that the device is enabled to connect to Remote Manager.

### Create a Remote Manager account

Before you can use Remote Manager, you must create a free trial account.

#### Account owner

Part of creating the Remote Manager account is creating the first user account in Remote Manager. The first user becomes the account owner, who may not be a particular person, but a role within your organization. You may want to choose a user name that reflects a role rather than an actual person. See [Determine the Account owner](#).

1. Go to [www.digi.com/remotemanager](http://www.digi.com/remotemanager).
2. Click **30-Day Free Trial**.
3. Complete the registration form, making note of the your user name and password for future reference.

---

**Note** This first account is the account owner for Remote Manager.

---



4. Review and accept the **Terms of Service**.
5. Enter the image code in the text field.
6. Click **Start Free Trial**. An account confirmation screen appears.
7. Check your email inbox for your account activation link.
8. Click the account activation link in your email.
9. You can now [log in](#) to your Remote Manager account and [begin adding devices](#) to your device inventory.

## Log in to Remote Manager

After you have created your Remote Manager account, you can log in.

---

**Note** See [Create a Remote Manager account](#) for instructions on how to create an account.

---

1. In a web browser, type <https://remotemanager.digi.com>.
2. Type your login credentials in the **Username** and **Password** fields.

---

**Note** If you have forgotten your credentials, click **Forgot Username or Password** and follow the online instructions. See [Forgot user name or password](#).

---

3. Click **Log in**.

## Add a Connect IT to your inventory

This topic explains how to add a Connect IT to Remote Manager.

---

**Note** You can also add multiple devices using a CSV file. See [Add multiple devices using a CSV file](#).

---

1. [Log in to Remote Manager](#).
2. Click **Device Management > Devices**.
3. Click **Add Devices**. The **Add Devices** dialog appears.

4. For each device you want to add:
  - a. From the drop-down menu, select the device identifier type to use for the device: **MAC address**, **IMEI #**, or **Device ID**. Typically, you can find the MAC address or IMEI number on the device label.

---

**Note** If a device has both a MAC address and an IMEI #, you must use the MAC address to add the device.

---
  - b. Type in the device identifier.
  - c. In the **Install Code** field, enter the installation code found on the device label. If you attempt to add a device that requires an installation code with a missing or incorrect code, you receive an error message. For devices that were not manufactured with an associated installation code, the installation code is optional.
  - d. Click **Add**. The device is added to the device list box.
  - e. Repeat this process to add additional devices.
5. When you have finished entering devices, review the listed devices. If necessary, use **Remove** to [remove any incorrect entries](#).
6. Click **OK** to add all the listed devices to your Remote Manager inventory.
7. After a few minutes, click the refresh icon in the toolbar to refresh the device list. The new devices appear in your device inventory.
8. Information about the added device is saved in the event log. Click **Admin > Event Log** to display the [Event log view](#).

## Update the firmware on Connect IT from Remote Manager

You can update the firmware on Connect IT from Remote Manager. You must first get the current firmware file, and then you can upload it to the device.

1. [Download the Connect IT firmware to your PC](#).
2. [Log in to your Remote Manager account](#).
3. Click **Device Management**.
4. From the list of devices, click on the Connect IT for which you want to update the firmware.
5. In the toolbar, click **More > Update Firmware**. The **Update Firmware** dialog appears.
6. Click **Browse** to select the firmware file you just downloaded.
7. Click **Update Firmware** to immediately update the firmware.

---

**Note** By default, the firmware will update when you click the **Update Firmware** button. If you want to schedule when you want the update to occur, click the gear icon to display the options. See [Schedule an action](#) in the *Digi Remote Manager User Guide* for detailed information about the schedule options.

---

## View identifying information about the Connect IT on the Home page

You can display information about Connect IT in the **Home** page, such as the IP address, global address, and the Connect IT device ID. From this page you can also view the data stream and device file.

1. [Log into your Remote Manager account.](#)
2. Click the **Device Management** tab.
3. Click **Devices**.
4. From the list of devices, find the Connect IT for which you want to view identifying information.

---

**Note** You can use the search bar to search for the Connect IT by an identifier, such as the MAC address, device ID, or device type.

---

5. Double-click on the device or click **Properties** in the toolbar. The **Home** page for the Connect IT appears.

## Access the Remote Manager configuration page

You can display basic identification and version information about the selected Connect IT in the configuration **Home** page. You can also configure the device from this page.

---

**Note** The configuration options in Remote Manager are the same as the configuration options in the web user interface.

---

1. [Log into your Remote Manager account.](#)
2. Click **Device Management > Devices**.
3. Click **Devices**.
4. From the list of devices, click the Connect IT that you want to configure.
5. In the toolbar, click **Configure**.

As an alternative, click **Properties** in the toolbar and then from the **Home** page, click **Edit Device Configuration**.

6. The configuration **Home** page appears, and shows basic identification and version information about the selected Connect IT.

7. You can use the links in the toolbar to manage the Connect IT.
  - **Home:** Click **Home** to return to the configuration **Home** page.
  - **Config:** Click **Config** to display configuration menu options:
    - [Authentication](#)
    - [Central management](#)
    - [Firewall](#)
    - [Monitoring](#)
    - [Network](#)
    - [Serial](#)
    - [Services](#)
    - [System](#)
    - [VPN](#)
  - **Status:** Click **Status** to display a system status menu option:
    - [Communications](#)
    - [System](#)

## Schedule system maintenance from Remote Manager

You can schedule the system to run a set of system maintenance tasks to run within a specified time window. You can also schedule a custom script to run at the specified time and frequency.

---

**Note** If you are scheduling a custom script, you must have previously created the script.

---

For example, you can specify a start time of 10:00 and a duration window of 2 hours. In this example, the system maintenance can take place and custom scripts run at any time between 10:00 and 12:00.

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Config > System** in the toolbar. The **System** page appears.
4. Expand the **Schedule Tasks** section.

5. Configure a system maintenance task.
  - a. Expand the **System maintenance** section.
  - b. Enter the field values:

Field	Description
<p><b>Start time</b></p>	<p>The start time of the maintenance window. All enabled maintenance tasks take place at any random time within the time block specified in the <b>Duration window</b> field.</p> <p>If this field is empty, maintenance is not scheduled and no maintenance tasks will run.</p> <p><b>Syntax:</b> <i>HH:MM</i></p> <p>If the duration in the <b>Duration window</b> field is set to 1 or more hours, the minutes field is truncated.</p>
<p><b>Duration window</b></p>	<p>The window of time during which the maintenance tasks are scheduled to run. The default values is <b>2 hours</b>.</p> <ul style="list-style-type: none"> <li>■ <b>24 hours:</b> If this option is selected, the start time entered in the <b>Start Time</b> field becomes obsolete, as a value of 24 hours means the maintenance tasks are scheduled to run at any time during a 24-hour time period.</li> <li>■ <b>Immediately:</b> If this option is selected, all maintenance processes will execute at the same time. This could potentially be dangerous, as this action may stress the system.</li> </ul>
<p><b>Frequency</b></p>	<p>The frequency at which the modem firmware check and update tasks will run. The default value is <b>Daily</b>.</p> <ul style="list-style-type: none"> <li>■ <b>Daily:</b> The device runs the modem firmware check and update once a day within the given time window.</li> <li>■ <b>Weekly:</b> The device runs the modem firmware check and update any day within the given time window only once during the week.</li> </ul>

Field	Description
<b>Modem firmware update</b>	Select this option to enable the modem firmware update to be scheduled to occur within the specified maintenance window. The system looks for all available firmware over the air and in flash memory to see if an update is needed. If a newer firmware version is available, the update will occur.
<b>Configuration check</b>	Select this option to enable the system to check if configuration updates are scheduled to occur within the specified maintenance window. This check is in addition to the check defined in the <b>Central Management</b> section.

6. Configure a custom script to be run during the specified maintenance window
  - a. Expand the **Custom scripts** section.
  - b. Click the plus sign icon to specify a script. The section expands.
  - c. Running a custom script is enabled by default. Verify that the **Enable** slider is blue.
  - d. Complete the fields in each of the sections. You can hover over a field name to display information about what you should enter in each field.
7. Click **Apply** at the top of the screen to save the changes.

## Configure FIPS mode from Remote Manager

You can place the system into FIPS mode. In FIPS mode, the available services and methods for accessing the device is restricted to only those that are FIPS compliant.

---

**Note** Changing this setting erases configuration settings and also requires a reboot.

---

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Config > System** in the toolbar. The **System** page appears.
4. Click the **FIPS** option to enable FIPS mode. The slider is blue when it is selected.
5. Enter values into the fields.

Field	Description
<b>Name</b>	The name for the Connect IT. This name displays in prompts and log messages.
<b>Contact</b>	Contact information for this Connect IT.

Field	Description
<b>Location</b>	A description of the Connect IT's physical location
<b>Banner</b>	A banner message that displays when a user accesses terminal services on this device.

