Digi IX14

User Guide

Revision history—90002291

Revision	Date	Decription
A	January 2019	Initial release.

Trademarks and copyright

Disclaimers

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

Warranty

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

www.digi.com/howtobuy/terms

Customer support

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

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

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

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi IX14 User Guide, 90002291 A) in the subject line of your email.

Notes, cautions, and warnings

WARNING! To comply with FCC/IC RF exposure limits, maintain at least a **20** cm distance between any Digi IX14antennas and any user at all times.

WARNING! CA PROP 65: This product contains chemicals designated by the state of California to cause cancer, birth defects, or harm to human reproduction.

WARNING! This device must be powered off where blasting in progress, where explosive atmospheres are present, or near medical or life support equipment.

CAUTION! Do not use an antenna not supplied by Digi. If a different antenna is required, consult Digi for antenna recommendations for your environment.

CAUTION! When you use the **Reset** button to reset the device, the current configuration is removed and the Digi IX14 reverts to factory default settings.

Restricted access location notice for Digi IX14

WARNING! Installations with operating temperatures greater than **64° C** (**147° F**) must be limited to **Restricted Access Locations** accessible only to trained service personnel.

ATTENTION! Les installations dont la température de fonctionnement est supérieure à 64 ° C (147 ° F) doivent être limitées aux emplacements d'accès restreint accessibles uniquement au personnel de service qualifié.

WARNING! Hot surface. Do not touch.
ATTENTION! Surface chaude. Ne pas toucher.

Regulatory and safety statements

RF exposure statement

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antenna or antennas and the user should not be less than **20 cm**.

Federal Communication (FCC) Part 15 Class B

Radio Frequency Interference (RFI) (FCC 15.105)

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet that is on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC ID: MCQ-CCIMX6UL and FCC ID: RI7LE910NAV2

If the FCC ID is not visible when installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module FCC ID.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Digi may void the user's authority to operate this equipment.

Digi IX14 Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for Digi IX14 concerning emissions, EMC, and safety. For more information, see www.digi.com/resources/certifications.

Important note

Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

CE mark (Europe)

The Digi IX14 is certified for use in several European countries. For information, visit www.digi.com/resources/certifications.

If the Digi IX14 is incorporated into a product, the manufacturer must ensure compliance of the final product with articles 3.1a and 3.1b of the RE Directive (Radio Equipment Directive). A Declaration of Conformity must be issued for each of these standards and kept on file as described in the RE Directive (Radio Equipment Directive)

Furthermore, the manufacturer must maintain a copy of the Digi IX14 user manual documentation and ensure the final product does not exceed the specified power ratings, antenna specifications, and/or installation requirements as specified in the user manual. If any of these specifications are exceeded in the final product, a submission must be made to a notified body for compliance testing to all required standards.

Maximum power and frequency bands

Max power	Frequencies
2 W	Cellular 850 and 900 MHz bands
1 W	Cellular 1800 and 1900 MHz bands
63.1 mW	13 overlapping channels each 22 or 40 MHz wide and spaced at 5 MHz. Centered at 2.412 to 2.472 MHz
31.62 mW	165 overlapping channels, each 22 or 40 MHz wide and spaced at 5 MHz. Centered at 5180 to 5825 MHz.

Innovation, Science, and Economic Development Canada (IC) certifications

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications. This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Contains IC: 1864A-CCIMX6UL and IC: 5131A-LE910NAV2

Le present appareil numerique n’emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class B prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Safety notices

- Read all instructions before installing and powering the router. You should keep these instructions in a safe place for future reference.
- If the power supply shows signs of damage or malfunction, stop using it immediately, turn off the power and disconnect the power supply before contacting your supplier for a repair or replacement.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Use only the accessories, attachments, and power supplies provided by the manufacturer-connecting non-approved antennas or power supplies may damage the router, cause interference or create an electric shock hazard, and will void the warranty.
- Do not attempt to repair the product. The router contains no electronic components that can be serviced or replaced by the user. Any attempt to service or repair the router by the user will void the product warranty.
- Ports that are capable of connecting to other apparatus are defined as SELV ports. To ensure conformity with IEC60950 ensure that these ports are only connected to ports of the same type on other apparatus.

Special safety notes for wireless routers

Digi International products are designed to the highest standards of safety and international standards compliance for the markets in which they are sold. However, cellular-based products contain radio devices which require specific consideration. Take the time to read and understand the following guidance. Digi International assumes no liability for an end user's failure to comply with these precautions.

Wireless routers incorporate a wireless radio module. Users should ensure that the antenna(s) is (are) positioned at least 1 meter away from themselves and other persons in normal operation.
When in a hospital or other health care facility, observe the restrictions on the use of mobile phones. Do not use the router in areas where guidelines posted in sensitive areas instruct users to switch off mobile phones. Medical equipment may be sensitive to RF energy.
The operation of cardiac pacemakers, other implanted medical equipment and hearing aids can be affected by interference from cellular terminals such as the wireless routers when places close to the device. If in doubt about potential danger, contact the physician or the manufacturer of the device to verify that the equipment is properly shielded. Pacemaker patients are advised to keep the wireless router away from the pacemaker while it is on.

Wireless routers must NOT be operated on aircraft. The operation of wireless appliances in an aircraft is forbidden to prevent interference with communications systems. Failure to observe these instructions may lead to the suspension or denial of cellular services to the offender, legal action, or both.

As with any electrical equipment, do not operate the router in the presence of flammable gases, fumes or potentially explosive atmospheres. Do not use radio devices anywhere that blasting operations occur.

Wireless routers receive and transmit radio frequency energy when power is on. Interference can occur when using the router close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always power off your router wherever forbidden or when it may cause interference or danger.

SOS IMPORTANT! Wireless routers operate using radio signals and cellular networks cannot be guaranteed to connect in all possible conditions. Therefore, never rely solely upon any wireless device for life critical communications.

For environments where the temperature is 64° C or above, this device must be installed in a restricted access area.

Product disposal instructions

The WEEE (Waste Electrical and Electronic Equipment: 2002/96/EC) directive has been introduced to ensure that electrical/ electronic products are recycled using the best available recovery techniques to minimize the impact on the environment.

This product contains high quality materials and components which can be recycled. At the end of its life this product MUST NOT be mixed with other commercial waste for disposal. Check with the terms and conditions of your supplier for disposal information.

Digi International Ltd WEEE Registration number: WEE/HF1515VU

Certifications

This product complies with the requirements of the following Electromagnetic Compatibility standards.

There are no user-serviceable parts inside the product. Contact your Digi representative for repair information.

Certification category	Standards
Electromagnetic Compatibility (EMC) compliance standards	■ EN 300 328 v1.8.1 ■ EN 301-489-17 V3.1.12017 ■ EN 301-489-52 V1.1.0:2016 ■ FCC Part 15 Subpart B Class B
Safety compliance standards	EN 60950-1, CSA 22.2 EN 62368-1
Environmental	MIL-STD-810G
Cellular carriers	See the current list of carriers on the Digi IX14 datasheet, available on the Digi IX14 product page.

Contents

Initial configuration

Authentication

System administration

Services and applications

Run Python applications

Digi Remote Manager

Monitoring

Virtual private networks (VPNs)

Diagnostics

Welcome

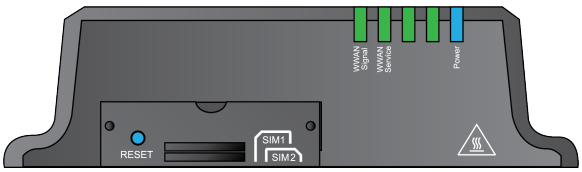
Digi IX14 features and specifications

Digi IX14 is a compact LTE CAT1 machine-to-machine (M2M) router suitable for a broad range of applications in rugged industrial environments. Key features include:

- Industrial grade components (operating temperatures from -29° F to +165° F/-34° C to +74° C)
- LTE Category 1 cellular network speed up to 10 Mbps
- LAN speed 10/100 BaseT

See Digi IX14 product page for details.

Digi IX14 front view



Connector/port	Description
SIM door	See Install SIM cards.
Reset button	See Reset to factory default settings using Reset button.
LEDs	See Digi IX14 LEDs.

Digi IX14 back view

Port/connector	Description
WAN/ETH1	See Connect the WAN/ETH1 port.
SERIAL1	See Connect the serial port and Configure serial interfaces.
Power	See Power on the Digi IX14.
WWAN1-1 **WWAN1-2**	See Attach and position antennas.

Digi IX14 LEDs

Power

Solid blue
Initial power on as router prepares to boot up

Flashing blue
Router is booting up

Solid blue
Router bootup is complete when flashing stops

WWAN signal

Solid red
Very Poor signal (-113 dBm to -99 dBm)

Solid orange
Poor signal (-98 dBm to -87 dBm)

Solid yellow
Fair signal (-86 dBm to -76 dBm)

Solid light green
Good signal (-75 dBm to -64 dBm)

Solid green
Excellent signal. (-63 dBm to -51 dBm)

WWAN service

Off
No cellular service

Flashing yellow
Cellular connection coming up

Solid yellow
Connected to 2G or 3G

Solid green
Connected to 4G

WAN/ETH1 port

Solid yellow
100 Mbps connection; Off for no connection

Solid green
Valid link detected; Flashing for Ethernet activity

Digi IX14 power supply requirements

Digi IX14 is intended to be powered by a certified power supply with output rated at either 12 VDC/0.75 A or 24 VDC/0.375 A minimum.

