



IX14

---

User Guide

## Revision history—90002291

Revision	Date	Description
A	January 2019	Initial release of Digi IX14 firmware version 19.1.
B	September 2019	Digi IX14 firmware version 19.8 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)

## 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](http://www.digi.com/support).

## Feedback

To provide feedback on this document, email your comments to

[techcomm@digicom.com](mailto:techcomm@digicom.com)

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

# Contents

---

## What's new in Digi IX14 version 19.8

## Digi IX14 hardware reference

IX14 features and specifications .....	12
IX14 front view .....	12
IX14 back view .....	12
IX14 power supply requirements .....	13
IX14 LEDs .....	13
Digi IX14 serial connector pinout .....	14
IX14 accessory kits .....	14
IX14 antennas .....	15

## IX14 quick start

### Quick start with Digi Remote Manager mobile app

Step 1: What's in the box .....	17
Step 2: Gather accessories .....	17
Step 3: Connect hardware .....	18
Step 4: Quick setup using the Digi Remote Manager mobile app .....	19
Next steps .....	19

### Quick start with IX14 local WebUI

Step 1: What's in the box .....	20
Step 2: Gather accessories .....	20
Step 3: Connect hardware .....	21
Step 4: Sign up for Digi Remote Manager .....	22
Step 5: Access the IX14 local web interface .....	22
Step 6: Configure cellular connection using the web interface .....	23
Step 7: Add your IX14 to your Digi Remote Manager account .....	23
Next steps .....	24

## Hardware setup

Install SIM cards .....	26
Attach and position antennas .....	26
Connect the WAN/ETH1 port .....	27

Connect the serial port .....	27
Power on the IX14 .....	27

## Configuration and management

Review IX14 default settings .....	29
Reset default password for root .....	29
Configuration Options .....	30
Using the Digi Remote Manager .....	31
Access the Digi Remote Manager .....	31
Using the web interface .....	31
Log out of the web interface .....	31
Using the command line .....	32
Access the command line interface .....	32
Log in to the command line interface .....	32
Exit the command line interface .....	33

## Initial configuration

Configure cellular modem APNs .....	35
Change the default LAN subnet .....	37
Change the LAN address type .....	38
Configure SIM PIN .....	39
Configure system settings .....	39
Enable or disable Bluetooth service .....	46

## User authentication

About IX14 user authentication .....	49
Configure user authentication methods .....	49
Change the predefined authentication method .....	50
Add a new authentication method .....	51
Delete an authentication method .....	53
Rearrange the position of authentication methods .....	54
Configure authentication groups .....	57
Add an authentication group .....	57
Change the access rights for a predefined group .....	61
Delete an authentication group .....	62
Local users .....	64
Change a local user's password .....	64
Configure a local user .....	65
Delete a local user .....	71
Terminal Access Controller Access-Control System Plus (TACACS+) .....	73
TACACS+ user configuration .....	73
TACACS+ server failover and fallback to local authentication .....	74
Configure your IX14 device to use a TACACS+ server .....	74
Remote Authentication Dial-In User Service (RADIUS) .....	78
RADIUS user configuration .....	78
RADIUS server failover and fallback to local configuration .....	79
Configure your IX14 device to use a RADIUS server .....	79
Set the idle timeout for IX14 users .....	82
Example user configuration .....	84
Example 1: Administrator user with local authentication .....	84

Example 2: RADIUS, TACACS+, and local authentication for one user .....	85
---	----

## Firewall

Firewall configuration .....	91
Create a custom firewall zone .....	91
Configure the firewall zone for a network interface .....	92
Show firewall zones .....	93
Delete a custom firewall zone .....	95
Configure port forwarding .....	96
Enable or disable a port forwarding rule .....	99
Show port forwarding rules .....	101
Delete a port forwarding rule .....	102
Configure packet filtering .....	104
Enable or disable a packet filtering rule .....	107
Show packet filtering rules .....	108
Delete a packet filtering rule .....	109
Configure custom firewall rules .....	111
Configure Quality of Service options .....	112
Enable the preconfigured bindings .....	112
Create a new binding .....	114

## System administration

Review device status .....	117
Configure system information .....	118
Update system firmware .....	119
Manage firmware updates using Digi Remote Manager .....	119
Certificate management for firmware images .....	120
Update the system firmware from the WebUI .....	120
Update cellular module firmware .....	122
Reboot your IX14 device .....	122
Reboot your device immediately .....	122
Schedule reboots of your device .....	123
Reset the device to factory defaults .....	124
Configuration files .....	126
Save configuration changes .....	126
Save configuration to a file .....	127
Restore the device configuration .....	128
Schedule system maintenance tasks .....	130
Create a Virtual LAN (VLAN) route .....	135
Example: Configure VPN access with IPsec tunnels .....	137
Task One: Configure the Tunnel .....	137
Task two: Configure the firewall .....	138
Serial port .....	143
Configure the serial port .....	143
Show serial status and statistics .....	145

## Services

Allow remote access for web administration and SSH .....	148
Configure the web administration service .....	149
Configure SSH access .....	155

Use SSH with key authentication .....	160
Generating SSH key pairs .....	160
Configure telnet access .....	162
Configure DNS .....	166
Simple Network Management Protocol (SNMP) .....	172
SNMP Security .....	172
Configure Simple Network Management Protocol (SNMP) .....	172
Use the SNMP service .....	176
System time .....	176
Configure the system time .....	177
Network Time Protocol .....	179
Configure the device as an NTP server .....	179
Configure a multicast route .....	184
Enable service discovery (mDNS) .....	186

## Applications

Configure applications to run automatically .....	191
Task one: Upload the application .....	191
Task two: Configure the application to run automatically .....	192
Run a Python application at the shell prompt .....	196
Start an interactive Python session .....	197
Digidevice module .....	199
Use digidevice.cli to execute CLI commands .....	200
Use digidevice.datapoint to upload custom datapoints to Remote Manager .....	201
Use digidevice.config for device configuration .....	203
Use Python to respond to DRM SCI requests .....	205
Use digidevice runtime to access the runtime database .....	212

## Central management with Digi Remote Manager

Digi Remote Manager support .....	217
Configure Digi Remote Manager .....	217
Collect device health data and set the sample interval .....	219
Log into Digi Remote Manager .....	220
Use Digi Remote Manager to view and manage your device .....	221
Add a device to Digi Remote Manager .....	222
View Digi Remote Manager configuration and connection status .....	222
Use the Digi Remote Manager mobile app .....	223
Configure multiple devices using profiles .....	224
Learn more .....	224

## Monitoring

Enable IntelliFlow .....	226
System resources chart .....	227
Top data users chart .....	228
Top servers accessed chart .....	229
Data over time chart .....	229
Port usage chart .....	230
Change chart view options .....	230
Export chart to PNG .....	231
Print a chart .....	231

Configure NetFlow Probe .....	231
-------------------------------	-----

## Diagnostics

Generate a support report .....	236
View event and system logs .....	237
Configure syslog servers .....	239
Configure options for the event and system logs .....	240
Analyze network traffic .....	245
Start capturing packets .....	245
Define filters for capturing data traffic .....	246
Example filters for capturing data traffic .....	246
Show captured traffic data .....	247
Save captured data traffic to a file .....	248
Download captured data to your PC .....	249
Clear captured data .....	249
Use the ping command to troubleshoot network connections .....	250
Ping to check internet connection .....	250
Stop ping commands .....	250
Use the traceroute command to diagnose IP routing problems .....	250

## File system

File system .....	253
Display directory contents .....	253
Create a directory .....	253
Display file contents .....	254
Copy a file or directory .....	255
Move or rename a file or directory .....	255
Delete a file or directory .....	256
Upload and download files .....	257
Upload or download files using the Secure Copy command .....	257
Upload or download files using SFTP .....	258