6. Click **Apply** at the top of the screen to save the changes.

## Configure VPN using Remote Manager

### Configure an IPsec tunnel for a VPN from Remote Manager

You can configure an IPsec tunnel for a VPN.

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Config > VPN** in the toolbar. The **VPN** page appears.
4. Expand the **IPsec** section.
5. Set the NAT keep alive time.
  - a. Expand the **advanced** section.
  - b. In the **NAT keep alive time** field, enter the length of time to keep NAT alive for IPSEC tunnels. the default is **40** seconds. The syntax for the entry is *number {w|d|h|m|s}*.
6. Create an IPsec tunnel.
  - a. Expand the **Tunnels** section.
  - b. Expand the **IPsec tunnel** section.
  - c. Click the plus sign icon to define an IPsec tunnel. The **Add IPsec tunnel** dialog appears.
  - d. Enter an IPsec tunnel name in the field.
  - e. Click **OK**.
  - f. The tunnel is enabled by default. Verify that the **Enable** slider is blue.
  - g. Complete the fields in each of the sections. You can hover over a field name to display information about what you should enter in each field.
7. Click **Apply** at the top of the screen to save the changes.

### Configure an OpenVPN server from Remote Manager

You can configure an OpenVPN server and client list.

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Config > VPN** in the toolbar. The **VPN** page appears.

4. Expand the **OpenVPN** section.
5. Define an OpenVPN server.
  - a. Expand the **Servers** section.
  - b. Expand the **OpenVPN server** section.
  - c. Click the plus sign icon to define an OpenVPN server. The **Add OpenVPN server** dialog appears.
  - d. Enter an OpenVPN server name in the field.
  - e. Click **OK**.
  - f. The tunnel is enabled by default. Verify that the **Enable** slider is blue.
  - g. Complete the fields in each of the sections. You can hover over a field name to display information about what you should enter in each field.
6. Create a client list for the OpenVPN server.
  - a. Expand the **Clients** section.
  - b. Expand the **OpenVPN client** section.
  - c. Click the plus sign icon to define a client. The **Add OpenVPN client** dialog appears.
  - d. Enter a client name in the field.
  - e. Click **OK**.
7. Click **Apply** at the top of the screen to save the changes.

## Configure an IP tunnel for a VPN from Remote Manager

You can configure an IP tunnel for a VPN.

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Config > VPN** in the toolbar. The **VPN** page appears.
4. Expand the **IP Tunnels** section.
5. Click the plus sign icon to define an IP tunnel. The **Add IP tunnel** dialog appears.
6. Enter an IP tunnel name in the field.
7. Click **OK**.
8. The tunnel is enabled by default. Verify that the **Enable** slider is blue.
9. Create an IP tunnel.
  - a. Expand the **Tunnels** section.
  - b. Expand the **IPsec tunnel** section.
  - c. Click **OK**.
  - d. The tunnel is enabled by default. Verify that the **Enable** slider is blue.
  - e. Complete the fields in each of the sections. You can hover over a field name to display information about what you should enter in each field.
10. Click **Apply** at the top of the screen to save the changes.



## View system status information from Remote Manager

You can display identifying information about the Connect IT and information about load average, disk usage, and RAM usage.

1. [Log into your Remote Manager account.](#)
2. [Access the Remote Manager configuration page.](#)
3. Click **Status > System** in the toolbar. The **System** page appears. Identifying information for the Connect IT displays at the top of the page.
  - Expand the **Load average** section to display the load average for the last 1, 5, and 15 minutes.
  - Expand the **RAM usage** section to display information about the percentage of RAM used.
  - Expand the **Disk usage** section to display various filesystem sections. You can expand each of the following sections to display information about the filesystem space used: **Config Filesystem**, **/opt Filesystem**, **/var Filesystem**, and **/tmp Filesystem**.

## View Connect IT summary dashboard

Remote Manager tracks connection history between a Connect IT and Remote Manager. You can a graph of the connection information. See [View Connect IT connection history](#) for detailed information.

1. [Log into your Remote Manager account.](#)
2. Click **Device Management**.
3. Click **Devices**.
4. From the list of devices, click on the Connect IT for which you want to view connection history.
5. Click **Properties** in the toolbar. The **Home** page for the Connect IT appears.
6. Click **Summary Dashboard** in the left pane. The connection history graph for the Connect IT displays.

## View Connect IT connection history

Remote Manager tracks and displays a detailed connection history between a Connect IT and Remote Manager. You can view connection and disconnection times, connection methods, and disconnect reasons. See [View Connect IT summary dashboard](#) for a graph of the connection history.

1. [Log into your Remote Manager account.](#)
2. Click **Device Management**.
3. From the list of devices, click on the Connect IT for which you want to view connection history.
4. Click **Properties** in the toolbar. The **Home** page for the Connect IT appears.
5. Click **Connection History** in the left pane. The connection history displays.

## Configure Connect IT using the web user interface

---

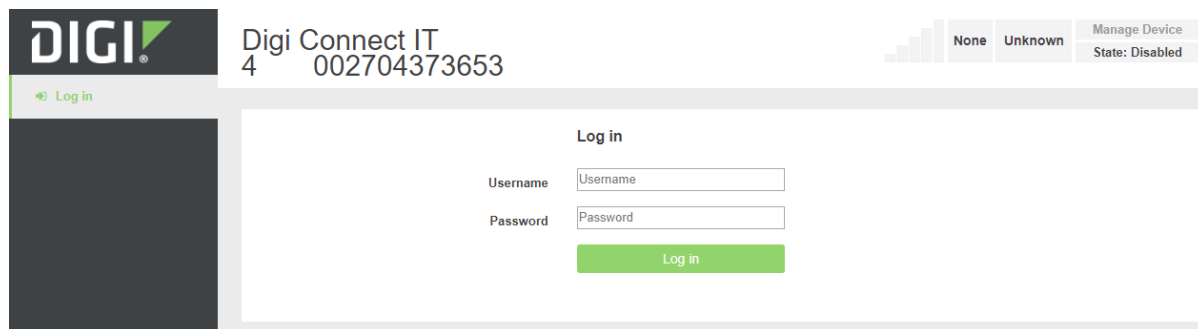
If your 4 is not provisioned in Remote Manager, you can use the web user interface which enables basic cellular connectivity (primary or backup) to your router. Your device operates as a transparent bridge and all traffic on all ports is passed directly to and from the equipment connected to the Connect IT's Ethernet port.

Log in to the Connect IT web UI .....	27
Manage users, groups, password, and two-factor authentication from the web UI .....	27
Update Connect IT firmware .....	33
Configure connection to Remote Manager from the web UI .....	33
Update modem firmware .....	34
Configure a serial port .....	34
Configure the modem in the Connect IT .....	39
Configure the network from the web UI .....	47
Configure FIPS mode from the web UI .....	47
Configure VPN from the web UI .....	48
Back up, restore, and delete the configuration .....	50
Configure the firewall from the web UI .....	50
Configure services from the web UI .....	51
Monitor the data from the Connect IT .....	52
Reboot from the web UI .....	53
Schedule system maintenance from the web UI .....	53
Synchronize system time from the web UI .....	55
View Connect IT status information .....	55
Download an archive of the supported MIBs .....	55
Download a support report file .....	56
Configure and view events and logs in the web UI .....	56

## Log in to the Connect IT web UI

To be able to access the web UI, your PC and the Connect IT must be connected by an Ethernet cable.

1. Connect your PC to the Connect IT with an Ethernet cable.
  - a. Connect one end of an Ethernet cable to your computer.
  - b. Connect the other end of the Ethernet cable to the LAN Ethernet port on the 4.
2. Open a web browser on your PC.
3. Type in the IP address for the Connect IT: 192.168.210.1
4. Press **Enter**. The login screen displays.



5. Enter the user name and password:
  - **User Name:** The default user name is: root
  - **Password:** The default password for the Connect IT is printed on the label attached to the device. Once you are logged in you can [change the password](#).
6. Click **Log in**. The Connect IT web user interface appears.

## Manage users, groups, password, and two-factor authentication from the web UI

You can manage the root user, add groups, and configure two-factor authentication.

### Configure idle timeout from the web UI

You can configure the length of time after which users are disconnected from services. If you do not enter a value, the idle timeouts feature is disabled, and the user will not be disconnected from services.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. In the **Idle timeout** field, enter the length of time after which users are disconnected from services. Leave this field blank to disable this feature.

**Syntax:** *number*{w|d|h|m|s}

5. Click **Save** at the bottom of the screen to save the changes.

## Add a new user from the web UI

You can add a new user.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Users** section.
5. In the **Add User** field, enter a unique user name.
6. Click **Add** to add the new user. The new user is immediately added to the list of users.
7. Click **Save** at the bottom of the screen to save the changes.

## Add a user group from the web UI

You can add a new group. After a group has been added, you can assign users to the group. The users assigned to the group have the rights specified for that group.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Groups** section.
5. In the **Add Group** field, enter the group name.
6. Click **Add**. The new group is immediately added to the list of groups.
7. A new user does not have access to any of the features on the Connect IT. See [Configure the user groups from the web UI](#) for configuration information.
8. Click **Save** at the bottom of the screen to save the changes.