- If the Digi IX14 is operated in an ambient temperature range from +0 C to +40 C, use the Digi power supply accessory kits 76002078 or 76002080 to meet the temperature criteria.
- If the Digi IX14 is operated in an ambient temperature range from -34 C to +74 C, use the Digi power supply accessory kits 76002079 or 76002081 to meet the temperature criteria.
- If you are providing the DC power source with a non-Digi power supply, you must use a certified LPS power supply rated at either 12 VDC/0.75 A or 24 VDC/0.375 A minimum. The voltage tolerance supports +/- 10% (9 VDC to 30 VDC) at 9 Watts minimum.

Digi IX14 serial pinout

The Digi IX14 is a DTE device. The pinout for the DB9 serial connector is as follows:

Signal name	RS232 signal	DTE signal direction	DB male 9 pin number
Transmit Data	TxD	In	3
Receive Data	RxD	Out	2
Ready To Send	RTS	In	7
Clear to Send	CTS	Out	8
Data Set Ready	DSR	Out	6
Ground	GND	N/A	5
Data Carrier Detect	DCD	Out	1
Data Terminal Ready	DTR	In	4
Ring Indicate	RI	Out	9

Digi IX14 accessory kits

Digi offers the following Digi IX14 accessories and accessory kits:

Digi part number	Description
76002078	Power supply: Standard temp AC/DC power
76002079	Power supply: Extended temp AC/DC power supply
76002080	Accessory kit Standard temp AC/DC power supply Ethernet cable Cellular antennas (2)
76002081	Accessory kit: Extended temp AC/DC power supply Ethernet cable Cellular antennas (2)

See Digi IX14 product page and click **Part numbers and accessories** for details.

Digi IX14 antennas

Digi IX14 obtained complete certification by using the antenna described here. Use an antenna that matches these specifications to maintain the product certification. You can use antennas of the same type but operating with a lower gain.

Attribute	Property
Frequency Range	699 MHz to 2690 MHz
Impedance	50 Ohm
VSWR	≤ 3:1
Gain	3 dBi (0 dBi at 900 MHz)
Polarization	Linear
Admitted Power	> 24 dBm

Digi IX14 quick start

Congratulations on your Digi IX14 purchase. Begin by selecting how you want to get started.

- **Quick start with Digi Remote Manager mobile app**

  If you have a smart phone or tablet, use the Digi Remote Manager mobile app to quickly set up your Digi IX14. Go to Quick start with Digi Remote Manager mobile app.

- **Quick start with Digi IX14 local web UI**

  If you do not have a smart phone or tablet, access the Digi IX14 local web UI to manually set up your Digi IX14. Go to Quick start with Digi IX14 local web UI.

Quick start with Digi Remote Manager mobile app

Congratulations on your Digi IX14 purchase. The following steps guide you through Digi IX14 setup using the Digi Remote Manager mobile app.

Note If you do not have a smart phone or tablet, access the Digi IX14 local web UI to manually set up your Digi IX14. Go to Quick start with Digi IX14 local web UI.

Step 1: What's in the box

When you open the Digi IX14 package, look for the following:

- **Welcome card**

  Links to this *Quick start*.

- **Digi IX14**

  Provides a product label on the bottom of the device. The label includes product identification information and the default password assigned to the device.

- **Digi IX14 label**

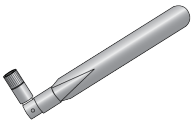
  Printed copy of the product label on the bottom of your device. You can affix this label to the top or side of the device such that you can access the label after the device is mounted or store the label in a safe place for future reference.

Note A subscription to **Digi Remote Manager** is bundled with your Digi IX14 purchase. See Digi Remote Manager product page to learn about Digi Remote Manager features.

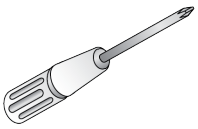
Step 2: Gather accessories

Note Digi offers several Digi IX14 accessory kits so you can purchase exactly what you need to support your Digi IX14. See Digi IX14 accessory kits for details or go to Digi IX14 support.

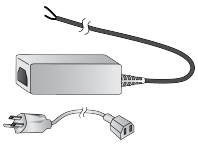
Here's the list of accessories used in this ***Quick start***:



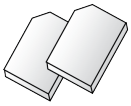
Antennas
Use antennas provided by a Digi accessory kit or use alternate antennas that comply with the Digi IX14 antenna requirements.



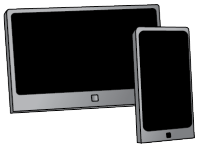
Phillips-head screwdriver
Use a #1 Phillips-head screwdriver to remove and replace the SIM door when installing SIM cards.



Power supply
Use a power supply provided by a Digi accessory kit or use an alternate power supply that complies with the power supply requirements.



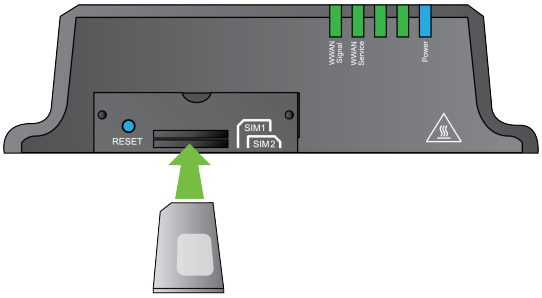
SIM card(s)
Acquire SIM cards as needed. Note the carrier, network APN (Access Point Name), and SIM pin (if any) for each card.



Smart phone or tablet
Use a smart phone or tablet to automatically register your Digi IX14 in your Digi Remote Manager account and connect to your cellular network.

Step 3: Connect hardware

a. Install SIM card(s). See Install SIM cards.

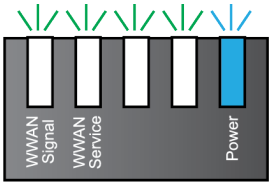


b. Attach antenna(s). See Attach and position antennas.

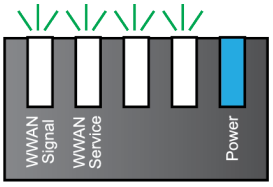
c. Power on the Digi IX14 by connecting a DC power source. See Digi IX14 power supply requirements.

d. Power LED is solid blue as the device prepares to boot up.

e. Power LED flashes blue as the device boots up.



Power LED is solid blue when the Digi IX14 is ready.



Step 4: Quick setup using the Digi Remote Manager mobile app

Use the Digi Remote Manager mobile app to:

- Register your device in your Digi Remote Manager account using the QR code on the Digi IX14 label.
- Configure your Digi IX14 cellular interface.
- Connect your device to Digi Remote Manager using the cellular connection.

Here's how:

a. Download the **Digi Remote Manager** mobile app from the **App Store** (iPhone) or **Google Play** (Android).

b. Click **Log in or Sign Up** and then click **Sign up** to create a new account.

c. You'll receive an email with login instructions.

d. From the **Digi Remote Manager** mobile app, click **Log in** and log into your new account.

e. From the menu, select **Install a device with a QR or bar code** and scan the installation QR code on the label.

Best practice for bluetooth Position your tablet or phone in front of the Digi IX14. The Digi IX14 does not appear in your mobile OS bluetooth settings—the Digi IX14 bluetooth connection status displays within the **Digi Remote Manager** mobile app only.

f. Follow the prompts to complete your Digi IX14 registration, configure your cellular connection, and connect your Digi IX14 to **Digi Remote Manager**.

Next steps

Congratulations! You have completed the Quick start.

- To manage and configure your Digi IX14 remotely using Digi Remote Manager, see Digi Remote Manager.
- To manage and configure your Digi IX14 locally using the local web interface, see Access the Digi IX14 local web UI.

Quick start with Digi IX14 local web UI

Congratulations on your Digi IX14 purchase. The following steps guide you through the Digi IX14 setup using the Digi IX14 local web UI.

Note If you have a smart phone or tablet, you can use the Digi Remote Manager mobile app to quickly set up your Digi IX14. Go to Quick start with Digi Remote Manager mobile app.

Step 1: What's in the box

When you open the Digi IX14 package, look for the following:

- **Welcome card**

  Links to this *Quick start*.

- **Digi IX14**

  Provides a product label on the bottom of the device. The label includes product identification information and the default password assigned to the device.

- **Digi IX14 label**

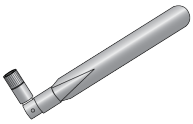
  Printed copy of the product label on the bottom of your device. You can affix this label to the top or side of the device such that you can access the label after the device is mounted or store the label in a safe place for future reference.

Note A subscription to **Digi Remote Manager** is bundled with your Digi IX14 purchase. See Digi Remote Manager product page to learn about Digi Remote Manager features.

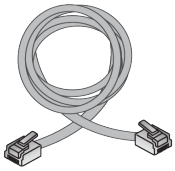
Step 2: Gather accessories

Note Digi offers several Digi IX14 accessory kits so you can purchase exactly what you need to support your Digi IX14. See Digi IX14 accessory kits for details or go to Digi IX14 support.

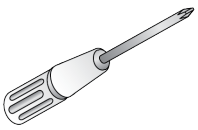
Here's the list of accessories used in ***Quick start with Digi IX14 local web UI***:



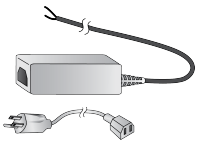
Antennas
Use antennas provided by a Digi accessory kit or use alternate antennas that comply with the Digi IX14 antenna requirements.



Ethernet cable
Use an Ethernet cable to connect the Digi IX14 **WAN/ETH1** port to a laptop or PC to access the local web interface via a browser or connect to a WAN.