## Digi IX14 regulatory and safety statements

RF exposure statement .....	261
Federal Communication (FCC) Part 15 Class B .....	261
Radio Frequency Interference (RFI) (FCC 15.105) .....	261
European Community - CE Mark Declaration of Conformity (DoC) .....	261
CE mark (Europe) .....	261
Maximum transmit power for radio frequencies .....	263
Innovation, Science, and Economic Development Canada (IC) certifications .....	263
RoHS compliance statement .....	264
Safety statements .....	264
Special safety notes for wireless routers .....	265
Product disposal instructions .....	266

## Command line interface

Access the command line interface .....	269
Log in to the command line interface .....	269
Exit the command line interface .....	270



Execute a command from the web interface .....	270
Display help for commands and parameters .....	271
The help command .....	271
The question mark (?) command .....	271
Display help for individual commands .....	272
Use the Tab key or the space bar to display abbreviated help .....	273
Auto-complete commands and parameters .....	273
Available commands .....	274
Use the scp command .....	275
Display status and statistics using the show command .....	276
show config .....	276
show system .....	277
show network .....	277
Device configuration using the command line interface .....	278
Execute configuration commands at the root Admin CLI prompt .....	278
Display help for the config command from the root Admin CLI prompt .....	278
Configuration mode .....	280
Enable configuration mode .....	280
Enter configuration commands in configuration mode .....	280
Save changes and exit configuration mode .....	281
Exit configuration mode without saving changes .....	281
Configuration actions .....	281
Display command line help in configuration mode .....	282
Move within the configuration schema .....	285
Manage elements in lists .....	285
The revert command .....	288
Enter strings in configuration commands .....	289
Example: Create a new user by using the command line .....	290
Command line reference .....	292
cp .....	293
ls .....	294
mkdir .....	295
modem at .....	296
modem at-interactive .....	297
modem pin change .....	298
modem pin disable .....	299
modem pin enable .....	300
modem pin status .....	301
modem pin unlock .....	302
modem puk status .....	303
modem puk unlock .....	304
modem reset .....	305
modem sim-slot .....	306
more .....	307
mv .....	308
ping .....	309
reboot .....	310
rm .....	311
scp .....	312
show arp .....	313
show cloud .....	314
show config .....	315
show dhcp-lease .....	316
show event .....	317
show ipsec .....	318

show log .....	319
show manufacture .....	320
show modem .....	321
show network .....	322
show openvpn client .....	323
show openvpn server .....	324
show route .....	325
show serial .....	326
show system .....	327
show version .....	328
show wifi ap .....	329
show wifi client .....	330
system backup .....	331
system factory-erase .....	332
system restore .....	333
system support-report .....	334
traceroute .....	335
update firmware .....	338

## **What's new in Digi IX14 version 19.8**

---

Digi IX14 firmware version 19.8 release.

## Digi IX14 hardware reference

---

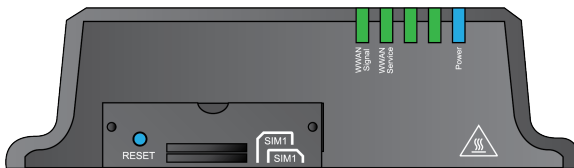
### IX14 features and specifications

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 [IX14 specifications](#) for a detailed list of IX14 hardware specifications.

### IX14 front view



Connector/port	Description
<b>SIM door</b>	See <a href="#">Install SIM cards</a> .
<b>Reset button</b>	See <a href="#">Reset the device to factory defaults</a>
<b>LEDs</b>	See <a href="#">IX14 LEDs</a> .

### IX14 back view



Port/connector	Description
<b>WAN/ETH1</b>	See <a href="#">Connect the WAN/ETH1 port</a> .
<b>SERIAL1</b>	See <a href="#">Connect the serial port</a> and <a href="#">Configure the serial port</a> .
<b>Power</b>	See <a href="#">Power on the IX14</a> .
<b>WWAN1-1</b> <b>WWAN1-2</b>	See <a href="#">Attach and position antennas</a> .

## IX14 power supply requirements

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 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 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.

## 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)

		<b>Solid green</b> Excellent signal. (-63 dBm to -51 dBm)
<b>WWAN service</b>		<b>Off</b> No cellular service
		<b>Flashing yellow</b> Cellular connection coming up
		<b>Solid yellow</b> Connected to 2G or 3G
		<b>Solid green</b> Connected to 4G
<b>WAN/ETH1 port</b>		
		<b>Solid yellow</b> 100 Mbps connection; Off for no connection
		<b>Solid green</b> Valid link detected; Flashing for Ethernet activity

## Digi IX14 serial connector pinout

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

Signal name	RS232 signal	DTE signal direction	DB9 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

## IX14 accessory kits

Digi offers the following 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 [IX14 product page](#) and click **Part numbers and accessories** for details.

## IX14 antennas

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

## IX14 quick start

---

Congratulations on your 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 IX14 local WebUI**

If you do not have a smart phone or tablet, access the IX14 local WebUI to manually set up your IX14. Go to [Quick start with IX14 local WebUI](#).



## Quick start with Digi Remote Manager mobile app

---

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

**Note** If you do not have a smart phone or tablet, access the IX14 local WebUI to manually set up your IX14. Go to [Quick start with IX14 local WebUI](#).

---

### Step 1: What's in the box

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

- **Welcome card**  
Links to this *Quick start*.
- **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.
- **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 IX14 purchase. See [Digi Remote Manager product page](#) to learn about Digi Remote Manager features.

---

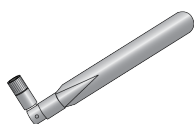
### Step 2: Gather accessories

---

**Note** Digi offers several IX14 accessory kits so you can purchase exactly what you need to support your IX14. See [IX14 accessory kits](#) for details or go to [IX14 support](#).

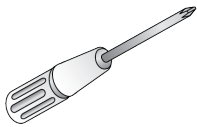
---

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



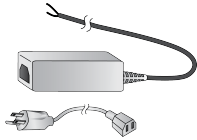
#### **Antennas**

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



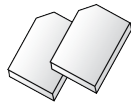
**Phillips-head screwdriver**

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.

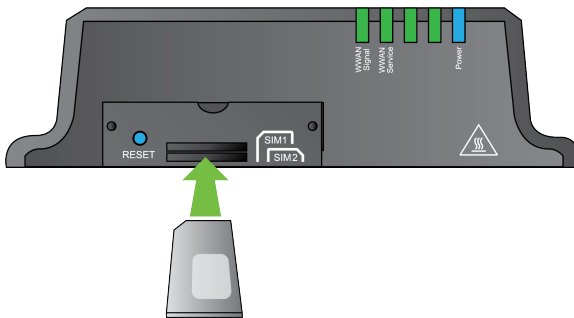


**Laptop or personal computer**

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

### Step 3: Connect hardware

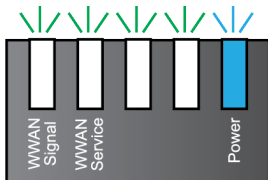
- a. Install SIM card(s). See [Install SIM cards](#).



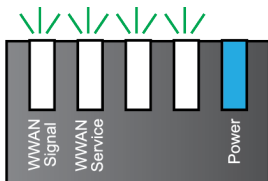
- b. Attach antenna(s). See [Attach and position antennas](#).



- c. Power on the IX14 by connecting a DC power source. See [IX14 power supply requirements](#) for 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 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 IX14 label.
- Configure your IX14 cellular interface.
- Connect your device to Digi Remote Manager using the cellular connection.