## Configure the user groups from the web UI

You can configure the user groups with access to the desired serial ports and processes.

Two groups are available by default: **admin** and **serial**:

- **admin**: Users in this group have full access to all of the features on the Connect IT.
- **serial**: Users in this group have access to all serial ports by default.

When you [add a new user](#), you can allow access to the desired features.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Groups** section.

5. Expand the group that you want to configure.
6. Configure the group as desired.

Setting	Description
<b>Admin access</b>	<p>When selected, allows members assigned to this group to manage the Connect IT.</p> <hr/> <p><b>Note</b> Members will have full access to the Connect IT.</p> <hr/>
<b>Shell access</b>	<p>When selected, allows members of this group access a shell process on this Connect IT.</p> <hr/> <p><b>Note</b> Members will have full access to the Connect IT.</p> <hr/>
<b>Serial access</b>	<p>When selected, allows members of this group access to the set of ports listed in the <b>Serial ports</b> section.</p>
<b>Serial ports</b>	<p>A list of ports to which members of this group may access. The <b>Serial access</b> option must be selected for the users in this group to have access to the ports.</p> <ol style="list-style-type: none"> <li>a. Click <b>Add</b>. A new port row is added.</li> <li>b. From the <b>Port</b> list box, select the appropriate port.</li> </ol>
<b>OpenVPN access</b>	<p>When selected, allows members of this group access the specified OpenVPN tunnels listed in the <b>OpenVPN</b> section.</p>
<b>OpenVPN</b>	<p>A list of OpenVPN tunnels to which members of this group may access.</p> <p>The <b>OpenVPN access</b> option must be selected for the users in this group to have access to the tunnels. You must have previously <a href="#">added at least one OpenVPN tunnel</a>.</p> <ol style="list-style-type: none"> <li>a. Click <b>Add</b>. A new tunnel row is added.</li> <li>b. From the <b>Tunnel</b> list box, select the appropriate tunnel.</li> </ol>
<b>Nagios access</b>	<p>When selected, allows members of this group to query the device for service status for Nagios.</p>

7. Click **Save** at the bottom of the screen to save the changes.

## Change a Connect IT password from the web UI

You can change either the root password for the web UI on the Connect IT or the password a user would use to log onto the web UI.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Users** section.
5. Determine for whom you want to change the password.
  - Expand the **root** section to change the root password for the Connect IT.
  - Expand a section with a **user name** to change the password that user would use when logging on to the web UI on the Connect IT.
6. In the **Password** field, enter a new password.
7. Select the **Show** option if you want the password to display in the field. If you don't select this option, a series of dots displays.
8. Click **Save** at the bottom of the screen to save the changes. The next time the user logs in to the web UI, they will need to use the new password.

## Configure the user groups from the web UI

You can configure the user groups with access to the desired serial ports and processes.

Two groups are available by default: **admin** and **serial**:

- **admin**: Users in this group have full access to all of the features on the Connect IT.
- **serial**: Users in this group have access to all serial ports by default.

When you [add a new user](#), you can allow access to the desired features.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Groups** section.

5. Expand the group that you want to configure.
6. Configure the group as desired.

Setting	Description
<b>Admin access</b>	When selected, allows members assigned to this group to manage the Connect IT. <hr/> <b>Note</b> Members will have full access to the Connect IT. <hr/>
<b>Shell access</b>	When selected, allows members of this group access a shell process on this Connect IT. <hr/> <b>Note</b> Members will have full access to the Connect IT. <hr/>
<b>Serial access</b>	When selected, allows members of this group access to the set of ports listed in the <b>Serial ports</b> section.
<b>Serial ports</b>	A list of ports to which members of this group may access. The <b>Serial access</b> option must be selected for the users in this group to have access to the ports. <ol style="list-style-type: none"> <li>a. Click <b>Add</b>. A new port row is added.</li> <li>b. From the <b>Port</b> list box, select the appropriate port.</li> </ol>
<b>OpenVPN access</b>	When selected, allows members of this group access the specified OpenVPN tunnels listed in the <b>OpenVPN</b> section.
<b>OpenVPN</b>	A list of OpenVPN tunnels to which members of this group may access. The <b>OpenVPN access</b> option must be selected for the users in this group to have access to the tunnels. You must have previously <a href="#">added at least one OpenVPN tunnel</a> . <ol style="list-style-type: none"> <li>a. Click <b>Add</b>. A new tunnel row is added.</li> <li>b. From the <b>Tunnel</b> list box, select the appropriate tunnel.</li> </ol>
<b>Nagios access</b>	When selected, allows members of this group to query the device for service status for Nagios.

7. Click **Save** at the bottom of the screen to save the changes.

## Configure two-factor authentication from the web UI

You can configure two-factor authentication for a user. for user login.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Users** section.
5. Expand the group that you want to configure for two-factor authentication.
6. Expand the **Two-factor authentication** section.
7. Click **Enable**.
8. Complete the fields in the section. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
9. Click **Save** at the bottom of the screen to save the changes.

## Configure authentication methods from the web UI

You can configure a list of the authentication methods to use when authenticating access to services on the Connect IT. The methods are attempted in the list order until the first successful authentication result is returned. A user fails authentication when no method succeeds.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Authentication** section.
4. Expand the **Methods** section. One method is included by default. The **Local users** option is selected by default.
5. You can add additional methods.
  - a. Click **Add**. The new row is immediately added to the list of methods.
  - b. From the **Method** list box, select the method that you want to use for authentication:
    - **Local users**: Authenticate using the users defined with the configuration.
    - **TACACS+**: Authenticate using an external TACACS+ server. If you choose this option, make sure you have configured an external TACACS+ server, in [Step 6](#).
6. Configure an external TACACS+ server. This allows access to services on this Connect IT to be authenticated externally, which is useful for central management of users.

---

**Note** This step is required only if you chose the **TACACS+** option in [Step 5](#).

---

Expand each sub-section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.

7. Click **Save** at the bottom of the screen to save the changes.



## Update Connect IT firmware

You can update the firmware on the Connect IT. Before you begin, you must download the desired version of the firmware onto your PC.

1. [Download the Connect IT firmware to your PC.](#)
2. [Log in to the Connect IT web UI.](#)
3. Select the **System** tab in the left pane.
4. In the **Device Firmware** section, click **Choose File**.
5. Browse for and select the firmware file downloaded to your PC.
6. Click **Update Firmware**.

### Download the Connect IT firmware to your PC

1. Go to [www.digi.com/support](http://www.digi.com/support).
2. Scroll down to the **Support Downloads** section.
3. Click **Firmware Updates**.
4. In the **Filter the list** box, enter **Connect IT**. As you type, matches display.
5. Click **Connect IT**.
6. From the list of options, select the **Connect IT 4** option.
7. From the **Firmware Updates** section, select the version you want to download. The file is downloaded to a folder on your computer. Make a note of the folder path and name.

## Configure connection to Remote Manager from the web UI

You can configure the settings for connection to Remote Manager in the Connect IT web UI.

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **Central management** section.
  - a. Select the **Enable central management** option to enable Connect IT to connect to Remote Manager.
  - b. From the **Service** list box, select the **Digi Remote Manager** option.
  - c. In the **Management server** field, enter the URL for Remote Manager.
  - d. In the **Retry interval** field, enter the interval at which Connect IT should attempt to connect to Remote manager, after a disconnect. The time is measured in seconds.
  - e. In the **Keep-alive interval** field, specify how often to send keep-alive messages when using a non-cellular interface.
4. Click **Save**.
5. Disconnect the Ethernet cable from the Connect IT and your PC.

## Update modem firmware

You can update the modem firmware on the Connect IT. Before you begin, you must download the desired version of the modem firmware onto your PC.

1. [Download the Connect IT firmware to your PC.](#)
2. [Log in to the Connect IT web UI.](#)
3. Select the **System** tab in the left pane.
4. Scroll down to the **Modem Firmware** section.
5. Click **Choose File**.
6. Browse for and select the modem firmware file downloaded to your PC.
7. Click **Upload & Install Firmware**.

## Configure a serial port

You can configure the connection, determine if changes are monitored, and enable a TCP, Telnet, or SSH connection for each serial port. Each port must be individually configured.

### Configure the connection settings for a serial port

You can configure the serial ports on the Connect IT. Each port must be configured individually.

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **Serial** section.
4. Expand the port that you want to configure.
5. Configure the settings.

Setting	Description
<b>Enable</b>	Select the <b>Enable</b> option to enable this port for use. If it is not selected, the port won't work.
<b>Serial mode</b>	Select an access mode for this serial port. <ul style="list-style-type: none"> <li>■ <b>Login:</b> Select this option to display the <b>Login Manger</b> screen when you access the web UI.</li> <li>■ <b>Remote access:</b> Select this option to allow OOB management. This is the default.</li> </ul>
<b>Label</b>	The name of the serial port. If left blank, the default label is used. An entry is optional.
<b>Baud rate</b>	The baud rate for the serial port. This value must match the baud rate configuration for the equipment connected to the Connect IT. The default is <b>9600</b> .