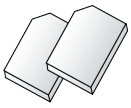


Phillips-head screwdriver
Use a #1 Phillips-head screwdriver to remove and replace the SIM door when installing SIM cards.



Power supply
Use a power supply provided by a Digi accessory kit or use an alternate power supply that complies with the power supply requirements.

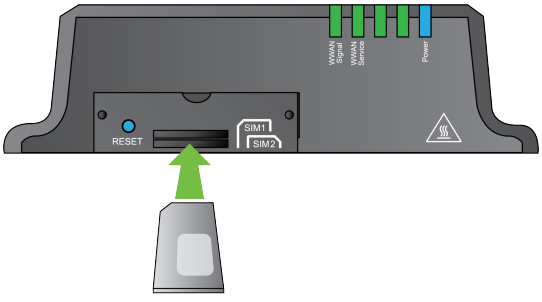
Laptop or personal computer
Use an Ethernet cable to connect the Digi IX14 **WAN/ETH1** port to a laptop or PC to access the local web interface via a browser.



SIM card(s)
Acquire SIM cards as needed. Note the carrier, network APN (Access Point Name), and SIM pin (if any) for each card.

Step 3: Connect hardware

a. Install SIM card(s). See Install SIM cards.



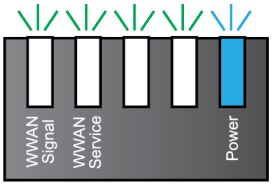
b. Attach antenna(s). See Attach and position antennas.

c. Use an Ethernet cable to connect your Digi IX14 **WAN/ETH1** port to your PC.

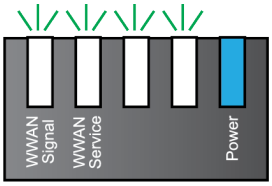
d. Power on the Digi IX14 by connecting a DC power source. See Digi IX14 power supply requirements for power supply requirements.

e. Power LED is solid blue as the device prepares to boot up.

f. Power LED flashes blue as the device boots up.



Power LED is solid blue when the Digi IX14 is ready.



Step 4: Sign up for Digi Remote Manager

Here's how to sign up with Digi Remote Manager:

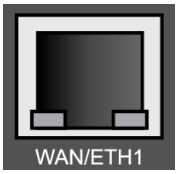
a. Click **Sign Up** to create a new account.

b. You'll receive an email with login instructions.

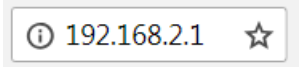
c. Click on the link in the email to log into Digi Remote Manager.

Step 5: Access the Digi IX14 local web interface

a. If you have not already done so, use an Ethernet cable to connect your Digi IX14 WAN/ETH1 port to your PC.



b. Open a browser and go to **192.168.2.1**.



c. Log into the Digi IX14:

User name: Use the default user name: **root**

Password: Use the unique password printed on the bottom label of the device (or the printed label included in the package)

The Digi IX14 local web UI main menu appears.

Step 6: Configure cellular connection using the web interface

a. From the navigation pane, click **Configuration**.
b. Open **Modem** and use default setting **Any SIM** for the **Match SIM by** option.
c. If you are using a PIN-locked SIM, enter the PIN for the SIM.
d. Open **APN list > APN** and enter the **APN** for the SIM.
e. Click **Save**.

The **WWAN service** LED flashes yellow when the cellular connection is coming up. See Digi IX14 LEDs.

Step 7: Add your Digi IX14 to your Digi Remote Manager account

a. From the web interface, click **Manage Device** in the top right of the display.
b. Log into Digi Remote Manager. (If you created an account in Quick start with Digi IX14 local web UI, look for the Digi Remote Manager email that provides your login credentials.)
c. Click **Device Management**.
d. Click **Add Devices**.

Select **MAC address** and provide the Ethernet MAC address for your device.

For **Install Code**, enter the default password on the printed label packaged with your device. (The same default password is also shown on the label affixed to the bottom of the device.)

a. Click **Add**.
b. Click **OK**.

Digi Remote Manager adds your Digi IX14 to your account and it appears in the **Device Management** view.

Next steps

Congratulations! You have completed the Quick start.

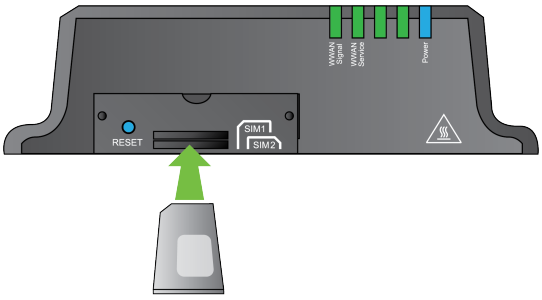
- To manage and configure your Digi IX14 remotely using Digi Remote Manager, see Digi Remote Manager.
- To manage and configure your Digi IX14 locally using the local web interface, see Access the Digi IX14 local web UI.

Hardware setup

Install SIM cards

To install SIM cards:

1. On the Digi IX14 front panel, use a #1 Phillips-head screwdriver to remove the SIM door.
2. If the Digi IX14 device is used in an environment with high vibration levels, SIM card contact fretting may cause unexpected SIM card failures. To protect the SIM cards, Digi strongly recommends that you apply a thin layer of dielectric grease to the SIM contacts prior to installing the SIM cards.
3. Insert the SIM card(s) into the SIM sockets. Position the SIM cards to match the diagram on the device.



4. After all SIM cards are in place, use a #1 Phillips-head screwdriver to carefully replace the SIM door.

WARNING! Take care when you tighten the screws on the SIM door. If you apply too much pressure and over-tighten the screws, you can damage the SIM door or strip the screw threads. Torque to 2.9 inch/pounds.

Attach and position antennas

Note The Digi IX14 does not include a power supply or antennas. See Digi IX14 accessory kits for information on Digi IX14 power supplies and antennas.

- Connect Digi IX14-compatible antennas to the **WWAN-1** and **WWAN-2** antenna connectors on the back of the device. Position the antennas for best reception.

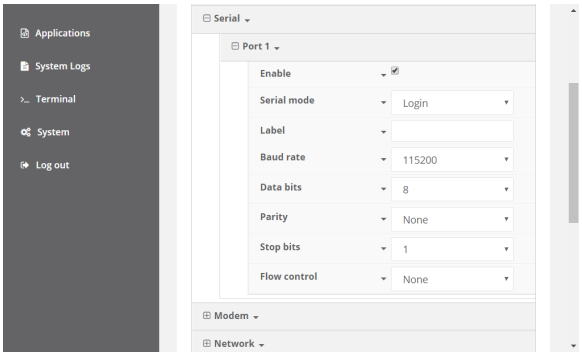
Connect the WAN/ETH1 port

Use an Ethernet cable to connect the Digi IX14 to your local laptop or PC or to your local network (LAN).

- If you connect directly to your PC, the factory default IP address is **192.168.2.1**
- If you connect to a LAN that has a DHCP server, reboot the device after you connect and wait for the DHCP server to assign an IP address to the device.

Connect the serial port

Use an RS-232 serial cable to establish a serial connection from your Digi IX14 to your local laptop or PC. Use a terminal emulator program to establish the serial connection. The serial port must be configured to match the configuration of the serial port to which you are connecting. Here is the default serial port configuration:



See Configure serial interfaces.

Power on the Digi IX14

Note The Digi IX14 does not include a power supply or antennas. See Digi IX14 accessory kits for information on Digi IX14 power supplies and antennas.

1. Power on the Digi IX14 by connecting a DC power source. If you are using a non-Digi power supply, see Digi IX14 power supply requirements.
2. **Power** LED is sold blue as the device prepares to boot up.
3. **Power** LED flashes blue as the device boots up.
4. When the **Power** LED stops flashing blue and returns to solid blue, the Digi IX14 is ready.

Initial configuration

Review Digi IX14 default settings

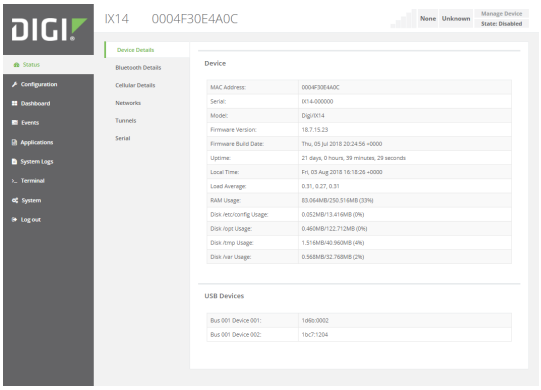
The following table lists factory default settings for the Digi IX14.

Central management	■ Digi Remote Manager enabled as the central management service
Interface priorities	■ Modem (cellular) is WAN interface with metric of 3 ■ LAN (Ethernet) with metric of 5
Modem configuration	■ SIM failover after 5 attempts
Network settings	■ LAN subnet of 192.168.2.1/24 ■ DHCP enabled ■ Source NAT enabled (outbound traffic)
Security policies	■ Packet filtering allows all outbound traffic ■ SSH, web admin, and local admin access enabled
Services	■ Bluetooth service enabled to allow the Digi Remote Manager mobile app to automatically register using the QR code on the device label. You can disable Bluetooth service after the device is provisioned.
Monitoring	■ Device heath metrics uploaded to Digi Remote Manager at 60 minute interval.