Here's how:

- Download the **Digi Remote Manager** mobile app from the [App Store](#) (iPhone) or [Google Play](#) (Android).
- Click **Log in or Sign Up** and then click **Sign up** to create a new account.
- You'll receive an email with login instructions.
- From the **Digi Remote Manager** mobile app, click **Log in** and log into your new account.
- 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 IX14. The IX14 does not appear in your mobile OS Bluetooth settings—the IX14 Bluetooth connection status displays within the **Digi Remote Manager** mobile app only.

---

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

## Next steps

Congratulations! You have completed the *Quick start*.

- ✓ To manage and configure your IX14 remotely using Digi Remote Manager, see [Configure Digi Remote Manager](#).
- ✓ To manage and configure your IX14 locally using the local web interface, see [Using the web interface](#).

## Quick start with IX14 local WebUI

---

The following steps guide you through the IX14 setup using the IX14 local WebUI.

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

---

### Step 1: What's in the box

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

- **Welcome card**  
Links to this *Quick start*.
- **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.
- **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 IX14 purchase. See [Digi Remote Manager product page](#) to learn about Digi Remote Manager features.

---

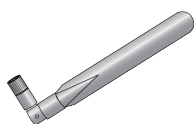
### Step 2: Gather accessories

---

**Note** Digi offers several IX14 accessory kits so you can purchase exactly what you need to support your IX14. See [IX14 accessory kits](#) for details or go to [IX14 support](#).

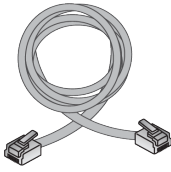
---

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



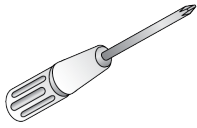
#### **Antennas**

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



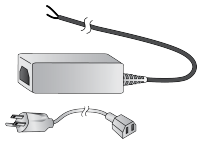
**Ethernet cable**

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



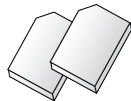
**Phillips-head screwdriver**

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.



**SIM card(s)**

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

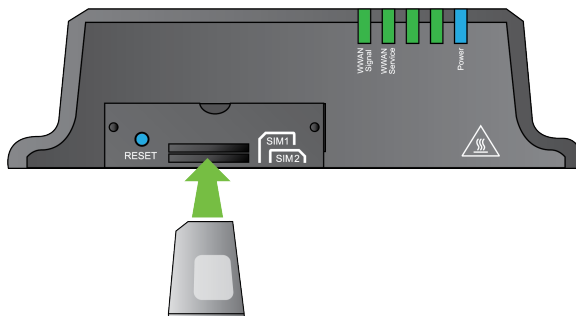


**Laptop or personal computer**

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

## Step 3: Connect hardware

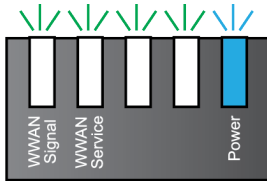
- a. Install SIM card(s). See [Install SIM cards](#).



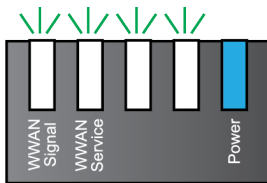
- b. Attach antenna(s). See [Attach and position antennas](#).



- c. Use an Ethernet cable to connect your IX14 **WAN/ETH1** port to your PC.
- d. Power on the IX14 by connecting a DC power source. See [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 IX14 is ready.



## Step 4: Sign up for Digi Remote Manager

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

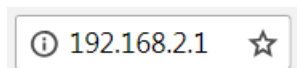
- a. Click [Sign Up](#) to create a new account.
- b. You'll receive an email with login instructions.
- c. Click on the link in the email to log into Digi Remote Manager.

## Step 5: Access the IX14 local web interface

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



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



- c. Log into the 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).

When you log into the product, you will be required to change the factory-assigned default password. See [Reset default password for root](#) for further information.

The IX14 local WebUI 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 [IX14 LEDs](#).

## Step 7: Add your 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 [Sign up for Digi Remote Manager](#), look for the Digi Remote Manager email that provides your login credentials.)
- c. Click **Device Management**.
- d. Click **Add Devices**.



The screenshot shows a web form for adding a device. It contains two rows of input fields. The first row has a label 'MAC Address:' followed by a dropdown menu and an empty text box. The second row has a label 'Install Code:' followed by an empty text box. To the right of the first row is a button labeled 'Add'.

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 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 IX14 remotely using Digi Remote Manager, see [Configure Digi Remote Manager](#).
- ✓ To manage and configure your IX14 locally using the local web interface, see [Using the web interface](#).



## Hardware setup

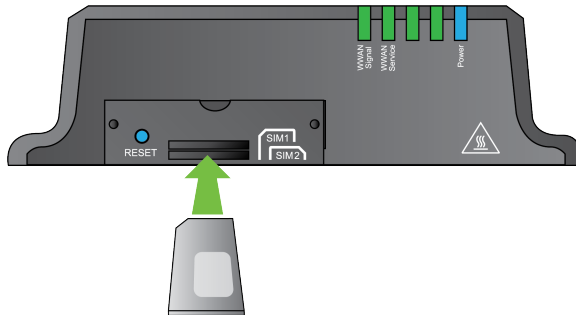
---

Install SIM cards .....	26
Attach and position antennas .....	26
Connect the WAN/ETH1 port .....	27
Connect the serial port .....	27
Power on the IX14 .....	27

## Install SIM cards

To install SIM cards:

1. On the IX14 front panel, use a #1 Phillips-head screwdriver to remove the SIM door.
2. If the 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 IX14 does not include a power supply or antennas. See [IX14 accessory kits](#) for information on IX14 power supplies and antennas.

- Connect 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 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 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. The default serial port configuration for the IX14 device is:

- Baud rate: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

See [Configure the serial port](#).

## Power on the IX14

---

**Note** The IX14 does not include a power supply or antennas. See [IX14 accessory kits](#) for information on IX14 power supplies and antennas.

---

1. Power on the IX14 by connecting a DC power source. If you are using a non-Digi power supply, see [IX14 power supply requirements](#).
2. **Power** LED is solid 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 IX14 is ready.

## Configuration and management

---

Review IX14 default settings .....	29
Reset default password for root .....	29
Configuration Options .....	30
Using the Digi Remote Manager .....	31
Access the Digi Remote Manager .....	31
Using the web interface .....	31
Using the command line .....	32
Access the command line interface .....	32
Log in to the command line interface .....	32
Exit the command line interface .....	33

## Review IX14 default settings

The following table lists factory default settings for the IX14.

<b>Central management</b>	<ul style="list-style-type: none"> <li>■ Digi Remote Manager enabled as the central management service.</li> </ul>
<b>Interface priorities</b>	<ul style="list-style-type: none"> <li>■ Modem (cellular) is WAN interface with metric of 3.</li> <li>■ LAN (Ethernet) with metric of 5.</li> </ul>
<b>Modem configuration</b>	<ul style="list-style-type: none"> <li>■ SIM failover after 5 attempts.</li> </ul>
<b>Network settings</b>	<ul style="list-style-type: none"> <li>■ LAN subnet of 192.168.2.1/24.</li> <li>■ DHCP enabled.</li> <li>■ Source NAT enabled (outbound traffic).</li> </ul>
<b>Security policies</b>	<ul style="list-style-type: none"> <li>■ Packet filtering allows all outbound traffic.</li> <li>■ SSH, web admin, and local admin access enabled.</li> </ul>
<b>Services</b>	<ul style="list-style-type: none"> <li>■ 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.</li> </ul>
<b>Monitoring</b>	<ul style="list-style-type: none"> <li>■ Device health metrics uploaded to Digi Remote Manager at 60 minute interval.</li> </ul>

## Reset default password for root

When you first log into the WebUI or the command line, you will be required to change the factory-assigned default password for the user **root** prior to being able to save any changes or exit the user interface.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Users > root**.
4. Enter a new password for the root user.
5. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

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

3. Enter a new password by using the following command:

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

4. Save the configuration and apply the change:

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

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

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

## Configuration Options

There are two primary methods for configuring your IX14 device:

- Web interface.