Setting	Description
<b>Data bits</b>	The number of data bits for the serial port. This value must match the data bits configuration for the equipment connected to the Connect IT. The default is <b>8</b> .
<b>Parity</b>	The type of parity bit for the serial port. This value must match the parity bit configuration for the equipment connected to the Connect IT. The default selection is <b>NONE</b> .
<b>Stop bits</b>	The number of stop bits for the serial port. This value must match the stop bits configuration for the equipment connected to the Connect IT. The default is <b>1</b> .
<b>Flow control</b>	The type of flow control for the serial port. This value must match the flow control configuration for the equipment connected to the Connect IT. The default selection is <b>NONE</b> .
<b>Escape sequence</b>	The sequence of characters used to start an escape sequence. Escape sequences allow a user to send control commands to the serial port interface. These commands are removed from the data stream and are not sent to the equipment connected to the serial port. If left blank, the escape sequence is disabled. The default is a tilde (~). An entry is optional.
<b>History size</b>	The number of bytes from the serial port which should be buffered. The buffered bytes are redisplayed when a user connects to the serial port. The minimum value is 0. The default is <b>4000</b> .
<b>Exclusive access</b>	Select this option if access to the serial port should be limited to a single active session. If not selected, multiple active sessions are available on the port.
<b>Idle timeout</b>	The length of time after which the active session is disconnected after a period of user inactivity. Syntax: <i>number</i> {w h m s} A setting of <b>0</b> disables idle timeouts. The default is <b>15m</b> .

6. Click **Save**.

## Monitor serial port changes

You can choose to monitor CTS and/or DCD changes on the serial port.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.

3. Expand the **Serial** section.
4. Expand the port that you want to configure: **Port 1**, **Port 2**, **Port 3**, or **Port 4**.
5. Expand the **Monitor** section.
6. Configure the settings.


Setting	Description
<b>CTS</b>	Select the <b>CTS</b> option to monitor CTS changes on this port.
<b>DCD</b>	Select the <b>DCD</b> option to monitor DCD changes on this port.

7. Click **Save**.

### Enable a Telnet connection on the serial port

You can enable a Telnet connection on the serial port.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Serial** section.
4. Expand the port that you want to configure: **Port 1**, **Port 2**, **Port 3**, or **Port 4**.
5. Expand the **Telnet connection** section.
6. Configure the settings.

Setting	Description
<b>Enable</b>	<p>Select the <b>Enable</b> option to allow the serial port to be directly accessed by a Telnet connection.</p> <hr/> <div style="display: flex; align-items: center;">  <p><b>WARNING!</b> This connection is not authenticated or encrypted.</p> </div> <hr/>
<b>Port</b>	<p>Specify the Telnet port for the service.                      Minimum value: 1                      Maximum value: 65535                      Default: <b>2001</b></p>

7. Specify the addresses, interfaces, and firewall zones which are allowed to access the serial port. Expand the **Access control list**.


Setting	Description
<b>IPv4 Addresses</b>	Expand the <b>IPv4 Addresses</b> section to add IPv4 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.
<b>IPv6 Addresses</b>	Expand the <b>IPv6 Addresses</b> section to add IPv6 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.
<b>Interfaces</b>	Expand the <b>Interfaces</b> section to add network interfaces from which this serial port can be accessed. Click <b>Add</b> to add an interface.
<b>Zones</b>	Expand the <b>Zones</b> section to add firewall zones from which this serial port can be accessed. Click <b>Add</b> to add a zone.

8. Click **Save**.

### Enable a TCP connection on the serial port

You can enable a TCP connection on the serial port.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Serial** section.
4. Expand the port that you want to configure: **Port 1**, **Port 2**, **Port 3**, or **Port 4**.
5. Expand the **TCP connection** section.
6. Configure the settings.

Setting	Description
<b>Enable</b>	<p>Select the <b>Enable</b> option to allow the serial port to be directly accessed by a raw TCP connection.</p> <hr/> <div style="display: flex; align-items: center;">  <p><b>WARNING!</b> This connection is not authenticated or encrypted.</p> </div> <hr/>
<b>Port</b>	<p>Specify the TCP port for the service.                      Minimum value: 1                      Maximum value: 65535                      Default: <b>4001</b></p>

7. Specify the addresses, interfaces, and firewall zones which are allowed to access the serial port. Expand the **Access control list**.

Setting	Description
<b>IPv4 Addresses</b>	Expand the <b>IPv4 Addresses</b> section to add IPv4 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.
<b>IPv6 Addresses</b>	Expand the <b>IPv6 Addresses</b> section to add IPv6 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.
<b>Interfaces</b>	Expand the <b>Interfaces</b> section to add network interfaces from which this serial port can be accessed. Click <b>Add</b> to add an interface.
<b>Zones</b>	Expand the <b>Zones</b> section to add firewall zones from which this serial port can be accessed. Click <b>Add</b> to add a zone.

8. Click **Save**.

## Enable an SSH connection on the serial port

You can enable an SSH connection on the serial port.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Serial** section.
4. Expand the port that you want to configure: **Port 1**, **Port 2**, **Port 3**, or **Port 4**.
5. Expand the **SSH connection** section.
6. Configure the settings.

Setting	Description
<b>Enable</b>	Select the <b>Enable</b> option to allow the serial port to be directly accessed by anSSH connection.
<b>Port</b>	Specify the SSH port for the service. Minimum value: 1 Maximum value: 65535 Default: <b>3001</b>

7. Specify the addresses, interfaces, and firewall zones which are allowed to access the serial port. Expand the **Access control list**.

Setting	Description
<b>IPv4 Addresses</b>	Expand the <b>IPv4 Addresses</b> section to add IPv4 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.

Setting	Description
<b>IPv6 Addresses</b>	Expand the <b>IPv6 Addresses</b> section to add IPv6 addresses or networks from which this serial port can be accessed. Click <b>Add</b> to add an address.
<b>Interfaces</b>	Expand the <b>Interfaces</b> section to add network interfaces from which this serial port can be accessed. Click <b>Add</b> to add an interface.
<b>Zones</b>	Expand the <b>Zones</b> section to add firewall zones from which this serial port can be accessed. Click <b>Add</b> to add a zone.

8. Click **Save**.

## Configure the modem in the Connect IT

You can enable a modem in the Connect IT and configure the modem to enable gateways and network interfaces.

### Configure the modem

You can configure the modem in the Connect IT.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Modem** section.
4. Configure the settings.

Setting	Description
<b>Enable</b>	Select <b>Enable</b> to enable the network interface.
<b>Interface type</b>	The address configuration method for the network interface. <ul style="list-style-type: none"> <li>■ <b>Modem</b>: The address is determined by the cellular modem.</li> </ul> The default is <b>Modem</b> .
<b>Zone</b>	The firewall zone assigned to this network interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface. The default is <b>External</b> .
<b>Device</b>	The modem used by this network interface. The default is <b>Modem</b> .

Setting	Description
<p><b>Match SIM by</b></p>	<p>The match criteria to apply when determining if this interface should be used.</p> <ul style="list-style-type: none"> <li>■ <b>Any SIM:</b> Apply this interface to the modem with any SIM.</li> <li>■ <b>SIM slot:</b> Apply this interface when a specified SIM slot is active. An entry in the <b>Match SIM slot</b> field is required.</li> <li>■ <b>Carrier:</b> Apply this interface with SIM cards from a particular cellular carrier. An entry in the <b>Match SIM carrier</b> field is required.</li> <li>■ <b>PLMN identifier:</b> Apply this interface with SIM cards that have a specific PLMN identifier. An entry in the <b>Match PLMN identifier</b> field is required.</li> <li>■ <b>IMSI:</b> Apply this interface with SIM cards that have a specific IMSI. An entry in the <b>Match IMSI</b> field is required.</li> <li>■ <b>ICCID:</b> Apply this interface with SIM cards that have a specific ICCID. An entry in the <b>Match ICCID</b> field is required.</li> </ul>
<p><b>Match SIM slot</b></p>	<p>This conditional field displays when the <b>SIM slot</b> option is selected from the <b>Match SIM by</b> list box. Enter the SIM slot match criteria. The interface is applied when the modem is using this SIM slot. Modems with a single SIM slot will always match <b>SIM1</b>. The default value is <b>SIM1</b>.</p>
<p><b>Match SIM carrier</b></p>	<p>This conditional field displays when the <b>Carrier</b> option is selected from the <b>Match SIM by</b> list box. Select the appropriate SIM carrier from the list box. The interface is applied when the SIM card is provisioned from the carrier. The default value is <b>AT&amp;T</b>.</p>
<p><b>Match PLMN identifier</b></p>	<p>This conditional field displays when the <b>PLMN identifier</b> option is selected from the <b>Match SIM by</b> list box. Enter the SIM PLMN (Public Land Mobile Network) match criteria. The interface is applied when the SIM card is provisioned from the carrier with this PLMN carrier. The PLMN identifier consists of the Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).</p>