Access the Digi IX14 local web UI

To connect to the Digi IX14 local web UI:

1. Use an Ethernet cable to connect the Digi IX14 **WAN/ETH1** port to a laptop or PC.
2. Open a browser and go to **192.168.2.1**.
3. Log into the device using the default user name **root** and the unique password printed on the label packaged with your device. The local web admin main screen appears.



Access the admin command line interface (cli)

To access the command line interface:

1. From the menu, click **Terminal**.
2. Provide your username and password.

```
IX14 login: root
Password:

Connecting now, 'exit' to disconnect from Admin CLI ...

#
```

End an admin command line interface (cli) session

To exit the admin CLI:

- At the command prompt, enter **exit**:

```
# exit


Disconnected from Admin CLI
```

Get help for commands

To get help while using commands, enter the **?** (question mark) character.

For example:

```
# ?
atcmd           Run AT comands on the modem
modem           Modem CLI
analyzer        Analyzer CLI
config          View and modify the configuration
exit            Exit the CLI
ping            Ping network diagnostic
cp              Copy files
mv              Move files
rm              Remove files
mkdir           Make directories
more            Display files
scp             Secure copy files
reboot          Reboot the system
show            Show status information
traceroute      Trace route network diagnostic
ipsec           Show IPSEC debug information
#
```

Reset default password for root

Digi recommends you change the factory-assigned default password for user **root** after initial login.

Local web UI

To change a Digi IX14 user password using the local web UI:

1. From the menu, click **Configuration**.
2. Open **Authentication > Users**.
3. Expand the **root** user and enter a new password.
4. Click **Save**.

Digi Remote Manager

To change the default password for root using Digi Remote Manager:

1. Click **Security > Users**.
2. Select the **root** user and click **Change Password**.
3. Enter a new password and confirm the new password.
4. Click **OK**.

Configure modem (cellular) APNs

To configure the APNs for the modem:

1. From the menu, click **Configuration > Modem > APN list**.
2. Click **Add** and enter options for the APN:

APN: Enter the access point name to use to connect to the cellular network.

IP version: Select the IP version. The default is **Automatic**.

Authentication method: Select the authentication method. The default is **None**.

3. Click **Save**.

Change the default LAN subnet

You can change the Digi IX14 default LAN subnet—192.168.2.1/24—to any range of private IPs. The local DHCP server range will also change to the range of the LAN subnet.

To change the LAN subnet:

1. From the menu, click **Configuration**.
2. Open **Network > Interfaces > LAN**.
3. Open the **IPv4** option. The Address field contains the range of available IPs you can assign. You must also specify the subnet mask.
4. Click **Save**.

Change the LAN address type

By default, the LAN interface uses a static IP address. To use a DHCP address:

1. From the menu, click **Configuration**.
2. Open **Network > Interfaces > LAN**.
3. Open the **IPv4** option and change the **Type** to **DHCP address**.
4. Click **Save**.

Configure SIM pin

If your cellular provider requires a SIM pin, configure the PIN for a SIM:

1. From the menu, click **Configuration > Modem**.
2. Enter the PIN in the **PIN** field.
3. Click **Save**.

Configure serial interfaces

To configure the serial interface:

1. From the menu, click **Configuration**.
2. Open **Serial** and configure the port. The configuration should match the serial configuration of the device to which you want to connect.

   Enable: Enable the port.

   Serial mode: Select the mode for the serial port: Login or Remote Access. The default is **Login**.

   Label: (Optional) Enter a label to associate with the port.

   Baud rate: Select the Baud rate. The default is **115200**.

   Data bits: Select the number of data bits. The default is **8**.

   Parity: Select the parity type. The default is **None**.

   Stop bits: Select the number of stop bits. The default is **1**.

   Flow control: Select the flow control. The default is **None**.
3. Click **Save**.

Configure system settings

To configure system settings:

1. From the menu, click **Configuration**.
2. Open **System**.
3. Provide the system information settings:

   Name: (Optional) Enter a name for the system.

   Contact: (Optional) Enter a contact for the system.

   Location: (Optional) Enter a location for the system.

   Banner: (Optional) Enter banner text to appear when a user logs into the system.
4. Configure **Scheduled tasks**:

   Reboot time: (Optional) If you want to reboot the system daily, enter the time for the daily reboot.

   Start time/Duration window: Enter a start time and duration window for system maintenance.

   Frequency: Enter the frequency for the maintenance window.
5. If you want to add **Custom scripts**, click **Add** and configure the script.
6. Configure Time:

   Timezone: Select the timezone for the Digi IX14.

   NTP servers: If you want to add an NTP server, click ADD and specify the URL for the server.
7. Configure Log options:

   Heartbeat interval: Enter the minimum time between sending heartbeat status events.

   Event categories: Open the Event categories and enable/diable the event categories you want to log.
8. Configure syslog servers:

   Open **Server** and click **Add** to confgure an additional syslog server.
9. Click **Save**.

Enable or disable Bluetooth service

By default, Bluetooth service is enabled. To disable or enable Bluetooth service:

1. From the menu, click **Configuration**.
2. Open **Services > Bluetooth**.
3. Enable or disable the Bluetooth service as needed.
4. Click **Save**.

Note You will not see the Digi IX14 Bluetooth service listed on your smart phone or tablet.

Authentication

About Digi IX14 authentication

As released, a Digi IX14 is configured with the following authentication defaults:

- **Idle timeout:** Determines how long a user session can be idle before the system automatically disconnects. The default is no idle timeout.
- **Methods:** Determines how users are authenticated for access: **local users** or **TACACS+**. The default is **local users**.
- **Groups:** Associates access permissions for a group. By default, there are two groups: **admin** and **serial**. The **admin** group allows admin and shell access. The **serial** group allows serial access. You can modify the released groups and create additional groups as needed for your site. A user can be assigned to more than one group.
- **Users:** Local users for the Digi IX14. By default, there is one local user named **root** that belongs to both the **admin** and **serial** groups.
- **TACACS+:** Terminal Access Controller Access-Control System Plus servers and users. By default, TACACS+ is not configured.

Configure idle timeout

You can force an automatic disconnect for user sessions that remain idle for a configured amount of time. By default, the idle timeout is not configured.

To configure the idle timeout:

1. From the menu, click **Configuration**.
2. Open **Authentication > Idle Timeout**.
3. Enter the amount of idle time allowed before the system disconnects. Use the following format:

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

   For example, to force a disconnect after 5 minutes of idle time, enter **5m**.
4. Click **Save**.

Note To disable idle timeout, set the idle timeout to no value (blank).

Configure the authentication method

The Digi IX14 allows two authentication methods: **local users** and **TACACS+**. The default authentication method is **local users**.

To add or remove an authentication method:

1. From the menu, click **Configuration**.
2. Open **Authentication > Methods**.

To add an authentication method, click **Add** and then select the method.

To remove an authentication method, right-click on the method and select **Delete**.

3. Click **Save**.

Configure user groups

A group defines a set of user access permissions. By default, there are two configured groups: **admin** and **serial**. You can modify the default groups and/or create additional groups to meet site requirements.

To configure a group:

1. From the menu, click **Configuration**.
2. Open **Authentication > Groups**.

   To modify an existing group, open the group you want to modify.

   To create a new group, enter a name for the new group and click **Add**.
3. Enable or disable access permissions for the group.
4. Click **Save**.

Create a new user

Access permissions for a user are determined by the group(s) assigned to the user. By default, there are two configured groups: **admin** and **serial**. The default user **root** is assigned to both **admin** and **serial** groups.

To create a new user for your Digi IX14:

1. From the menu, click **Configuration**.
2. Open **Authentication > Users**.
3. Enter a name for the new user and click **Add**.
4. Configure options for the user:

   Enable: Enable the user.

   Password: Enter a password for the new user.

   Groups: Select one or more groups for the user to control access permissions for the user. See Configure user groups.

   SSH keys: If you use SSH keys for SSH access, enter the SSH public key for the user.

   Two-factor authentication: If you want to implement two-factor authentication, configure the type implemented at your site.
5. Click **Save**.

System administration

Review device status

To review Digi IX14 status:

1. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
2. From the menu, click **Status**.
3. Open the details panel for the status you want to view.

Upgrade device firmware

To update firmware using the local web UI:

1. Download the firmware file to your local machine.
2. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
3. From the menu, click **System**.
4. Under **Device Firmware**, click **Choose File**.
5. Browse to and select the firmware file.
6. Provide **Options** as needed.
7. Click **Update Firmware**.

Update cellular modem firmware

To update cellular modem firmware:

1. Download the firmware file to your local machine.
2. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
3. From the menu, click **System**.
4. Under **Modem Firmware**, click **Choose File**.
5. Browse to and select the firmware file.
6. Provide **Options** as needed.
7. Click **Update Firmware**.

Reboot the device

To reboot the device:

1. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
2. From the menu, click **System**.
3. Under **Device Reboot**, click **Reboot**.

Save and restore configuration(s)

The Digi IX14 provides the following configuration management options:

- Save the current configuration to a file.
- Restore the configuration from a saved file
- Erase all configurations and return to factory defaults

To save the current configuration to a file:

1. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
2. From the menu, click **System**.
3. Under **Configuration Management**, click **Save Config**.

To restore the configuration from a previously saved configuration file:

1. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
2. From the menu, click **System**.
3. Under **Configuration Management**, click **Choose File**
4. Browse to and select a configuration file.
5. Click **Restore Config**.