The web interface can be accessed in two ways:

- Central management using the Digi Remote Manager, a cloud-based device management and data enablement platform that allows you to connect any device to any application, anywhere. With the Remote Manager, you can configure your IX14 device and use the configuration as a basis for a profile which can be applied to other similar devices. See [Using the Digi Remote Manager](#) for more information about using the Remote Manager to manage and configure your IX14 device.
- The local web interface. See [Using the web interface](#) for more information about using the local web interface to manage and configure your IX14 device.

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

- Command line.

A robust command line allows you to perform all configuration and management tasks from within a command shell. Both the Remote Manager and the local web interface also have the option to open a terminal emulator for executing commands on your IX14 device. See [Using the command line](#) for more information about using the command line to manage and configure your IX14 device.

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

 **WebUI**

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

 **Command line**

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

## Using the Digi Remote Manager

By default, your IX14 device is configured to use Digi Remote Manager as its central management server. No configuration changes are required to begin using the Remote Manager.

For information about configuring central management for your IX14 device, see [Central management with Digi Remote Manager](#).

## Access the Digi Remote Manager

To access the Digi Remote Manager:

1. If you have not already done so, go to <https://myaccount.digi.com/> to sign up for a Digi Remote Manager account.

Check your email for Digi Remote Manager login instructions.

2. Go to [remotemanager.digi.com](https://remotemanager.digi.com).
2. Enter your username and password.

The Digi Remote Manager Dashboard appears.

## Using the web interface

To connect to the IX14 local WebUI:

1. Use an Ethernet cable to connect the 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.

The screenshot displays the Digi IX14 web interface. At the top, the Digi logo is on the left, followed by 'Digi IX14' and the MAC address '000000000000'. On the right, there are signal strength indicators, '4G' and 'LTE' labels, and a 'Manage Device' button with 'State: Connected' below it. The main content area is divided into a left sidebar with navigation options (Status, Configuration, Events, Applications, System Logs, Terminal, System, Log out (admin)) and a central 'Device Details' section. The 'Device Details' section includes a table with the following information:

Device	
MAC Address:	000000000000
Serial:	IX14-000077
Model:	Digi IX14
Firmware Version:	19.8.1.30
Firmware Build Date:	Fri, 16 Aug 2019 12:38:58 +0000
Digi Remote Manager:	Connected
Uptime:	8 days, 17 hours, 14 minutes, 33 seconds
Local Time:	Wed, 21 Aug 2019 14:43:35 +0000
Load Average:	0.38, 0.48, 0.45

## Log out of the web interface

- At the main menu, click **Log out**.

## Using the command line

The Digi IX14 device provides a command-line interface that you can use to configure the device, display status and statistics, update firmware, and manage device files.

See [Command line interface](#) for detailed instructions on using the command line interface, and see [Command line reference](#) for information on available commands.

## Access the command line interface

You can access the IX14 command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

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

To access the command line, your device must be configured to allow access, and you must log in with a user who has been configured for the appropriate access. For further information about configuring access to these services, see:

- Serial: [Configure the serial port](#)
- WebUI: [Configure the web administration service](#)
- SSH: [Configure SSH access](#)
- Telnet: [Configure telnet access](#)

## Log in to the command line interface

### Command line

1. Connect to the IX14 device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See [Access the command line interface](#) for more information.
  - For serial connections, the default configuration is:
    - **115200** baud rate
    - **8** data bits
    - **no** parity
    - **1** stop bit
    - **no** flow control
  - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** on the WAN/ETH1 .
2. At the login prompt, enter the username and password of a user with Admin access:

---

```
login: root
Password: *****
```

---

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



- Depending on your device model and the configuration of your user, you may be presented with another menu, for example:

---

Access selection menu:

```
a: Admin CLI
1: Serial: port1      (9600,8,1,none,none)
2: Serial: port2      (9600,8,1,none,none)
q: Quit
```

---

Select access or quit [admin] :

---

Type **a** or **admin** to access the IX14 command line.

You will now be connected to the Admin CLI:

---

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

>

---

## Exit the command line interface

### Command line

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

---

```
> exit
```

---

- Depending on your device model and the configuration of your user, you may be presented with another menu, for example:

---

Access selection menu:

```
a: Admin CLI
1: Serial: port1      (9600,8,1,none,none)
2: Serial: port2      (9600,8,1,none,none)
q: Quit
```

---

Select access or quit [admin] :

---

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

## Initial configuration

---

Configure cellular modem APNs .....	35
Change the default LAN subnet .....	37
Change the LAN address type .....	38
Configure SIM PIN .....	39
Configure system settings .....	39
Enable or disable Bluetooth service .....	46

## Configure cellular modem APNs

The IX14 device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. However, you can configure the system to use an APN.

To configure the APN:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Modem > APN list**.
4. Click **Add**.
5. For **APN**, type the Access Point Name (APN) to be used when connecting to the cellular carrier.
6. (Optional) **IP version**:

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

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

The default is **Automatic**.

7. (Optional) **Authentication method**:  
For **Authentication method**, select one of the following:
  - **None**: No authentication is required.
  - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
  - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
  - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

If **Automatic**, **CHAP**, or **PAP** is selected, enter the **Username** and **Password** required to authenticate.

The default is **None**.

8. Repeat this procedure to configuration additional APNs.
9. (Optional) To configure the device to bypass its preconfigured APN list and only use the configured APNs, click **Modem** and enable **APN list only**.
10. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. At the config prompt, type:

---

```
(config)> add modem modem apn end
(config network interface modem modem apn 1)>
```

---

4. Set the APN:

---

```
(config network interface modem modem apn 1)> APN 12345
(config network interface modem modem apn 1)>
```

---

5. (Optional) Set the IP version:

---

```
(config network interface modem modem apn 1)> ip_version version
(config network interface modem modem apn 1)>
```

---

where *version* is one of the following:

- **auto**: Requests both IPv4 and IPv6 address.
- **ipv4**: Requests only an IPv4 address.
- **ipv6**: Requests only an IPv6 address.

The default is **auto**.

6. (Optional) Set the authentication method:

---

```
(config network interface modem modem apn 1)> auth method
(config network interface modem modem apn 1)>
```

---

where *method* is one of the following:

- **none**: No authentication is required.
- **auto**: The device will attempt to connect using CHAP first, and then PAP.
- **chap**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
- **pap**: Uses the Password Authentication Profile (PAP) to authenticate.

If **auto**, **chap**, or **pap** is selected, enter the **Username** and **Password** required to authenticate:

---

```
(config network interface modem modem apn 1)> username name
(config network interface modem modem apn 1)> password pwd
(config network interface modem modem apn 1)>
```

---

The default is **none**.

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

---

```
(config network interface modem modem apn 1)> .. .. apn_lock true
(config network interface modem modem apn 1)>
```

---

8. Save the configuration and apply the change:

---

```
(config network interface modem modem apn 1)> save
Configuration saved.
>
```

---

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

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

## Change the default LAN subnet

You can change the 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:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Network > Interfaces > LAN > IPv4**.
4. For **Address**, change the IP address to an alternate private IP. You must also specify the subnet mask. It must have the syntax of *IPv4\_address/netmask*.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, set the IP address to an alternate private IP:

---

```
(config)> network interface lan ipv4 address IPv4_address/netmask
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

## Change the LAN address type

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

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Network > Interfaces > LAN > IPv4**.
4. For the **Type** option, select **DHCP address**.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:  

---

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

---
3. At the config prompt, set the LAN to use a DHCP address:  

---

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

---
4. Save the configuration and apply the change:  

---

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

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

## Configure SIM PIN

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

### WebUI

1. Click **Configuration** > **Modem**.
2. Enter the PIN in the **PIN** field.
3. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, set the SIM PIN:

---

```
(config)> modem modem pin pin
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

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

## Configure system settings

To configure system settings:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System**.