Setting	Description
<b>Match IMSI</b>	This conditional field displays when the <b>IMSI</b> option is selected from the <b>Match SIM by</b> list box. Enter the IMSI (International Mobile Subscriber Identity) match criteria. The interface is applied when the SIM card has this IMSI.
<b>Match ICCID</b>	This conditional field displays when the <b>ICCID</b> option is selected from the <b>Match SIM by</b> list box. Enter the ICCID (Integrated Circuit Card Identifier) match criteria. The interface is applied when the SIM card has this ICCID.
<b>PIN</b>	The PIN required to unlock the SIM card. Leave blank if not PIN is required.
<b>Phone Number</b>	The phone number stored on the SIM card will be automatically reported to enable SMS services. If the SIM is not provisioned with a phone number, or it contains an incorrect phone number, it will be necessary to complete this field with the correct phone number to reach this device. In normal operation, this field should be blank.
<b>Roaming</b>	Enable roaming to allow connections to data services outside of the original country of the SIM. When enabled, the cost of data use may increase significantly.
<b>Use DNS</b>	Specify when this interface's DNS servers will be used. <ul style="list-style-type: none"> <li>■ <b>Always:</b> Always use the DNS servers provided for this interface. If multiple interfaces have the same DNS server, requests to the DNS server will be routed through the interface with the lowest metric.</li> <li>■ <b>When primary default route:</b> Use the DNS servers provided for this interface only when the interface is the primary default route. This is the default.</li> <li>■ <b>Never:</b> Never use the DNS servers provided for this interface.</li> </ul>
<b>SIM failover</b>	Enable <b>SIM failover</b> to automatically switch the active SIM slot to the next available SIM if the modem interface fails to connect.
<b>Connection attempts before SIM failover</b>	The number of unsuccessful connection attempts before switching to the next SIM slot. Minimum value: <b>1</b> The default value is <b>5</b> .

Setting	Description
<b>SIM failover alternative</b>	<p>The action to perform when the connection retries have been exceeded but no other SIM is available to switch to.</p> <ul style="list-style-type: none"> <li>■ <b>None:</b> Perform no alternative action.</li> <li>■ <b>Reset modem:</b> Reset the modem if the <b>SIM failover</b> feature is not enabled and thus automatic SIM switching is not available.</li> <li>■ <b>Reboot device:</b> Reboot the device if the <b>SIM failover</b> feature is not enabled and thus automatic SIM switching is not available.</li> </ul>
<b>APN list only</b>	<p>Determine which APN should be used.</p> <ul style="list-style-type: none"> <li>■ <b>Enabled:</b> When enabled, the APN list is used exclusively.</li> <li>■ <b>Disabled:</b> When disabled, configured APNs are tried before the APNs built into the firmware are tried.</li> </ul>

5. Click **Save**.

## Define a custom APN

You can define a list of custom APNs to try when connecting to the cellular network.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **APN list** section.
4. Expand the **Modem** section.
5. In the **Add APN** field, enter the custom APN.
6. Click **Add**.
7. If the custom APN requires a specific user name and password, enter them in the **Username** and **Password** fields.
8. Click **Save**.

## Configure an IP passthrough for the modem

You can configure an IP passthrough. This is used to assign the address obtained from the cellular network to an external device using DHCP, rather than assigning it to the modem device in this Connect IT.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.

3. Expand the **Modem** section.
4. Expand the **Passthrough** section.
5. Configure the settings.

Setting	Description
<b>Enable</b>	Select <b>Enable</b> to enable IP passthrough for this network interface.
<b>Device</b>	The network device that the external device is connected to. The address from the cellular network will be assigned to the external device via DHCP, rather than being assigned to the modem device in this unit. Options are: <b>Loopback, LAN, or WAN.</b>
<b>Zone</b>	The firewall zone assigned to the passthrough network interface. This can be used by packet filtering rules and access control lists to restrict network traffic on the passthrough interface. Options are: <b>Any, Loopback, Internal, External, Setup, IPsec, Dynamic routes.</b>
<b>Packet filtering</b>	Enable firewall packet filtering rules for the passthrough network traffic. If this setting is disabled, then network traffic is allowed in both directions, and it is the responsibility of the external device to provide its own firewall.
<b>Allow all addresses</b>	Enable forwarding between the cellular network and any network/address connected using the passthrough device. This allows connected devices to forward and receive packets without NAT. Disable this option unless specifically required, as some cellular networks will disconnect modems that send packets that are not from the carrier-assigned IP address(es).
<b>Ancillary addressing</b>	When enabled, the ancillary address and gateway will be provided to the connected client while the passthrough modem is not connected.
<b>Ancillary address/netmask</b>	When the passthrough modem is not connected, the ancillary address/netmask will be provided to clients to allow functional local networking. <b>Syntax:</b> <i>IPv4_address/netmask</i> <b>Default:</b> 10.0.0.2/24

Setting	Description
<b>Ancillary gateway</b>	When the passthrough modem is not connected, the ancillary gateway will be provided to clients to allow functional local networking. <b>Syntax:</b> <i>IPv4_address/netmask</i> <b>Default:</b> 10.0.0.1
<b>Ancillary DNS redirect</b>	When the passthrough modem is not connected, the ancillary gateway will resolve all DNS requests to itself. HTTP traffic will be redirected to the device's web administration page.

6. Click **Save**.

### Configure a custom gateway for the modem

You can configure a custom gateway/netmask that overrides the automatic values normally provided. This is particularly useful when supporting a group of static UP addresses that communicate directly.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Modem** section.
4. Expand the **Custom gateway** section.
5. Configure the settings.

Setting	Description
<b>Enable</b>	Select <b>Enable</b> to enable a custom gateway for this network interface.
<b>Gateway/Netmask</b>	The gateway address and netmask to use for this network interface. If either the gateway address or the netmask is all 0's, it is not overridden. For example, 0.0.0.0/32 will operate as normal using the network-provided gateway IP, but with a /32 netmask.

6. Click **Save**.

### Configure an IPv4 network interface for the modem

You can configure an IPv4 network interface.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Modem** section.
4. Expand the **IPv4** section.
5. Configure the settings.

Setting	Description
<b>Enable</b>	Select <b>Enable</b> to enable an IPv4 network interface.
<b>Metric</b>	The priority of routes associated with the network interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used. <b>Default:</b> 3 <b>Minimum:</b> 0 <b>Maximum:</b> 65535
<b>Weight</b>	The relative weight of default routes associated with this network interface. If there are multiple active default routes with the same metric, then connections will be load-balanced between the default routes in proportion to their weight. <b>Default:</b> 10 <b>Minimum:</b> 1 <b>Maximum:</b> 65535
<b>Management priority</b>	The management priority assigned to this interface. An interface that is up and has the highest management priority will have its address reported as the preferred contact address for central management and direct device access. <b>Default:</b> 0 <b>Minimum:</b> 0 <b>Maximum:</b> 1000
<b>MTU</b>	Specify a desirable Maximum Transmission Unit (MTU) for this interface. If this is a non-static (DHCP) interface, the lower MTU value of the one offered by the DHCP and the one specified will be in effect. <b>Default:</b> 1500 <b>Minimum:</b> 576 <b>Maximum:</b> 65535
<b>Active recovery</b>	Active recovery performs regular network tests to determine if working connections can be made to remote targets. The network tests available are ping tests, HTTP/HTTPS tests, and DNS tests. This interface's default route will be disabled when the connectivity tests fail, allowing other interfaces with lower metrics to take precedence.

6. Click **Save**.

## Configure an IPv6 network interface for the modem

You can configure an IPv6 network interface.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.

3. Expand the **Modem** section.
4. Expand the **IPv6** section.
5. Configure the settings.

Setting	Description
<b>Enable</b>	Select <b>Enable</b> to enable an IPv4 network interface.
<b>Metric</b>	<p>The priority of routes associated with the network interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used.</p> <p><b>Default:</b> 3  <b>Minimum:</b> 0  <b>Maximum:</b> 65535</p>
<b>Weight</b>	<p>The relative weight of default routes associated with this network interface. If there are multiple active default routes with the same metric, then connections will be load-balanced between the default routes in proportion to their weight.</p> <p><b>Default:</b> 10  <b>Minimum:</b> 1  <b>Maximum:</b> 65535</p>
<b>Management priority</b>	<p>The management priority assigned to this interface. An interface that is up and has the highest management priority will have its address reported as the preferred contact address for central management and direct device access.</p> <p><b>Default:</b> 0  <b>Minimum:</b> 0  <b>Maximum:</b> 1000</p>
<b>MTU</b>	<p>Specify a desirable Maximum Transmission Unit (MTU) for this interface. If this is a non-static (DHCP) interface, the lower MTU value of the one offered by the DHCP and the one specified will be in effect.</p> <p><b>Default:</b> 1500  <b>Minimum:</b> 576  <b>Maximum:</b> 65535</p>
<b>Active recovery</b>	<p>Active recovery performs regular network tests to determine if working connections can be made to remote targets. The network tests available are ping tests, HTTP/HTTPS tests, and DNS tests. This interface's default route will be disabled when the connectivity tests fail, allowing other interfaces with lower metrics to take precedence.</p>

6. Click **Save**.

## Configure the network from the web UI

You can configure the network for the Connect IT.