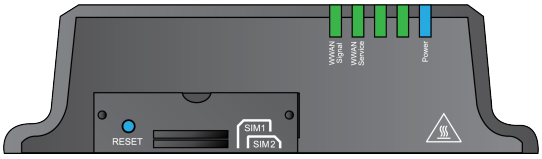
To erase all configurations and return to factory default:

1. Access the Digi IX14 local web UI. See Access the Digi IX14 local web UI.
2. From the menu, click **System**.
3. Under **Configuration Management**, click **Erase Config**.
4. Click **OK**.

Reset to factory default settings using Reset button

To reset the device to factory default settings:

1. Short press and release the **RESET** button located on the SIM gasket cover:



2. Wait for the device to reboot.
3. Short press and release the **RESET** button again.

The device resets to factory default settings.

Note If you perform a Reset only once, the device resets to factory default settings but retains SSH keys.

Reset to factory default settings using System menu

To erase the config and restore factory default settings:

1. From the menu, click **System**.
2. Under the **Configuration Management**, click **Erase Config**.
3. Click **OK**.

Configure firewall

Firewall configuration includes the following configuration options:

- **Zones:** A list of network interface groups you can use with packet filtering and access control lists. Default zones include: **Any**, **Loopback**, **Internal**, **External**, **Setup**, **IPsec**, and **Dynamic routes**.
- **Port forwarding:** A list of rules that allow network connections to the Digi IX14 to be forwarded to other servers by translating the destination address.
- **Packet filtering:** A list of packet filtering rules that determine whether to accept or reject network connections that are forwarded through the Digi IX14.
- **Custom rules:** A script that is run to install advanced firewall rules beyond the scope/capabilities of the standard device configuration.

Configure packet filtering

By default, packet filtering is enabled and monitors traffic going to and from the Digi IX14. The predefined settings are intended to block unauthorized inbound traffic while providing an unrestricted flow of data from LAN to WAN.

To configure a packet filtering rule:

1. From the menu, click **Configuration**.
2. Open **Firewall > Packet filtering**.

3. Click **Add** to add a rule and configure the rule.
4. Click **Save**.

Configure port forwarding

Remote computers can access applications or services hosted on a local network with the Digi IX14 by setting up port forwarding. It provides mapping instructions that direct incoming traffic to the proper device on a LAN.

To configure port forwarding:

1. From the menu, click **Configuration**.
2. Open **Firewall > Port Forwarding**.
3. Click **Add**.
4. Select the relevant **LAN Interface**.
5. The **IP version** and **Protocol** can be left at their default values unless changes are required by the request being serviced by this port forwarding configuration.
6. Specify the public-facing **Port** for remote access.
7. In the **To** fields, specify the **Port** and the **IP address** associated with the intended destination device.
8. If necessary, open the **Access Control List** to create a white list that determines which devices are authorized to leverage this particular forwarding route.
9. Click **Save**.

Create a Virtual LAN (VLAN) route

To create a VLAN:

1. If you have not already done so, create the network interface for the VLAN. See Create new network interfaces.
2. Open **Network > Virtual LAN**.
3. Type a name for the VLAN and click **Add**.
4. Provide settings for the new VLAN:

   Device: Select the network interface for the VLAN.

   ID: Assign a unique numeric ID to the VLAN.
5. Click **Save**.

Services and applications

Allow remote access for ssh, web administration, or remote control services

To allow remote access for SSH, web administration, or remote control:

- Device must have a publicly reachable IP address.
- **External** zone is added for the SSH, web administration, or remote control services. (See Configure firewall for information on zones.)

Note The steps below open external access to your device. Make sure you change the device password to a more secure key to prevent intrusions.

To allow ssh, web administration, or remote control for the external zone:

Add External zone to SSH service:

1. From the menu, click **Configuration**.
2. Open **Services > SSH > Access Control List > Zones**.
3. Add a new entry for **External**.
4. Click **Save**.

Add External zone to web administration service:

1. From the menu, click **Configuration**.
2. Open **Services > Web Administration > Access Control List > Zones**.
3. Add a new entry for **External**.
4. Click **Save**.

Add External zone to remote control service:

1. From the menu, click **Configuration**.
2. Open **Services > Remote Control > Access Control List > Zones**.
3. Add a new entry for **External**.
4. Click **Save**.

Configure DNS

To add a DNS server:

1. From the menu, click **Configuration**.
2. Open **DNS > DNS servers**.
3. Click **Add** and configure the DNS server.
4. Click **Save**.

To configure DNS:

1. From the menu, click **Configuration**.
2. Open **Services > DNS**.

3. Configure DNS options.
4. Click **Save**.

Configure Simple Network Management Protocol (SNMP)

To configure SNMP:

1. From the menu, click **Configuration**.
2. Open **Services > SNMP**.
3. Select **Enable** to enable the SNMP service.
4. Configure the **Access control list** (addresses, interfaces, and/or firewall zones) for the SNMP service.
5. Specify the **Username** and **Password** for the connection to this SNMP agent.
6. Ensure the **Authentication Type**, **Privacy passphrase**, and **Privacy protocol** options are set to the appropriate values.
7. Click **Save**.

Once the configuration has been set, you can connect to the device agent. Since the agent is read-only, command changes to the device are not possible.

To download the default MIBs provided by Digi:

1. From the menu, click **System**.
2. Under the **SNMP MIBS**, click **Download MIBs**.

Configure a multicast route

To configure a multicast route:

1. From the menu, click **Configuration**.
2. Open **Services > Multicast**.
3. Provide a name for the route and click **Add**.
4. Enable the route.
5. Enter the source address for the route.
6. Enter a source port, for example **4242**. Ensure the port is not used by another protocol.
7. Select a source interface, for example **LAN**.
8. Select a destination interface for the route, for example **Modem**.
9. Click **Save**.

Schedule tasks and applications

To schedule a task or application:

1. Upload an application file:
    a. From the menu, click **Applications**.
    b. Click **Choose File** to select a local application or script file to upload, and click **Upload**.
2. Run or schedule application execution:
    a. From the menu, click **Configuration**.
    b. Open **Applications**.
    c. Click **Add** and select the application you want to schedule.
    d. Provide options for the application.
3. Click **Save**.

Run Python applications

Digi IX14 supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. You can also specify Python programs to be run each time the device starts up or with a specified schedule.

Start an interactive Python session

Use the **python** command without specifying any parameters to start an interactive Python session. The Python session operates interactively using REPL (Read Evaluate Print Loop) to allow you to write Python code on the command line:

```
# python
Python 3.6.4
You can obtain the list of available python modules using the help
("modules") call:
# python

Python 3.6.4
>>> help("modules")
Please wait a moment while I gather a list of all available modules...

__future__          argparse            hmac                selectors
_ast                array               html                shelve
.
.
.
>>>
```

Note Python interactive session is not available in CLI. You must access a device shell in order to execute python.

Run a Python application interactively

Use the **python** command to run a Python application interactively. The Python application runs until it exits, displaying output and prompting for additional user input if needed. If you want to interrupt the application, enter CTRL-C.

For example, the following command:

```
# python test.py arg1 arg2
<Python program execution output>
#
```

Runs the test.py application and passes two parameters to the application: arg1 and arg2.

Note Python command is not available in CLI. You must access a device shell in order to execute python.

Get help with Python programming on the Digi IX14

You can use the following Digi tools to assist in Python programming for a Digi IX14 device

- digidevice.cli module
- Help for executing CLI commands
- digidevice.datapoint module
- Help for uploading datapoints
- digidevice.config module
- Help for reading and modifying configurations

- digidevice.runt module
- Help for reading and modifying the device runtim database

digidevice.cli module

Use the digidevice.cli module to execute CLI commands and retrieve command output. For example:

```
# python

Python 3.6.4
>>> from digidevice import cli
>>> print(cli.execute("show version"))
Digi/IX14 Version 18.6.114.2-7ece3f3 --  Thu, 28 Jun 2018 16:51:08
+0000
>>>
```

Help for executing CLI commands

Get help executing a CLI command by accessing help for cli.execute:

```
# python

Python 3.6.4
>>> from digidevice import cli
>>> help(cli.execute)
Help on function execute in module digidevice.cli:

execute(command, timeout=5)
    Execute a CLI command with the timeout specified returning the
results.
.
.
.
>>>
```

digidevice.datapoint module

Use the digidevice.datapoint module to upload data points to Digi Remote Manager. The Digi Remote Manager connection must be enabled and connected. For example:

```
# python

Python 3.6.4
>>> from digidevice import datapoint
>>> datapoint.upload('test/stream/my_datapoint', 73)
>>>
```

Help for uploading datapoints

Get help for uploading datapoints to your Digi Remote Manager account by accessing help for datapoint.upload:

```
# python
```

```
Python 3.6.4
>>> from digidevice import datapoint
>>> help(datapoint.upload)
Help on function upload in module digidevice.datapoint:

upload(stream_id:str, data, *, description:str=None,
timestamp:float=None, units:str=None, geo_location:Tuple[float, float,
float]=None, quality:int=None, data_
type:digidevice.datapoint.DataType=None, timeout:floa
t=None)
.
.
.
>>>
```

digidevice.config module

Use the digidevice.config module to access and modify the device configuration.