4. Provide the system information settings:
  - **Name:** (Optional) Enter a name for the device. The name will appear in log messages and at the command line prompt.
  - **Contact:** (Optional) Enter a contact for the device.
  - **Location:** (Optional) Enter a location for the device.
  - **Description:** (Optional) Enter a description for the device.
  - **Banner:** (Optional) Enter banner text to appear when a user logs into the device.
5. Expand **Scheduled tasks:**
  - **Reboot time:** (Optional) If you want to reboot the system daily, enter the time for the daily reboot.
  - Expand **System maintenance.**
    - **Start time/Duration window:** Enter a start time and duration window for system maintenance.
    - **Frequency:** Enter the frequency for the maintenance window.
    - Select **Modem firmware update** to enable the update of modem firmware during the maintenance window.
6. If you want to add **Custom scripts**, click **Add** and configure the script. See [Schedule system maintenance tasks](#) for more information.
7. Configure Time:
  - **Timezone:** Select the timezone for the IX14.
  - **NTP servers:** If you want to add an NTP server, click **ADD** and specify the URL for the server.
8. Configure Log options:
  - **Heartbeat interval:** Enter the minimum time between sending heartbeat status events.
  - **Event categories:** Open the Event categories and enable/disable the event categories you want to log.
9. Expand **Server list** and click **Add** to configure an additional syslog server.
10. Select **Preserve system logs** to keep the current system logs when the device is rebooted.
11. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:
 

---

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

---
3. Provide the system information settings:
  - (Optional) Set a name for the device. This name will appear in log messages and at the command prompt.



---

```
(config)> system name 192.168.3.1
(config)>
```

---

- (Optional) Set the contact for the device:

---

```
(config)> system contact "Jane User"
(config)>
```

---

- (Optional) Set the location for the device:

---

```
(config)> system location "9350 Excelsior Blvd., Suite 700, Hopkins, MN"
(config)>
```

---

- (Optional) Set the banner for the device. This is displayed when users access terminal services on the device.

---

```
(config)> system banner "Welcome to the Digi IX14."
(config)>
```

---

#### 4. Configure scheduled tasks:

- Set the reboot time:

---

```
(config)> system schedule reboot_time time
(config)>
```

---

where *time* is the time of the day that the device should reboot, using the format *HH:MM*.

- Schedule maintenance tasks:

- Configure the time of day that the maintenance window should start, using the syntax *HH:MM*. If the start time is not set, maintenance tasks are not scheduled and will not be run.

---

```
(config)> system schedule maintenance from HH:MM
(config)>
```

---

- Configure the duration length (the amount of time that the maintenance tasks will be run). If **0** is used, all scheduled tasks will begin at the start time as defined in the previous step.

---

```
system schedule maintenance length num
(config)>
```

---

where *num* is any whole number between **0** and **24**.

- Configure the frequency that the maintenance tasks should be run:

---

```
system schedule maintenance frequency value
(config)>
```

---

where *value* is either **daily** or **weekly**. **daily** is the default.

- Configure the device to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. The device will look for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

---

```
system schedule maintenance modem_fw_update value
(config)>
```

---

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

- Allow for the configuration to be updated, including by custom scripts, during the maintenance window:

---

```
system schedule maintenance config_check value
(config)>
```

---

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

5. If you want to add custom scripts, see [Schedule system maintenance tasks](#) for more information.
6. (Optional) Set the timezone for the location of your IX14 device. The default is **UTC**.

---

```
(config)> system time timezone value
(config)>
```

---

Where *value* is the timezone using the format specified with the following command:

---

```
(config)> system time timezone ?
```

---

Timezone: The timezone for the location of this device. This is used to adjust the time for log messages. It also affects actions that occur at a specific time of day.

Format:

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
```

---

```
(config)>
```

---

7. (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.

---

```
(config)> add ntp server end time.server.com
(config)>
```

---

8. Configure log options:

- (Optional) Set the minimum time between sending heartbeat status events.

---

```
(config)> system log heartbeat_interval value
(config)>
```

---

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

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

---

```
(config)> system log heartbeat_interval 600s
(config)>
```

---

The default is 30 minutes.

- (Optional) By default, all event categories are enabled for logging. To disable an event category, or to change the status interval:

---

**Note** Status events create periodic reports of the status of the applicable event, rather than reporting when changes occur. The status interval determines how often the status event is reported. The value of the status interval uses the format *number{w|d|h|m|s}*.

---

- Disable informational logging of arping events:

---

```
(config)> system log event arping info false
(config)>
```

---

- Disable error and informational logging of configuration updates:

---

```
(config)> system log event config error false
(config)> system log event config info false
(config)>
```

---

- Disable informational and status event logging of DHCP server events, or change the status interval for DHCP status event logging from the default of 30 minutes:

---

```
(config)> system log event dhcpserver info false
(config)> system log event dhcpserver status false
(config)> system log event dhcpserver status_interval value
(config)>
```

---

- Disable error and status event logging of firmware events, or change the status interval for firmware status event logging from the default of 30 minutes:

---

```
(config)> system log event firmware error false
(config)> system log event firmware status false
(config)> system log event firmware status_interval value
(config)>
```

---

- Disable status events related to location information, or change the status interval for location status event logging from the default of 30 minutes:

---

```
(config)> system log event location status false
(config)> system log event location status_interval value
(config)>
```

---

- Disable status events related to modem information, or change the status interval for modem status event logging from the default of 5 minutes:

---

```
(config)> system log event modem status false
(config)> system log event modem status_interval value
(config)>
```

---

- Disable error and informational logging of active recovery tests:

---

```
(config)> system log event netmon error false
(config)> system log event netmon info false
(config)>
```

---

- Disable status events related to the addresses and routes of network interfaces, or change the status interval for network status event logging from the default of 5 minutes:

---

```
(config)> system log event network status false
(config)> system log event network status_interval value
(config)>
```

---

- Disable status events related to OpenVPN events, or change the status interval for OpenVPN status event logging from the default of 5 minutes:

---

```
(config)> system log event openvpn status false
(config)> system log event openvpn status_interval value
(config)>
```

---

- Disable informational logging of remote control commands:

---

```
(config)> system log event remote info false
(config)>
```

---

- Disable informational logging when the device restarts:

---

```
(config)> system log event restart info false
(config)>
```

---

- Disable informational logging of serial status events:

---

```
(config)> system log event serial info false
(config)>
```

---

- Disable informational logging of SMS messages:

---

```
(config)> system log event sms info false
(config)>
```

---

- Disable error or informational logging of speed test results:

---

```
(config)> system log event speed error false
(config)> system log event speed info false
(config)>
```

---

- Disable status events related to network statistics, or change the status interval for network statistics event logging from the default of 30 minutes:

---

```
(config)> system log event network status false
(config)> system log event network status_interval value
(config)>
```

---

- Disable informational logging of user access events:

```
(config)> system log event user info false
(config)>
```

- Disable informational logging of Wake-On-LAN (WOL) remote control commands:

```
(config)> system log event wol info false
(config)>
```

9. To keep the current system logs when the device is rebooted:

```
(config)> system log persistent true
(config)>
```

10. (Optional) Configure additional syslog servers:

- a. Add the additional syslog server:

```
(config)> add system log remote end
(config system log remote 1)>
```

- b. Enable the syslog server:

```
(config system log remote 1)> enable true
(config system log remote 1)>
```

- c. Set the syslog server URL:

```
(config system log remote 1)> server log.server.com
(config system log remote 1)>
```

- d. Determine the types of events to be sent to this server:

- To send error events:

```
(config system log remote 1)> error true
(config system log remote 1)>
```

- To send informational events:

```
(config system log remote 1)> info true
(config system log remote 1)>
```

- To send status events:

```
(config system log remote 1)> status true
(config system log remote 1)>
```

11. Save the configuration and apply the change:

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

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

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

## Enable or disable Bluetooth service

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

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > Bluetooth**.
4. Enable or disable the Bluetooth service as needed.
5. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable or disable the Bluetooth service:

- To enable the Bluetooth service:

---

```
(config)> service bluetooth enable true
(config)>
```

---

- To disable the Bluetooth service:

---

```
(config)> service bluetooth enable false
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

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

---

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

---

## User authentication

---

About IX14 user authentication .....	49
Configure user authentication methods .....	49
Configure authentication groups .....	57
Local users .....	64
Terminal Access Controller Access-Control System Plus (TACACS+) .....	73
Remote Authentication Dial-In User Service (RADIUS) .....	78
Set the idle timeout for IX14 users .....	82
Example user configuration .....	84



## About IX14 user authentication

As released, a IX14 is configured with the following user 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**, **TACACS+**, or **RADIUS**. 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 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.
- **RADIUS:** Remote Authentication Dial-In User Service servers and users. By default, RADIUS is not configured.

## Configure user authentication methods

To configure user authentication methods, you must be logged in to the IX14 device as a user with Admin access.

### *Required configuration items*

- The types of authentication method to be used:
  - Local user authentication.  
See [Local users](#) for information about configuring local user authentication.
  - Users authenticated by using a remote RADIUS server for authentication.  
See [Remote Authentication Dial-In User Service \(RADIUS\)](#) for information about configuring RADIUS authentication.
  - Users authenticated by using a remote TACACS+ server for authentication.  
See [Terminal Access Controller Access-Control System Plus \(TACACS+\)](#) for information about configuring TACACS+ authentication.

Multiple types of authentication can be defined for IX14 users. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned.

## Change the predefined authentication method

By default, one authentication method is predefined and uses local users authentication. To change the authentication type used by the predefined method:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Methods**.
4. For the predefined method, select the appropriate method from the **Method** drop-down.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:  

---

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

---
3. Delete the existing method:  

---

```
(config)> del auth method 0
(config)>>
```

---
4. Add the new method:  

---

```
(config)> add auth method end auth_type
(config)>
```

---

where *auth\_type* is one of **local**, **radius**, or **tacacs+**.
5. Save the configuration and apply the change:  

---

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

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

## Add a new authentication method

To add an authentication method:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Methods**.
4. Click **Add**.
5. Select the appropriate authentication type for the new method from the **Method** drop-down.

---

**Note** Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. See [Rearrange the position of authentication methods](#) for information about how to reorder the authentication methods.

---

6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This procedure describes how to add methods to various places in the list.

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Add the new authentication method to the appropriate location in the list:

- To determine the current list of authentication methods:

- a. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- b. At the command line, type **config** to enter configuration mode:

---

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

---

- c. Use the **show auth method** command to display the current authentication methods configuration:

---

```
(config)> show auth method
0 local
(config)>
```

---

- To add the new authentication method to the beginning of the list, use the index value of **0** to indicate that it should be added as the first method:

---

```
(config)> add auth method 0 auth_type
(config)>
```

---

where *auth\_type* is one of **local**, **radius**, or **tacacs+**.

- To add the new authentication method to the end of the list, use the index keyword **end**:

---

```
(config)> add auth method end auth_type
(config)>
```

---

where *auth\_type* is one of **local**, **radius**, or **tacacs+**.

- To add the new authentication in another location in the list, use an index value to indicate the appropriate position. For example:

---

```
(config)> add auth method 1 auth_type
(config)>
```

---

where *auth\_type* is one of **local**, **radius**, or **tacacs+**.

- You can also use the **move** command to rearrange existing methods. See [Rearrange the position of authentication methods](#) for information about how to reorder the authentication methods.

4. Save the configuration and apply the change:

---

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

---

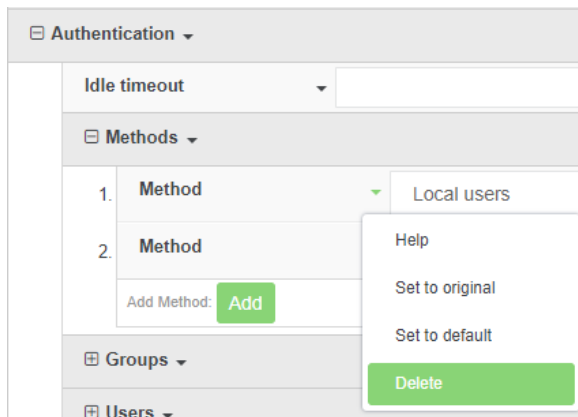
5. Type **exit** to exit the Admin CLI.

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

## Delete an authentication method

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Methods**.
4. Click the down arrow (▼) next to the field label and select **Delete**.



5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Use the **show auth method** command to determine the index number of the authentication method to be deleted:

---

```
(config)> show auth method
0 local
1 radius
2 tacacs+
(config)>
```

---

4. Delete the appropriate authentication method:

```
(config)> del auth method n
```

Where *n* is index number of the authentication method to be deleted. For example, to delete the TACACS+ authentication method as displayed by the example **show** command, above:

```
(config)> del auth method 2
```

5. Save the configuration and apply the change:

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

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

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

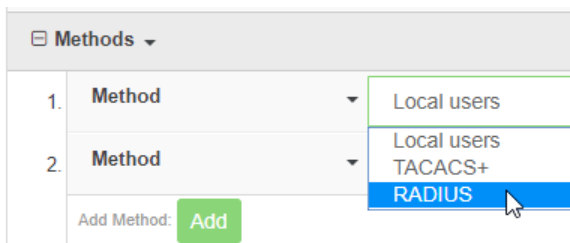
## Rearrange the position of authentication methods

Authentication methods are reordered by changing the method type in the **Method** drop-down for each authentication method to match the appropriate order.

For example, if a configuration currently has **Local users** as the first method, and **RADIUS** as the second, to reorder these so that **RADIUS** is first and **Local users** is second:

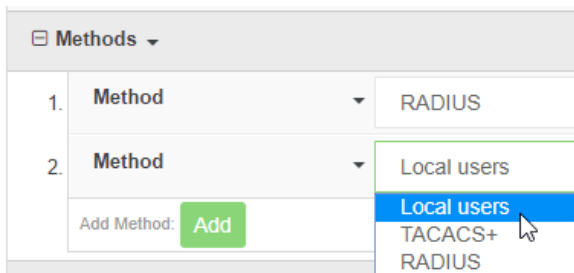
### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click to expand the first **Method**.
4. In the **Method** drop-down, select **RADIUS**.



5. Click to expand the second **Method**.

- In the **Method** drop-down, select **Local users**.



- Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

- Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

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

- Use the **show** command to display current configuration:

```
(config)> show auth method
0 local
1 radius
(config)>
```

- Use the **move** command to rearrange the methods:

```
(config)> move auth method 1 0
(config)>
```

- Use the **show** command again to verify the change:

```
(config)> show auth method
0 radius
1 local
(config)>
```

- Save the configuration and apply the change:

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

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

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



## Configure authentication groups

Authentication groups are used to assign access rights to IX14 users. Three types of access rights can be assigned:

- **Admin access:** Users with Admin access have the ability to manage the IX14 device by using the WebUI or the CLI.
- **Shell access:** Users with Shell access have the ability to access the shell when logging into the IX14 via telnet, ssh, or the serial console.
- **Serial access:** Users with Serial access have the ability to log into the IX14 device by using the serial console.

### ***Preconfigured authentication groups***

The IX14 device has two preconfigured authentication groups:

- The admin group is configured by default to have Admin access.
- The serial group is configured by default to have Serial access.

The preconfigured authentication groups cannot be deleted, but the access rights defined for the group are configurable.

## Add an authentication group

### **Required configuration items**

- The access rights to be assigned to users: one or more of the following:
  - Admin access
  - Shell access
  - Serial access

Multiple types of access rights can be included in the same authentication group.

### **Additional configuration items**

- Access rights to OpenVPN tunnels, and the tunnels to which they have access.
- Access rights to captive portals, and the portals to which they have access.
- Access rights to query the device for Nagios monitoring.

To add an authentication group:

### **WebUI**

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Groups**.
4. For **Add Group**, type a name for the group.
5. Click **Add**.

6. Click the box next to the following options, as appropriate, to enable or disable access rights for each:
  - **Admin access**
  - **Shell access**
  - **Serial access**
7. (Optional) Configure OpenVPN access:
  - a. Enable OpenVPN access rights for users of this group by checking the box next to **OpenVPN access**.
  - b. Click **OpenVPN** to expand the **OpenVPN** node.
  - c. Click **Add**.
  - d. In the **Tunnel** dropdown, select an OpenVPN tunnel to which users of this group will have access.
  - e. Click **Add** again to add additional OpenVPN tunnels.
8. (Optional) Configure captive portal access:
  - a. Enable captive portal access rights for users of this group by checking the box next to **Captive portal access**.
  - b. Click **Captive portals** to expand the **Captive portal** node.
  - c. Click **Add**.
  - d. In the **Captive portal** dropdown, select a captive portal to which users of this group will have access.
  - e. Click **Add** again to add additional captive portals.
9. (Optional) Enable the user to query the device for Nagios monitoring by checking the box next to **Nagios access**.
10. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:
 

```
> config
(config)>
```
3. Use the **add auth group** command to add a new authentication. For example, to add a group named **test**:
 

```
(config)> add auth group test
(config auth group test)>
```
4. Enable access rights for the group:
  - Admin access:
 

```
(config auth group test)> acl admin enable true
```

- Shell access:

---

```
(config auth group test)> acl shell enable true
```

---

- Serial access:

---

```
(config auth group test)> acl serial enable true
```

---

5. (Optional) Configure OpenVPN access:

- a. Enable OpenVPN access rights for users of this group:

---

```
(config auth group test)> acl openvpn enable true
```

---

- b. Add an OpenVPN tunnel to which users of this group will have access:

- i. Return to the config prompt by typing three periods (...):

---

```
(config auth group test)> ...
```

---

- ii. Determine available tunnels:

---

```
(config)> show vpn openvpn
no client
server
    vpnservers
        acl
            no address
            no address6
            no interface
            no zone
        advanced_options
            enable false
            no extra
            override false
        authentication passwd
        autogenerate false
        cacert 1
        device_type tun
        diffie 1
        enable true
        metric 0
        port 1194
        no server_address
        server_cert 1
        server_first_ip 80
        server_key 1
        server_last_ip 99
        zone external

(config)>
```

---

- iii. Add a tunnel:

```
(config)> add auth group test acl openvpn tunnels end
/vpn/openvpn/server/vpnserver
```

6. (Optional) Configure captive portal access:

- a. Enable captive portal access rights for users of this group:

```
(config)> auth group test acl portal enable true
```

- b. Add a captive portal to which users of this group will have access:

- i. Determine available portals:

```
(config)> show firewall portal
portal1
    auth none
    enable true
    http redirect
    no interface
    no message
    no redirect_url
    no terms
    timeout 24h
    no title
(config)>
```

- ii. Add a captive portal:

```
(config)> add auth group test acl portal portals end portal1
```

7. (Optional) Configure Nagios monitoring:

```
(config)> auth group group test acl nagios enable true
```

8. Save the configuration and apply the change:

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

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

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

## Change the access rights for a predefined group

By default, two authentication groups are predefined: **admin** and **serial**. To change the access rights of the predefined groups:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Groups**.
4. Click the predefined authentication group to be changed, either **admin** or **serial**, to expand its configuration node.
5. Click the box next to the following options, as appropriate, to enable or disable access rights for each:
  - **Admin access**
  - **Shell access**
  - **Serial access**
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable or disable access rights for the group. For example:

- Admin access:

- To disable Admin access for the **admin** group:

---

```
(config)> auth group admin acl admin enable false
```

---

- Shell access:

- To enable Shell access for the **serial** group:

---

```
(config)> auth group serial acl shell enable true
```

---

- Serial access:

- To enable Serial access for the **admin** group:

---

```
(config)> auth group admin acl serial enable true
```

---

4. Save the configuration and apply the change:

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

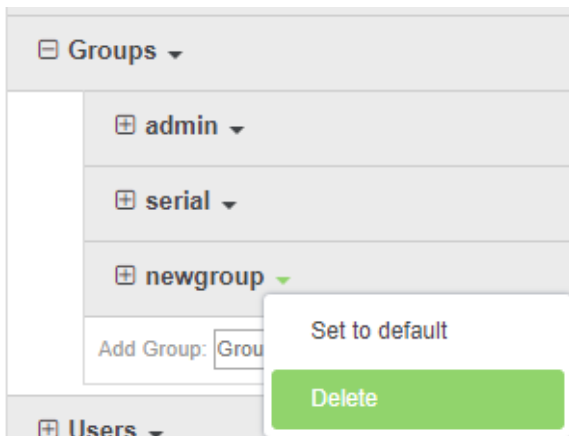
5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete an authentication group

To delete an authentication group from your IX14:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Groups**.
4. Click the down arrow (▼) next to the name of the user to be deleted and select **Delete**.



5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:  

---

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

---
3. At the config prompt, type:  

---

```
(config)> del auth group groupname
```

---
4. Save the configuration and apply the change:  

---

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

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

## Local users

Local users are authenticated on the device without using an external authentication mechanism such as TACACS+ or RADIUS. Local user authentication is enabled by default, with one preconfigured default user.

### Default user

At manufacturing time, each IX14 device comes with a default user configured as follows:

- Username: **root**.
- Password: The default password is displayed on the label on the bottom of the device.

---

**Note** The default password is a unique password for the device, and is the most critical security feature for the device. If you reset the device to factory defaults, you must log in using the default user and password, and you should immediately [change the password](#) to a custom password. Before deploying or mounting the IX14 device, record the default password, so you have the information available when you need it even if you cannot physically access the label on the bottom of the device.

---

The default **root** user is preconfigured with both Admin and Serial access. You can configure the **root** user account to fit with the needs of your environment.

## Change a local user's password

To change a user's password:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Users**.
4. Click the username to expand the user's configuration node.
5. For **Password**, enter the new password.
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.



 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, type:

---

```
(config)> auth user username password pwd
```

---

Where:

- *username* is the name of the user.
  - *pwd* is the new password for the user.
4. Save the configuration and apply the change:

---

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

---

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

## Configure a local user

To add, modify, or delete a user, you must be assigned the **super** access level. See [Local users](#) for descriptions of user access levels.