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **Network** section.
4. Each sub-section enables you to configure a different network type. Expand the sub-section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.

Section	Description
<b>Interfaces</b>	Configure the interface types that you want to use.
<b>Virtual LAN</b>	A list of virtual LAN devices supporting the IEEE 802.1Q standard. These are virtual devices that are layered over an Ethernet device by including a VLAN tag within the Ethernet frame. The VLAN tag contains the VLAN identifier associated with the virtual LAN.
<b>Bridges</b>	A list of bridges supporting that IEEE 802.1D standard. A bridge learns which addresses are associated with devices on the bridge, and automatically forwards packets between devices as required. Bridged packets bypass the firewall.
<b>Routes</b>	Configure a list of the routing methods you want to use.
<b>Modems</b>	Settings for cellular modems. Each modem configuration describes the modem it applies to, and the settings for the modem.
<b>Dynamic DNS</b>	Dynamic DNS allows the IP address of a network interface to be registered with an external dynamic DNS service provider. This is useful when external systems need to initiate connections to this device, but the IP address assigned to the interface is not static.
<b>VRRP</b>	A list of VRRP (Virtual Router Redundancy Protocol) instances.
<b>Advanced</b>	Configure the ULA prefix for this site, and the TCP read and write buffer window size.

5. Click **Save** at the bottom of the screen to save the changes.

## Configure FIPS mode from the web UI

You can place the system into FIPS mode. In FIPS mode, the available services and methods for accessing the device is restricted to only those that are FIPS compliant.

---

**Note** Changing this setting erases configuration settings and also requires a reboot.

---

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **System** section.
4. Enter values into the fields.

Field	Description
<b>Name</b>	The name for the Connect IT. This name displays in prompts and log messages.
<b>Contact</b>	Contact information for this Connect IT.
<b>Location</b>	A description of the Connect IT's physical location
<b>Banner</b>	A banner message that displays when a user accesses terminal services on this device.

5. Click **Save** at the bottom of the screen to save the changes.

## Configure VPN from the web UI

### Configure an IPsec tunnel for a VPN from the web UI

You can configure an IPsec tunnel for a VPN.

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **VPN** section.
4. Expand the **IPsec** section.
5. Set the NAT keep alive time.
  - a. Expand the **advanced** section.
  - b. In the **NAT keep alive time** field, enter the length of time to keep NAT alive for IPSEC tunnels. the default is **40** seconds. The syntax for the entry is *number {w|d|h|m|s}*.
6. Create an IPsec tunnel.
  - a. Expand the **Tunnels** section.
  - b. In the **Add IPsec tunnel** field, enter a name for the tunnel.
  - c. Click **Add**.
  - d. The tunnel is enabled by default. Verify that the **Enable** option is selected.
  - e. Complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
7. Click **Save** at the bottom of the screen to save the changes.



## Configure an OpenVPN server from the web UI

You can configure an OpenVPN server and define clients.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **VPN** section.
4. Expand the **OpenVPN** section.
5. Define an OpenVPN server.
  - a. Expand the **OpenVPN** section.
  - b. Expand the **Servers** section.
  - c. In the **Add OpenVPN server** field, enter a name for the server.
  - d. Click **Add**.
  - e. The server is enabled by default. Verify that the **Enable** option is selected.
  - f. Complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
6. Define a client.
  - a. Expand the **Clients** section.
  - b. In the **Add OpenVPN client** field, enter a name for the client.
  - c. Click **Add**.
  - d. Verify that the **Enable** option is selected.
  - e. Verify that the **Use .ovpn** file option is selected.
  - f. Complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
7. Click **Save** at the bottom of the screen to save the changes.

## Configure an IP tunnel for a VPN from the web UI

You can configure an IP tunnel for a VPN.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **VPN** section.
4. Expand the **IP Tunnels** section.
5. In the **Add IP tunnel** field, enter a name for the tunnel.
6. Click **Add**.
7. The tunnel is enabled by default. Verify that the **Enable** option is selected.
8. Complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
9. Click **Save** at the bottom of the screen to save the changes.

## Back up, restore, and delete the configuration

You can back up, restore, or delete configuration settings for a Connect IT.

### Back up the Connect IT configuration

From the **System** page in the web UI, you can back up the Connect IT configuration file and save it to your PC. You can then use that file to [restore](#) the saved configuration to any Connect IT.

1. [Log in to the Connect IT web UI](#).
2. Click **System** in the left pane.
3. Scroll to the **Configuration Management** section.
4. In the **Passphrase** field, enter a password for the configuration file you are going to save. This is used when you restore the configuration file.
5. Click **Save Config**. The file is created and saved in the download folder on your PC.

### Restore the Connect IT configuration

From the **System** page in the web UI, you can restore a Connect IT configuration file that was previously [backed up](#).

This feature is useful if you want to copy the configuration from one Connect IT to others.

1. [Log in to the Connect IT web UI](#).
2. Click **System** in the left pane.
3. Scroll to the **Configuration Management** section.
4. In the **Passphrase** field, enter the password for the configuration file that you want to restore.
5. Click **Choose File** to select a configuration file that was previously [backed up](#).
6. Browse for and select the file. The file name appears in the page.
7. Click **Restore Config** to copy the configuration from the file to the Connect IT.

### Delete the Connect IT configuration

From the **System** page in the web UI, you can remove the Connect IT configuration.

1. [Log in to the Connect IT web UI](#).
2. Click **System** in the left pane.
3. Scroll to the **Configuration Management** section.
4. Click **Erase Config** to remove the configuration from the Connect IT.

## Configure the firewall from the web UI

You can configure the firewall for the Connect IT.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Firewall** section.

- Each sub-section enables you to configure a firewall component. Expand the sub-section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.

Section	Description
<b>Zones</b>	Configure the groups of network interfaces that can be referred to by packet filtering rules and access control lists.
<b>Port forwarding</b>	Configure a list of port forwarding rules. These rules allow network connections to the Connect IT to be forwarded to other servers by translating the destination address.
<b>Packet filtering</b>	Configure a list of packet filtering rules. These rules define whether to accept or reject network connections that are forwarded through the Connect IT.
<b>Custom rules</b>	Configure a script that is run to install advanced firewall rules beyond the scope or capabilities of the standard Connect IT configuration.
<b>Quality of Service</b>	Configure the quality of service, bandwidth allocation, traffic shaping, and traffic prioritizing features.

- Click **Save** at the bottom of the screen to save the changes.

## Configure services from the web UI

You can configure services for the Connect IT.

- [Log in to the Connect IT web UI.](#)
- Click **Configuration** in the left pane.
- Expand the **Services** section.
- Each sub-section enables you to configure a different service. Expand the sub-section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.

Section	Description
<b>Web administration</b>	The web administration service provides an HTTPS interface for managing the Connect IT.
<b>SSH</b>	The SSH service provides an SSH server for managing the Connect IT.

Section	Description
<b>Telnet</b>	The Telnet service provides a Telnet server for managing the Connect IT.  <b>Note</b> Telnet is an insecure protocol. It should only be used for compatibility reasons, and only if steps have been taken to ensure the network connection is secure.
<b>DNS</b>	The DNS service provides a caching DNS server. This server forwards queries to the DNS servers that are associated with the network interfaces, and caches the results.  <b>Note</b> This server is used within the Connect IT, and cannot be disabled. Use the access control list to restrict external access to this server.
<b>Remote control</b>	Not available.
<b>SNMP</b>	The SNMP service provides an SNMP agent for using SNMP management on this Connect IT.
<b>Multicast</b>	The multicast service provides a multicast route.

5. Click **Save** at the bottom of the screen to save the changes.

## Monitor the data from the Connect IT

You can configure the network for the Connect IT.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **Monitoring** section.
4. Each sub-section enables you to configure a different monitoring method. Expand the sub-section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.

Section	Description
<b>NetFlow probe</b>	Probe network traffic on this device and export statistics to NetFlow collectors.
<b>Device Health</b>	Device Health is a system monitor that collects and stores metrics over a period of time and reports them to Digi Remote Manager.
<b>intelliFlow</b>	Reserved for future use.

5. Click **Save** at the bottom of the screen to save the changes.

## Reboot from the web UI

You can choose to reboot the Connect IT immediately, or schedule a daily reboot.

### Immediately reboot the Connect IT

From the **System** page in the web UI, you can reboot the Connect IT. The device is immediately restarted.

---

**Note** You can also choose to schedule a daily reboot. See [Schedule a reboot from the web UI](#).

---

1. [Log in to the Connect IT web UI](#).
2. Click **System** in the left pane.
3. In the **Device Reboot** section, click **Reboot**.