The code snippet below demonstrates how to read the device configuration using the digidevice.config module:

```
# python

Python 3.6.4
>>> from digidevice import config
>>> cfg = config.load()
>>> print(cfg)
action.ModemManager.config.0=action.ModemManager.debug
action.ModemManager.config_restart=false
action.ModemManager.cron=
action.ModemManager.debug=false
.
.
.
>>> print(cfg.get("system.name"))
IX14
interfaces = cfg.get("network.interface")
print(interfaces.keys())
['aview', 'defaultip', 'defaultlinklocal', 'lan', 'loopback', 'modem']
>>> print(interfaces.get("lan.ipv4.address"))
192.168.2.1/24
>>>
```

The code snippet below demonstrates how to write the device configuration using the digidevice.config module:

```
# python

Python 3.6.4
>>> from digidevice import config
>>> cfg = config.load(writable=True)
>>> cfg.set("system.name", "New-Name")
>>> cfg.commit()
True
>>> print(cfg.get("system.name"))
New-Name
>>>
```

Help for reading and modifying configurations

Get help for reading and modifying the device configuration by accessing help for digidevice.config:

```
# python

Python 3.6.4
>>> from digidevice import config
>>> help("digidevice.config")
Help on module acl.config in digidevice:

NAME
    acl.config - Python interface to ACL configuration (libconfig).
.
.
.
>>>
```

digidevice.runt module

Use the digidevice.runt module to access and modify the device runtime database.

The code snippet below demonstrates how to read the device runtime database using the digidevice.runt module:

```
# python

Python 3.6.4
>>> from digidevice import runt
>>> runt.start()
>>> print(runt.keys(""))
['advanced', 'firmware', 'mm', 'my-variable', 'network', 'system',
'vpn']
>>> print(runt.keys("system"))
['cpu_temp', 'disk', 'load_avg', 'local_time', 'mac', 'model', 'ram',
'serial', 'uptime']
>>> print(runt.get("system.mac"))
0004F30E48A8
>>> runt.stop()
>>>
```

The code snippet below demonstrates how to write the device runtime database using the digidevice.runt module:

```
# python

Python 3.6.4
>>> from digidevice import runt
>>> runt.start()
>>> runt.set("my-variable", "my-value")
>>> print(runt.get("my-variable"))
my-value
>>> runt.stop()
>>>
```

Help for reading and modifying the device runtim database

Get help for reading and modifying the device runtime database by accessing help for digidevice.runt:

```
# python

Python 3.6.4
>>> from digidevice import runt
>>> help("digidevice.runt")
Help on module acl.runt in digidevice:

NAME
    acl.runt - Python interface to ACL runtime database (runtd).
.
.
.
>>>
```

Run custom applications

To run a custom application:

1. Upload an application
2. Configure application execution

Upload an application

To upload an application from your local PC to your device:

1. From the menu, click **Applications**.
2. Click **Choose File** and select the application file you want to upload.
3. Click **Upload**.

The uploaded file is stored in **/etc/config/scripts**.

To configure execution of the application, see Configure application execution.

Configure application execution

To configure how to execute an application:

1. If you have not already done so, upload the application file. See Upload an application.
2. From the menu, click **Configuration**.
3. Open the **Applications** folder.
4. Click **Add** and complete the following fields:
   - **Enable:** Enable the script.
   - **Label(Optional)**: Provide a label for the script.
   - **Run mode**: Select the run mode: On boot, Interval, Set time, or During system maintenance.
   - **Command**: Specify the name of the application. By default, the system looks for the application in the /**etc/config/scripts** directory. If you want to specify an application in another directory, provide the complete path for the application file.
   - **Log script output**: Save stdout to the system log.
   - **Log script errors**: Save stderr to the system log.

- **Once**: Enable this option if you want to execute the application only once at specified set time.
- **Sandbox**: Enable this option if you want to run the application in a protected sandbox to prevent the application execution from affecting the system.

5. Click **Save**.

Digi Remote Manager

Digi recommends you use Digi Remote Manager to manage Digi IX14 routers. Use the local web admin only when necessary.

Configure Central management

By default, your Digi IX14 is configure to use central management using Digi Remote Manager.

To configure central management:

1. From the menu, click **Configuration**.
2. Open **Central management**.

   Enable central management: Enable or disable central management. The default is enabled.

   Management server: Enter the URL for the central management server.

   Retry interval: Enter a retry interval. The default is 30 seconds.

   Keep-alive interval: Enter the keep-alive interval. The default is 60 seconds.

   Cellular keep-alive interval: Enter a keep-alive interval for cellular connections. The default is 290 seconds.

   Allowed keep-alive misses: Enter the number of allowed keep-alive misses. The default is 3.
3. Click **Save**.

Log into Digi Remote Manager

To start Digi Remote Manager

1. If you have not already done so, click here to sign up for a Digi Remote Manager account.
2. Check your email for Digi Remote Manager login instructions.
3. Go to remotemanager.digi.com.
4. Log into your Digi Remote Manager account.

Add a device to Digi Remote Manager

1. From the web interface, click **Manage Device** in the top right of the display.
2. Log into Digi Remote Manager. (If you created an account in Add a device to Digi Remote Manager, look for the Digi Remote Manager email that provides your login credentials.)
3. Click **Device Management**.
4. Click **Add Devices**.

   Select **MAC address** and provide the Ethernet MAC address for your device.

   For **Install Code**, enter the default password on the printed label packaged with your device. (The same default password is also shown on the label affixed to the bottom of the device.)

c. Click **Add**.

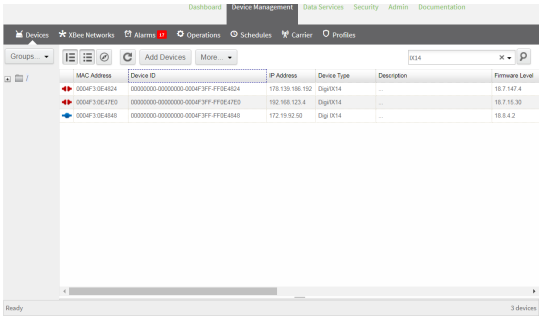
d. Click **OK**.

Digi Remote Manager adds your Digi IX14 to your account and it appears in the **Device Management** view.

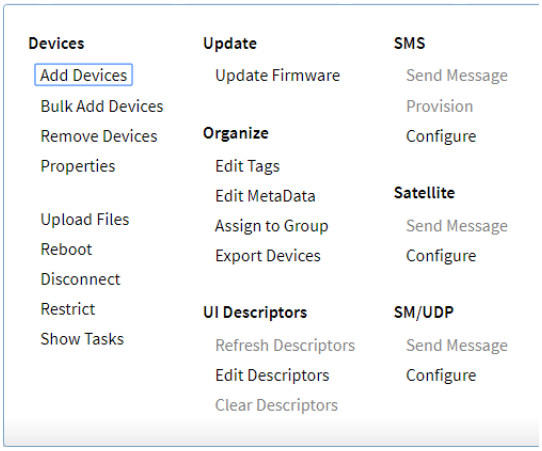
View and manage a Digi IX14 device

To view and manage your device:

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. User the Search bar to locate and select the Digi IX14 you want to manage.



4. Click **Properties** to view general information for your Digi IX14.
5. Click the **More** menu to perform a task.



Use the Digi Remote Manager mobile app

If you have a smart phone or tablet, you can use the Digi Remote Manager mobile app to automatically provision a new devices and monitor devices in your account.

To download the mobile app:

- For iPhone, go to the **App Store**
- For Android phones, go to **Google Play**

To sign up for a new Digi Remote Manager account using the mobile app:

1. From the menu, click **Log in or Sign Up**.
2. Click **Sign up** to create a new account.

3. You'll receive an email with login instructions.
4. From the **Digi Remote Manager** mobile app, click **Log in** and log into your new account.

To register a new device:

1. From the menu, select **Install a device with a QR or bar code** and scan the installation QR code on the label.
2. Follow the prompts to complete your Digi IX14 registration.

Digi Remote Manager registers your Digi IX14 and adds it to your Digi Remote Manager device list. You can now manage the device remotely using Digi Remote Manager.

Review Digi IX14 default settings

The following table lists factory default settings for the Digi IX14.

Central management	■ Digi Remote Manager enabled as the central management service
Interface priorities	■ Modem (cellular) is WAN interface with metric of 3 ■ LAN (Ethernet) with metric of 5
Modem configuration	■ SIM failover after 5 attempts
Network settings	■ LAN subnet of 192.168.2.1/24 ■ DHCP enabled ■ Source NAT enabled (outbound traffic)
Security policies	■ Packet filtering allows all outbound traffic ■ SSH, web admin, and local admin access enabled
Services	■ Bluetooth service enabled to allow the Digi Remote Manager mobile app to automatically register using the QR code on the device label. You can disable Bluetooth service after the device is provisioned.
Monitoring	■ Device heath metrics uploaded to Digi Remote Manager at 60 minute interval.

Configure multiple devices using profiles

Digi recommends you take advantage of Digi Remote Manager profiles to manage multiple Digi IX14 routers. Typically, if you want to provision multiple Digi IX14 routers:

1. Using the Digi IX14 local web UI, configure one Digi IX14 router to use as the model configuration for all subsequent Digi IX14s you need to manage.
2. Register the configured Digi IX14 in your Digi Remote Manager account.
3. In Digi Remote Manager, create a profile based on the configured Digi IX14.
4. Apply the profile to the Digi IX14 routers you need to configure.

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

Learn more

- For information on using Digi Remote Manager to configure and manage Digi IX14 routers, see the Digi Remote Manager User Guide.
- For information on using Digi Remote Manager APIs to develop custom applications, see the Digi Remote Manager Programmer Guide

Monitoring

Collect device health data

You can enable or disable the collection of device health data to upload to Digi Remote Manager.