### Schedule a reboot from the web UI

You can schedule the Connect IT to automatically reboot every day at a scheduled time.

---

**Note** You can also choose to reboot the Connect IT immediately. See [Immediately reboot the Connect IT](#).

---

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **System** section.
4. Expand the **Scheduled tasks** section.
5. In the **Reboot time** field, enter the time at which the Connect IT should reboot every day. If the Connect IT is unable to synchronize its time with an NTP server, the Connect IT automatically reboots after 24 hours of uptime. The syntax for this field is: *HH:MM*
6. Click **Save** at the bottom of the screen to save the changes.

## Schedule system maintenance from the web UI

You can schedule the system to run a set of system maintenance tasks to run within a specified time window. You can also schedule a custom script to run at the specified time and frequency.

---

**Note** If you are scheduling a custom script, you must have previously created the script.

---

For example, you can specify a start time of 10:00 and a duration window of 2 hours. In this example, the system maintenance can take place and custom scripts run at any time between 10:00 and 12:00.

1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **System** section.
4. Expand the **Scheduled tasks** section.
5. Enter values into the fields.

Field	Description
<b>Start time</b>	<p>The start time of the maintenance window. All enabled maintenance tasks take place at any random time within the time block specified in the <b>Duration window</b> field. If this field is empty, maintenance is not scheduled and no maintenance tasks will run.</p> <p><b>Syntax:</b> <i>HH:MM</i></p> <p>If the duration in the <b>Duration window</b> field is set to 1 or more hours, the minutes field is truncated.</p>
<b>Duration window</b>	<p>The window of time during which the maintenance tasks are scheduled to run. The default values is <b>2 hours</b>.</p> <ul style="list-style-type: none"> <li>■ <b>24 hours:</b> If this option is selected, the start time entered in the <b>Start Time</b> field becomes obsolete, as a value of 24 hours means the maintenance tasks are scheduled to run at any time during a 24-hour time period.</li> <li>■ <b>Immediately:</b> If this option is selected, all maintenance processes will execute at the same time. This could potentially be dangerous, as this action may stress the system.</li> </ul>
<b>Frequency</b>	<p>The frequency at which the modem firmware check and update tasks will run. The default value is <b>Daily</b>.</p> <ul style="list-style-type: none"> <li>■ <b>Daily:</b> The device runs the modem firmware check and update once a day within the given time window.</li> <li>■ <b>Weekly:</b> The device runs the modem firmware check and update any day within the given time window only once during the week.</li> </ul>
<b>Modem firmware update</b>	<p>Select this option to enable the modem firmware update to be scheduled to occur within the specified maintenance window. The system looks for all available firmware over the air and in flash memory to see if an update is needed. If a newer firmware version is available, the update will occur.</p>
<b>Configuration check</b>	<p>Select this option to enable the system to check if configuration updates are scheduled to occur within the specified maintenance window. This check is in addition to the check defined in the <b>Central Management</b> section.</p>

6. Configure a custom script to be run during the specified maintenance window.
  - a. Expand the **Custom Scripts** section.
  - b. Click **Add**.
  - c. Verify that the **Enable** option is selected.

- d. Complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field.
7. Click **Save** at the bottom of the screen to save the changes.

## Synchronize system time from the web UI

You can define the Connect IT time zone and specify the servers that should be used to synchronize its time.

1. [Log in to the Connect IT web UI.](#)
2. Click **Configuration** in the left pane.
3. Expand the **System** section.
4. Expand the **Time** section.
5. In the **Timezone** field, enter the time zone for the Connect IT's physical location. The time zone is used to adjust the time for logged messages and to start [scheduled system maintenance](#).
6. Specify the NTP servers used to synchronize the time on the Connect IT.
  - a. Expand the **NTP servers** section.
  - b. In the **Server** field, enter the name of the NTP server that is used to synchronize the time. The syntax is: `{hostname|UPv4_address|IPv6_address}`
  - c. If you want to enter an additional NTP server, click **Add** to add a new row and enter the NTP server name.
7. Click **Save** at the bottom of the screen to save the changes.

## View Connect IT status information

In the **Status** page in the web UI, you can view status information about the Connect IT, cellular modem, network connections, tunnels, and the equipment connected to the serial ports.

The **Status** page displays by default when you open the web UI.

1. [Log in to the Connect IT web UI.](#)
2. Click **Status** in the left pane.
3. Click the desired tab to display status information.
  - **Device Details:** Displays status information about the Connect IT.
  - **Cellular Details:** Displays status information about the cellular modem, cellular network connection, and the SIM cards.
  - **Networks:** Displays status information about the network interfaces and network devices.
  - **Tunnels:** Displays status information about open tunnels.
  - **Serial:** Displays information about the status of the serial ports.

## Download an archive of the supported MIBs

You can download a .zip archive of the MIBs supported by this device.

1. [Log in to the Connect IT web UI.](#)
2. Select the **System** tab in the left pane.
3. Scroll down to the **SNMP MIBs** section.
4. Click **Download MIBs**. The .zip archive file is downloaded to your downloads folder.

## Download a support report file

You can download a support report file for the Connect IT and include it with support requests.

1. [Log in to the Connect IT web UI.](#)
2. Select the **System** tab in the left pane.
3. Scroll down to the **Support Report** section.
4. Click **Download report**. The file is downloaded to your downloads folder.

## Configure and view events and logs in the web UI

You can configure and view events and log messages for a Connect IT.

### View events information

In the **Events** page in the web UI, you can view detailed information about events that have occurred. The type of event, level of activity, and a description is displayed.

1. [Log in to the Connect IT web UI.](#)
2. Click **Events** in the left pane.

Information	Description
<b>Type</b>	Describes the type of event. Options are: <ul style="list-style-type: none"> <li>■ network</li> <li>■ stat</li> <li>■ system</li> <li>■ firmware</li> <li>■ dhcpserver</li> </ul>
<b>Level</b>	Describes the level of the event. Options are: <ul style="list-style-type: none"> <li>■ status</li> <li>■ info</li> </ul>
<b>Information</b>	Includes a description of the event.

### Configure log messages from the web UI

You can configure the log messages for the Connect IT.



1. [Log in to the Connect IT web UI](#).
2. Click **Configuration** in the left pane.
3. Expand the **System** section.
4. Expand the **Log** section.
5. In the **Heartbeat** interval field, enter the minimum time interval between sending heartbeat status events. These events are only sent if no other events have been sent for this interval. If this field is blank, heartbeat events are disabled.
6. Configure log messages for individual event categories.
  - a. Expand the **Event categories** section.
  - b. For each category that you want to configure, expand the section and complete the fields in each of the sections. To display information about what you should enter in each field, click the down arrow and then **Help** next to each field
7. Click **Save** at the bottom of the screen to save the changes.

## View system log information

In the **System Logs** page in the web UI, you can view detailed debugging, warning, and critical messages.

1. [Log in to the Connect IT web UI](#).
2. Click **System Logs** in the left pane.
3. From the drop-down list box at the top of the screen, select the type of messages you want to view. By default, all messages are displayed.
  - **Select All:** All messages appear. This is the default.
  - **Critical messages:** Only critical messages appear. These display in red text.
  - **Warning messages:** Only warning messages appear. These display in blue text.
  - **Info messages:** Only informational messages appear. These display in black text.
  - **Debug messages:** Only debugging messages appear. These display in gray text.

## Troubleshooting

---

Cellular network fallback .....	59
Reset your device to the factory defaults .....	59
Tips for improving cellular signal strength .....	59
Download a support report .....	59

## Cellular network fallback

If the Connect IT 4 doesn't recognize the available 4G/LTE network, the Connect IT 4 automatically falls back to the highest available 3G network.

## Reset your device to the factory defaults

You can reset the Connect IT to the factory default settings. Resetting the device to factory defaults performs the following actions:

- Clears all configuration settings.
- All firmware updates are deleted.
- Deletes all user files, including Python scripts.
- Regenerates SSH keys.
- Clears event and system log files.
- Creates a new event in the event log, indicating a factory reset.

---

**Note** While the settings are reset, the device's firmware version remains the same.

---

1. Make sure that the Connect IT has been powered on for at least 30 seconds.
2. Locate the **ERASE** button on the right side of the device.
3. Locate the **ERASE** button on the back of the device.
4. Press and hold the **ERASE** button for 5 seconds. The device beeps five times during the reset.
5. The device resets to factory defaults and then reboots automatically.

## Tips for improving cellular signal strength

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

- If available, connect a different set of antennas.
- Purchase a Digi Antenna Extender Kit: [Antenna Extender Kit, 1 m](#).

## Download a support report

You can download a support report from the device to provide to technical support. The report file contains all of the current details for the device's state, and a full record of the system logs from the device.