1. From the menu, click **Configuration**.
2. Open **Monitoring > Device Health**.
3. Configure the following:

   Enable

   Health sample interval
4. Click **Save**.

Configure IntelliFlow

IntelliFlow keeps track of network data usage and traffic information and displays the information in a series of charts available the local web UI. To use IntelliFlow, the Digi IX14 must be powered on and you must have access to the local web UI. Once you enable IntelliFlow, the **Dashboard** option appears in the main navigation menu.

Note When Intelliflow is enabled, it adds an estimated 50MB of data usage for the device by reporting the metrics to Digi Remote Manager.

To enable or disable IntelliFlow:

1. From the menu, click **Configuration**.
2. Open **Monitoring > IntelliFlow** and set the following options:

   Enable: Enable or disable IntelliFlow.

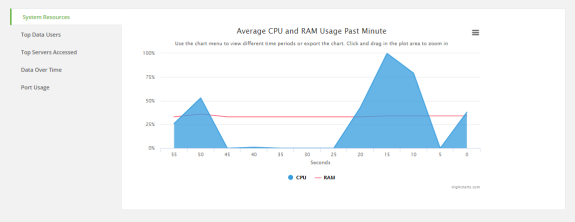
   Zone: Specify the firewall zone for the network interface clients to monitor. The default zone, Internal, is appropriate for most environments.
3. Click **Save**.

The **Dashboard** option is included in the local web UI main menu.

System resources chart

To generate a System resources chart:

1. If you have not already done so, enable IntelliFlow. See Configure IntelliFlow.
2. From the menu, click **Dashboard**.
3. Click **System Resources**.



Top data users chart

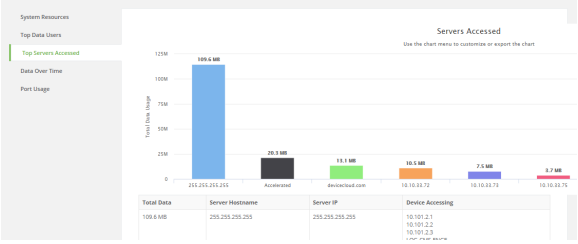
To generate a Top data users chart:

1. If you have not already done so, enable IntelliFlow. See Configure IntelliFlow.
2. From the menu, click **Dashboard**.
3. Click **Top Data Users**.

Top servers accessed chart

To generate a Top servers accessed chart:

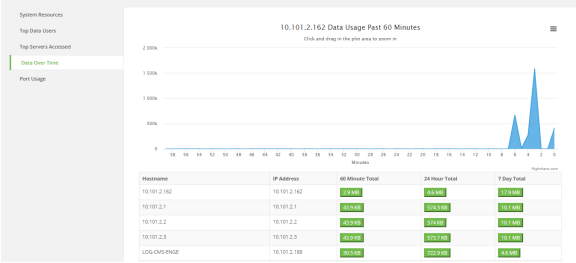
1. If you have not already done so, enable IntelliFlow. See Configure IntelliFlow.
2. From the menu, click **Dashboard**.
3. Click **Top Servers Accessed**.



Data over time chart

To generate a Data over time chart:

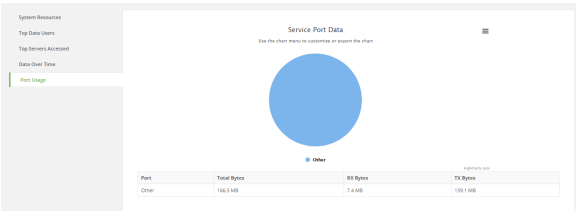
1. If you have not already done so, enable IntelliFlow. See Configure IntelliFlow.
2. From the menu, click **Dashboard**.
3. Click **Data Over Time**.



Port usage chart

To generate a Port usage chart:

1. If you have not already done so, enable IntelliFlow. See Configure IntelliFlow.
2. From the menu, click **Dashboard**.
3. Click **Port Usage**.



Change chart view options

You can use the Chart menu to select how you want to view chart data:

To change chart view options:

1. When a chart is displayed, click (Chart menu).
2. Select an available view for the chart.

Export chart to PNG

To export a chart to a PNG file:

1. When a chart is displayed, click (Chart menu).
2. Select **Export to PNG**.

The chart is saved as a PNG file and downloaded to your PC.

Print a chart

To print a chart:

1. When a chart is displayed, click (Chart menu).
2. Select **Print chart**.
3. Fill in print options and click **Print**.

Configure NetFlow Probe

NetFlow allows for in depth traffic analysis and bandwidth monitoring.

To probe network traffic and export statistics to NetFlow collectors:

1. From the menu, click **Configuration**.
2. Open **Monitoring > NetFlow probe** and set the following options:

   Enable: Enable or disable NetFlow probe.

   Protocol version: Select the protocol version. The default is **v10**.

   Flow sampler: Select a flow sampling method. The default is **None**.

   Flow sampler population: If you selected a flow sampler, enter the number of flows for the sampler.

   Inactive timeout: Amount of time a flow can be inactive before sent to a collector.

   Active timeout: Amount of time a flow can be active before sent to the collector.

   Maximum flows: Enter the maximum number of flows to probe simultaneously.

   Collectors: Add the server to send collected data.
3. Click **Save**.

Virtual private networks (VPNs)

Example: Configure VPN access with IPSec tunnels

This example demonstrates how to build an IPSec tunnel through the Digi IX14 WAN connection and use the IPSec tunnel to access endpoints inside a VPN.

To set up VPN access via an IPSec tunnel, you need the following:

- Active WAN connection on the Digi IX14
- IPsec credentials and settings to build a tunnel to the IPsec endpoint
- Rule to allow return traffic from the remote network through the IPsec tunnel back to the local LAN devices

The sample configuration shows a Digi IX14 with a tunnel to a VPN server at 12.13.14.15 through its cellular modem. The client laptop connected to the Digi IX14 LAN Ethernet port can then use the IPsec tunnel to access any IP address in the 10.255.0.0/16 range behind the IPsec server. Any traffic not destined for 10.255.0.0/16 goes through the cellular modem straight to the Internet.

To configure the IPSec tunnel on the Digi IX14

1. From the menu, click **Configuration**.
2. Open **VPN > IPsec > Tunnels**.
3. Add a new tunnel named **Tunnel** and configure the following options:

   Pre-shared key: Enter the pre-shared key to authenticate with the peer.

   (Optional) **XAUTH client**, check **Enable** and enter the XAUTH client **Username** and **Password**.

   Enable MODECFG client: Enable this option to allow receipt of the MODECFG attributes to configure the IP address and DNS server for the tunnel.

   Local endpoint: Do one of the following:

   - Set the **ID Type** to **KeyID** and set the **KeyID value**. This builds the tunnel through any available WAN interface.
   - Set the **Local endpoint > type** to the **Interface** and set the **Local endpoint > Interface** to **Modem**. This builds the tunnel only through the cellular modem WAN interface.

   Remote endpoint: Open **ID** and set the **ID Type** to **IPv4** and enter the **IPv4 ID value** for the hostname.

   IKE: Set the **IKE > Mode** to **Aggressive mode** and set the **IKE > Phase 1 Proposals** and **IKE > Phase 2 Proposals** to match the IKE settings required by the IPSec server. In this example, both proposals are set to **AES128**, **SHA1**, **MOD768**.

4. In **Tunnel > Policies**, add a new policy and set the following options:
   - Set **Policy > Local network > Type** to **Request a network**.
   - Set **Policy > Remote network** to the IPv4 network to access through the tunnel. In this sample, the remote network is **10.255.0.0/16**.

   Note If you want to have all outbound traffic go through this tunnel, set **Policy > Remote Network** to **0.0.0.0/0**.

5. Add a packet filtering rule to allow return traffic:
   - In **Firewall > Packet Filtering**, click **Add** to add a new packet filter.
   - Set **Label** to **Allow all incoming traffic to IPsec tunnel**.

- Set **Action** to **Accept**, set **IP version** to **Any**, and set **Protocol** to **Any**.
- Set **Source Zone** to **IPsec** and set **Destination Zone** to **Internal**.

6. Click **Save**.

Diagnostics

View event and system logs

To view events:

1. From the menu, click **Events**.
2. Use the pull-down filter to select the type of events you want to include in the log: All, Critical, Warning, Info, or Debug. The default is **All**.

To view system logs:

- From the menu, click **System Logs**.

Preserve system logs

By default, the Digi IX14 erases system logs each time the device is powered off or rebooted.

Note You should only enable **Preserve system logs** temporarily to debug issues. Once you are finished debugging, immediately disable **Preserve system logs** to avoid unnecessary wear to the flash memory.

To preserve system logs across reboots:

1. From the menu, click **Configuration**.
2. Under **System > Log**, enable **Preserve system logs**.
3. Click **Save**.

Analyze network traffic

Use the **analyzer** command to analyze network traffic. The analyzer tool captures data traffic on any of the WAN and LAN interfaces and decodes the captured data traffic for diagnostics. You can capture data traffic on multiple interfaces at the same time and define capture filters to reduce the captured data. You can capture up to 10 MB of data traffic in two 5 MB files per interface.

To perform a more detailed analysis, you can download the captured data traffic from the device and view it using a third-party application, such as Wireshark.

Format

```
analyzer state
analyzer interfaces
analyzer filter
analyzer show
analyzer clear
analyzer save
```

Note Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See Save captured data traffic to a file.

Start capturing packets

To start capturing packets:

1. Set the interfaces for capturing packets using the Analyze network traffic **interfaces** command. For example, to capture data on the ethernet and cellular interaces:

   ```
   # analyzer interfaces eth0 wwan0
   ```

   To display the available interfaces, enter the Analyze network traffic **interfaces** command without any options:

   ```
   # analyzer interfaces
   1.eth0 [Up, Running]
   2.wwan0 [Up, Running]
   3.any (Pseudo-device that captures on all interfaces) [Up, Running]
   4.lo [Up, Running, Loopback]
   5.nflog (Linux netfilter log (NFLOG) interface)
   6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
   7.usbmon1 (USB bus number 1)
   ```

   Enter an available interface or the keyword **any** to capture packets from all interfaces.

3. Start capturing packets by setting the Analyze network traffic **state** to **on**:

   ```
   # analyzer state on
   Starting network analyzer
   ```

   WARNING! Capturing data using analyzer can significantly affect device performance.

4. To stop capturing data, turn **off** the Analyze network traffic **state**:

   ```
   # analyzer state off
   Stopping network analyzer
   1 packet captured
   1 packet received by filter
   0 packets dropped by kernel
   27 packets captured
   27 packets received by filter
   0 packets dropped by kernel
   ```

You can capture up to 10 MB of data traffic in two 5 MB files per interface.

Note Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See Save captured data traffic to a file.

Define filters for capturing data traffic

To filter captured data, use the Analyze network traffic **filter** command. For example:

```
# analyzer filter ip host 192.168.1.1
```

See http://www.tcpdump.org/manpages/pcap-filter.7.html for more information on analyzer filters.

Show captured traffic data

To view captured data traffic, use the Analyze network traffic **show** command. The command output show the following information for each packet:

- The packet number
- The timestamp for when the packet was captured
- The length of the packet and the amount of data captured
- Whether the packet was sent or received by the device
- The interface on which the packet was sent or received
- A hexadecimal dump of the packet of up to 256 bytes
- Decoded information of the packet

The output indents captured packets as a visual cue for sent and received packets. In addition, you can use the following controls to view the paged output:

- **spacebar** to view the next page of data
- **PG UP** and **PG DOWN** keys to scroll up and down
- **Q** to navigate to the command prompt

For example:

```
# analyzer show
    1  2018-07-04 09:42:47.678638 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 192.168.2.134 tell 192.168.116.1, length 46
        0x0000:  ffff ffff ffff 6466 b302 03b6 0806 0001  ......df........
        0x0010:  0800 0604 0001 6466 b302 03b6 c0a8 7401  ......df......t.
        0x0020:  0000 0000 0000 c0a8 0286 0000 0000 0000  ................
        0x0030:  0000 0000 0000 0000 0000 0000            ............
    2  2018-07-04 09:42:47.729974 IP (tos 0x0, ttl 64, id 61390, offset 0, flags
[DF], proto UDP (17), length 274)
    192.168.11.143.micromuse-lm > 192.168.255.255.micromuse-lm: UDP, length 246
        0x0000:  ffff ffff ffff 0004 4c03 6501 0800 4500  ........L.e...E.
        0x0010:  0112 efce 4000 4011 bd2c c0a8 0b8f c0a8  ....@.@..,......
        0x0020:  ffff 05fe 05fe 00fe 1fa6 5443 4632 0200  ..........TCF2..
        0x0030:  0000 4944 3d54 4350 3a31 3932 2e31 3638  ..ID=TCP:192.168
        0x0040:  2e31 312e 3134 333a 3135 3334 004e 616d  .11.143:1534.Nam
        0x0050:  653d 5443 4620 4167 656e 7400 4f53 4e61  e=TCF.Agent.OSNa
        0x0060:  6d65 3d4c 696e 7578 2034 2e39 2e38 312d  me=Linux.4.9.81-
        0x0070:  6465 792b 6763 6363 3931 3436 0055 7365  dey+gccc9146.Use
        0x0080:  724e 616d 653d 726f 6f74 0041 6765 6e74  rName=root.Agent
        0x0090:  4944 3d38 6662 6431 3163 652d 3635 3266  ID=8fbd11ce-652f
        0x00a0:  2d34 3131 342d 6263 6563 2d61 3831 6163  -4114-bcec-a81ac
        0x00b0:  3039 3734 3864 6400 5472 616e 7370 6f72  09748dd.Transpor
        0x00c0:  744e 616d 653d 5443 5000 5365 7276 6963  tName=TCP.Servic
        0x00d0:  654d 616e 6167 6572 4944 3d38 6662 6431  eManagerID=8fbd1
        0x00e0:  3163 652d 3635 3266 2d34 3131 342d 6263  1ce-652f-4114-bc
        0x00f0:  6563 2d61 3831 6163 3039 3734 3864 642d  ec-a81ac09748dd-
        0x0100:  3000 506f 7274 3d31 3533 3400 486f 7374  0.Port=1534.Host
        0x0110:  3d31 3932 2e31 3638 2e31 312e 3134 3300  =192.168.11.143.
    3  2018-07-04 09:42:47.758796 IP (tos 0x0, ttl 1, id 28637, offset 0, flags
[none], proto UDP (17), length 202)
    192.168.107.3.63028 > 239.255.255.250.ssdp: UDP, length 174
        0x0000:  0100 5e7f fffa 0060 6ed5 93da 0800 4500  ..^....`n.....E.
        0x0010:  00ca 6fdd 0000 0111 2da0 c0a8 6b03 efff  ..o.....-...k...
        0x0020:  fffa f634 076c 00b6 dd88 4d2d 5345 4152  ...4.l....M-SEAR
```

```
0x0030:  4348 202a 2048 5454 502f 312e 310d 0a48  CH.*.HTTP/1.1..H
0x0040:  4f53 543a 2032 3339 2e32 3535 2e32 3535  OST:.239.255.255
0x0050:  2e32 3530 3a31 3930 300d 0a4d 414e 3a20  .250:1900..MAN:.
0x0060:  2273 7364 703a 6469 7363 6f76 6572 220d  "ssdp:discover".
0x0070:  0a4d 583a 2031 0d0a 5354 3a20 7572 6e3a  .MX:.1..ST:.urn:
0x0080:  6469 616c 2d6d 756c 7469 7363 7265 656e  dial-multiscreen
0x0090:  2d6f 7267 3a73 6572 7669 6365 3a64 6961  -org:service:dia
0x00a0:  6c3a 310d 0a55 5345 522d 4147 454e 543a  l:1..USER-AGENT:
0x00b0:  2047 6f6f 676c 6520 4368 726f 6d65 2f36  .Google.Chrome/6
0x00c0:  362e 302e 3333 3539 2e31 3831 2057 696e  6.0.3359.181.Win
0x00d0:  646f 7773 0d0a 0d0a                      dows....
```

Save captured data traffic to a file

Data traffic is captured to RAM and when the device reboots, the data is lost. To retain the captured data, first save the data to a file and then upload the file to a PC. To save captured traffic data to a file, use the **Analyze network traffic** **save** command. For example:

```
# analyzer save eth0.pcapng
File copied to: /etc/config/analyzer/eth0.pcpng
```

The file is stored in the **/etc/config/analyzer** directory. To transfer the file to your PC, see Download captured data to your PC.

Download captured data to your PC

You can download a file to your PC using the **scp** (secure copy file) command.

Linux PC

Use the following this syntax in your PC:

```
scp root@ix14_ip:/source/absolute/path/filename
/destination/absolute/path/filename
```

Option	Description
root	Login name of your Digi IX14.
ix14_ip	IP address of your host Digi IX14.
/source/absolute/path/filename	Full path of the file in the Digi IX14 tp transfer to your PC.
/destination/absolute/path/filename	Full path of the destination file in your host PC.

For example, to download the traffic saved in file **eth0.pcpng** to the **/home/john** directory for user **john** on a local PC with the IP **192.168.210.2**:

```
# scp /etc/config/analyzer/eth0.pcpng john@192.168.210.2:/home/john/eth0.pcpng


The authenticity of host '192.168.210.2 (192.168.210.2)' can't be established.
ED25519 key fingerprint is SHA256:FLKli9elWaTwqkseazuIWcnYZ7Ykjzy+By9RMZoZVg0.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/.ssh/known_hosts).
```

```
john@192.168.210.2's password:
eth0.pcpng                                    100%   11KB 851.3KB/s   00:00
```

Microsoft Windows PC

For Microsoft Windows, you can use any client with SSH support, such as **pscp**:

```
C:\>pscp.exe -scp root@ix14_ip:/source/absolute/path/filename
/destination/absolute/path/filename
```

Option	Description
root	Login name of your Digi IX14.
ix14_ip	IP address of your host Digi IX14.
/source/absolute/path/filename	Full path of the file in the Digi IX14 tp transfer to your PC.
/destination/absolute/path/filename	Full path of the destination file in your host PC.

For example, to download the traffic saved in **eth0.pcapng** file to **c:** directory of a local PC:

```
C:\>pscp.exe -scp root@192.168.210.1:/etc/config/analyzer/eth0.pcapng
C:/eth0.pcapng
Using keyboard-interactive authentication.
Password:
eth0.pcapng                | 12 kB |  13.0 kB/s | ETA: 00:00:00 | 100%
```

Clear captured data

To clear captured data traffic in RAM, use the analyzer clear command.

```
# analyzer clear
```

Note You can removed data traffic saved to a file using the **rm** (remove files) command.

Generate a support report

To generate a support report:

1. From the menu, click **System**.
2. Under **Support Report**, click **Download Report**.

Attach the support report to any support requests.