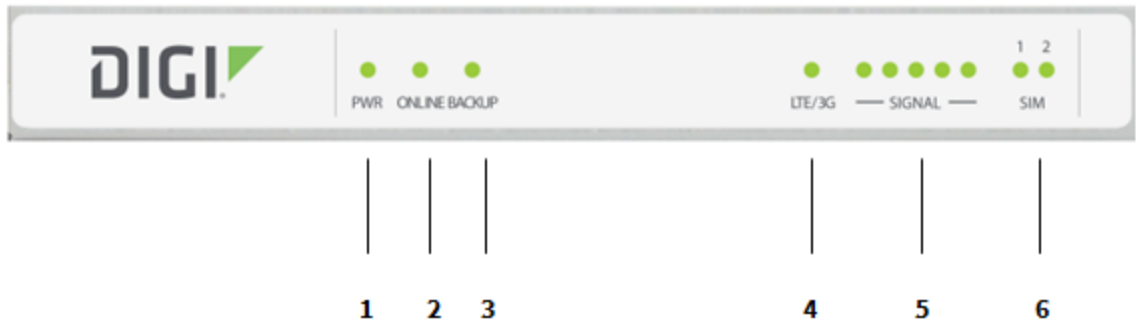
See [Download a support report file](#).

# Hardware

## Connect IT 4 hardware and LEDs

This section includes details about the front and back panels.

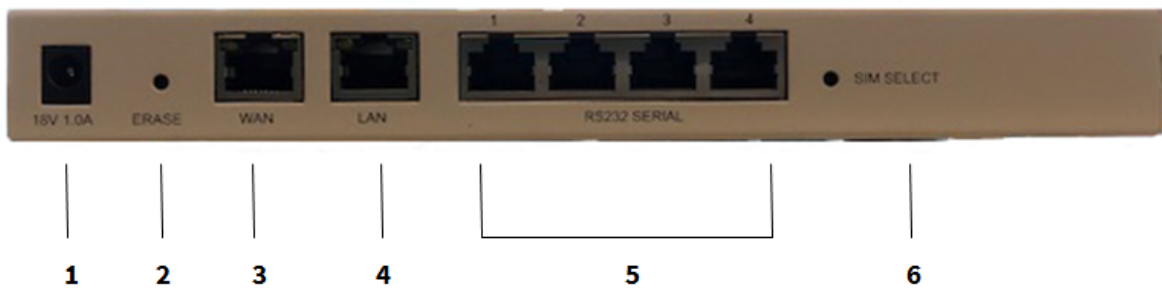
### Front panel and LEDs



Item	Name	Description
1	PWR	Indicates whether unit is powered up. This LED is hardwired to the power input.
2	ONLINE	Indicates status of the cellular network connection. <ul style="list-style-type: none"><li>■ Flashing: The unit is attempting to establish a cellular network connection.</li><li>■ Solid: A cellular connection has been established.</li></ul>
3	BACKUP	Indicates the status of the backup connection on the LAN. <ul style="list-style-type: none"><li>■ Flashing: The unit is attempting to establish a backup connection on the LAN.</li><li>■ Solid: A backup network connection has been established on the LAN.</li></ul>

Item	Name	Description
4	LTE/3G	Indicates a 4G\LTE or 2G/3G connection. See <a href="#">Cellular network fallback</a> .
5	SIGNAL	Indicates the cellular network signal strength. See <a href="#">Signal strength</a> .
6	SIM 1 SIM 2	Indicates which SIM has been selected, using the SIM SELECT button on the back of the unit. See <a href="#">Select SIM card</a> .

### Back panel








Item	Name	Description
1	Power	Connect the power supply unit to the device. For information about exchanging the power tips, see <a href="#">Exchange power tips</a> .
2	Erase	Press this switch to reset the device. See <a href="#">Reset your device to the factory defaults</a> .
3	WAN	Indicates connection to Ethernet network. See <a href="#">Connect hardware and connect to site network using an Ethernet LAN</a> .
4	LAN	Connect to an Ethernet port to establish backup connectivity, LAN connectivity using passthrough\bridge mode or DNCHP server\router mode.
5	Serial ports	Connect equipment to a serial port to provide console access to the equipment through the cellular network. See <a href="#">Connect equipment to the Connect IT serial ports</a> .
6	SIM SELECT	Use the SIM SELECT button to select a SIM card: 1 or 2. See <a href="#">Select SIM card</a> .

## Signal strength

The signal bars show the strength of the cellular network connection.

See [Cellular network fallback](#).

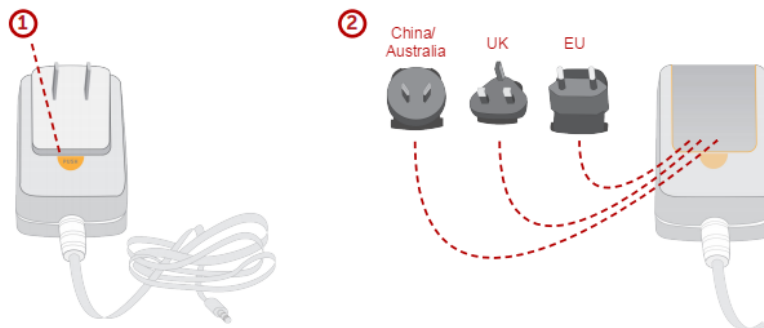
Signal Bars	dBm	Signal Strength Percent	Quality
	-110 to -106	0-11%	Bad
	-105 to -96	12-28%	Marginal
	-95 to -84	29-47%	OK
	-83 to -76	48-60%	Good
	-75 to -50	61-100%	Excellent

## Exchange power tips

The 4 may include four interchangeable plug tips that allow the Power Supply Unit (PSU) to operate in most countries. The PSU comes with the United States style plug installed.

To change the plug tip:

1. Place the tip of a small flathead screw driver in the half-circle area below the power prongs, and push in and upward.
2. Pull off the attached plug converter.
3. Slide the new tip down into place until it clicks.



**Note** For more information regarding power-tip compatibility with global deployments, visit [www.worldstandards.eu/electricity/plugs-and-sockets/](http://www.worldstandards.eu/electricity/plugs-and-sockets/).

## Select SIM card

You can use the SIM button on the back of the unit to select which SIM card you want to use: first or second.

1. Power on the unit.
2. Press the SIM SELECT button on the back of the unit.
3. On the front of the device, verify which SIM LED is illuminated: SIM 1 or SIM 2.
  - If the LED for the desired SIM LED is illuminated, the process is complete.
  - If the LED for the desired SIM LED is not illuminated, press the SIM SELECT button again. Verify that the desired SIM LED is illuminated.

## Regulatory and safety information

---

### FCC certifications

#### USA

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference as his own expense.

#### INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A)

This product is intended for operation in a commercial or industrial environment and should not be used in a residential environment. This product has been tested and found to comply with the requirements of:

ICES-003 -- Information Technology Equipment--Limits and Methods of Measurement Issue 5, August 2012

#### European Union

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

### Safety warnings

Review the following safety warnings for Connect IT.



**WARNING!** To comply with FCC/IC RF exposure limits at least 20 cm separation distance must be maintained between any antenna of the unit and any part of the user at all times.

---





**WARNING!** The unit must be powered off where blasting is in progress, where explosive atmospheres are present, or near medical or life support equipment. Do not power on the unit in any aircraft.



**WARNING!** CA Prop 65 warning: This product contains chemicals known to the state of California to cause cancer, birth defects or other reproductive harm.

---

**WARNING!**הוראות בטיחות לשימוש במטעןמטענים:

- יש לפעול ע"פ כללי הבטיחות הבאים בעת שימוש במטענים:
- ודא שלמות ותקינות כבל החשמל והתקע.
  - אין להכניס או להוציא את התקע מרשת החשמל בידיים רטובות
  - אין לפתוח את המטען, במקרה של בעיה כלשהי, יש לפנות למעבדת השירות הקרובה
  - יש להרחיק את המטען מנחלים
  - במקרה של ריח מוזר, רעשים שמקורם במטען, יש לנתקו מיידית מרשת החשמל ולפנות למעבדת שירות
  - המטען מיועד לשימוש בתוך המבנה בלבד, לא לשימוש חיצוני ולא לשימוש בסביבה לחה
  - אין לחתוך, לשבור, ולעקם את כבל החשמל
  - אין להניח חפצים על כבל החשמל או להניח לו להתחמם יתר על המידה, שכן הדבר עלול לגרום לנזק, דליקה או התחשמלות
  - לפני ניקוי המטען יש לנתקו מרשת החשמל
  - יש להקפיד לתחזק את התקן הניתוק במצב תפעולי ומוכן לשימוש
- אזהרה:
- אין להחליף את כבל הזינה בתחליפים לא מקוריים, חיבור לקוי עלול לגרום להתחשמלות המשתמש
  - בשימוש על כבל מאריך יש לוודא תקינות מוליך הארקה שבכבל
  - מיועד לשימוש פנימי בלבד



**CAUTION!** Do not use an antenna that wasn't supplied by the manufacturer. If a different antenna is required, first consult Digi International Inc. for recommendations that suit your circumstances.



**CAUTION!** By pressing the ERASE button when powered up, the configuration of the Digi Connect IT 4 is **erased** and the unit reverts to factory default settings.