To configure a user, you need to configure the following:

### Required configuration items

- A username.
- A password. For security reasons, passwords are stored in hash form. There is no way to get or display passwords in clear-text form.
- The authentication group or groups from which the user will inherit access rights. See [Configure authentication groups](#) for information about configuring groups.

### Additional configuration items

- An optional public ssh key, to authenticate the user when using passwordless SSH login.
- Two-factor authentication information for user login over SSH, the serial console, and telnet:
  - The verification type for two-factor authentication: Either time-based or counter-based.
  - The security key.
  - Whether to allow passcode reuse (time based verification only).
  - The passcode refresh interval (time based verification only).

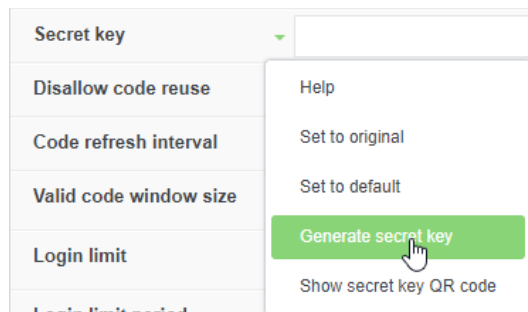
- The valid code window size.
- The login limit.
- The login limit period.
- One-time use eight-digit emergency scratch codes.

To configure a local user:

## WebUI

1. Log into the IX14 WebUI as a user with Admin access.
  2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
  3. Click **Authentication > Users**.
  4. In **Add User**:, type a name for the user.
  5. Click **Add**.  
The user is enabled by default. To disable, uncheck **Enable**.
  6. Enter a password for the user.
  7. Add groups for the user.  
Groups define user access rights. See [Configure authentication groups](#) for information about configuring groups.
    - a. Click **Groups**.
    - b. Click **Add**.
    - c. Select an appropriate group from the **Group** dropdown.
- 
- Note** Every user must be configured with at least one group. You can add multiple groups to a user by clicking **Add** again and selecting the next group.
- 
8. (Optional) Add SSH keys for the user to use passwordless SSH login:
    - a. Click **SSH keys**.
    - b. In **Add SSH key**, paste or type a public encryption key that this user can use for passwordless SSH login.
    - c. Click **Add**.
  9. (Optional) Configure two-factor authentication for telnet, SSH, and serial console login:
    - a. Click **Two-factor authentication**.
    - b. Check **Enable** to enable two-factor authentication for this user.
    - c. Select the **Verification type**:
      - **Time-based (TOTP)**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
      - **Counter-based (HOTP)**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.

- d. Generate a **Secret key**:
  - i. Click the down arrow (▼) next to the field label and select **Generate secret key**.



- ii. To display the QR code for the secret key, click the down arrow (▼) next to the field label and select **Show secret key QR code**.
- iii. Copy the secret key, or scan or copy the QR code, for use with an application or mobile device to generate passcodes.

---

**Note** To copy the QR code, right-click the QR code and select your browser's save image functionality.

---

- e. For time-based verification only, select **Disallow code reuse** to prevent a code from being used more than once during the time that it is valid.
- f. For time-based verification only, in **Code refresh interval**, type the amount of time that a code will remain valid.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**. For example, to set **Code refresh interval** to ten minutes, enter **10m** or **600s**.
- g. In **Valid code window size**, type the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the **Valid code window size** may be necessary when the clocks used by the server and client are not synchronized.
- h. For **Login limit**, type the number of times that the user is allowed to attempt to log in during the **Login limit period**. Set **Login limit** to **0** to allow an unlimited number of login attempts during the **Login limit period**.
- i. For **Login limit period**, type the amount of time that the user is allowed to attempt to log in.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**. For example, to set **Login limit period** to ten minutes, enter **10m** or **600s**.
- j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:
  - i. Click **Scratch codes**.
  - ii. Click **Add**.
  - iii. For **Code**, enter the scratch code. The code must be eight digits, with a minimum of 10000000.
  - iv. Click **Add** again to add additional scratch codes.

- Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

- Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

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

- Add a user. For example, to create a user named **new\_user**:

```
(config)> add auth user new_user
(config auth user new_user>
```

The user is enabled by default. To disable the user, type:

```
(config auth user new_user> enable false
```

- Assign a password to the user:

```
(config auth user new_user> password pwd
```

Where *pwd* is the password for the user.

- Add groups for the user.  
Groups define user access rights. See [Configure authentication groups](#) for information about configuring groups.
  - Add a group to the user. For example, to add the admin group to the user:

```
(config auth user new_user> add group end admin
```

**Note** Every user must be configured with at least one group.

- (Optional) Add additional groups by repeating the add group command:

```
(config auth user new_user> add group end serial
```

To remove a group from a user:

- Use the **show** command to determine the index number of the group to be deleted:

```
(config auth user new_user> show group
0 admin
1 serial
(config auth user new_user>
```

- Type the following:

```
(config auth user new_user)> del group n
```

Where *n* is index number of the authentication method to be deleted. For example, to delete the serial group as displayed by the example **show** command, above:

---

```
(config auth user new_user)> del group 1
```

---

6. (Optional) Add SSH keys for the user to use passwordless SSH login:

- a. Change to the user's ssh\_key node:

---

```
(config auth user new_user)> ssh_key
(config auth user new_user ssh_key)>
```

---

- b. Add the key by using the ssh\_key command and pasting or typing a public encryption key that this user can use for passwordless SSH login:

---

```
(config auth user new_user ssh_key)> ssh_key key
```

---

7. (Optional) Configure two-factor authentication for SSH, serial console, and telnet login:

- a. Change to the user's two-factor authentication node:

---

```
(config auth user new_user)> 2fa
(config auth user new_user 2fa)>
```

---

- b. Enable two-factor authentication for this user:

---

```
(config auth user new_user 2fa)> enable true
```

---

- c. Configure the verification type. Allowed values are:

- **totp**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
- **hotp**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.

The default value is **totp**.

---

```
(config auth user new_user 2fa)> type totp
```

---

- d. Add a secret key:

---

```
(config auth user new_user 2fa)> secret key
```

---

This key should be used by an application or mobile device to generate passcodes.

- e. For time-based verification only, enable **disallow\_reuse** to prevent a code from being used more than once during the time that it is valid.

---

```
(config auth user new_user 2fa)> disallow_reuse true
```

---

- f. For time-based verification only, configure the code refresh interval. This is the amount of time that a code will remain valid.

---

```
(config auth user new_user 2fa)> refresh_interval value
```

---

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

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

---

```
(config)> auth user name 2fa refresh_interval 600s
(config)>
```

---

The default is **30s**.

- g. Configure the valid code window size. This represents the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the valid code window size may be necessary when the clocks used by the server and client are not synchronized.

---

```
(config auth user new_user 2fa)> window_size 3
```

---

- h. Configure the login limit. This represents the number of times that the user is allowed to attempt to log in during the Login limit period. Set to 0 to allow an unlimited number of login attempts during the Login limit period

---

```
(config auth user new_user 2fa)> login_limit 3
```

---

- i. Configure the login limit period. This is the amount of time that the user is allowed to attempt to log in.

---

```
(config auth user new_user 2fa)> login_limit_period value
```

---

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

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

---

```
(config)> auth user name 2fa login_limit_period 600s
(config)>
```

---

The default is **30s**.

- j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:
- i. Change to the user's scratch code node:

---

```
(config auth user new_user 2fa)> scratch_code
(config auth user new_user 2fa scratch_code)>
```

---

- ii. Add a scratch code:

---

```
(config auth user new_user 2fa scratch_code)> add end code
```

---

Where *code* is an digit number, with a minimum of 10000000.

- iii. To add additional scratch codes, use the **add end code** command again.

8. Save the configuration and apply the change:

---

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

---

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

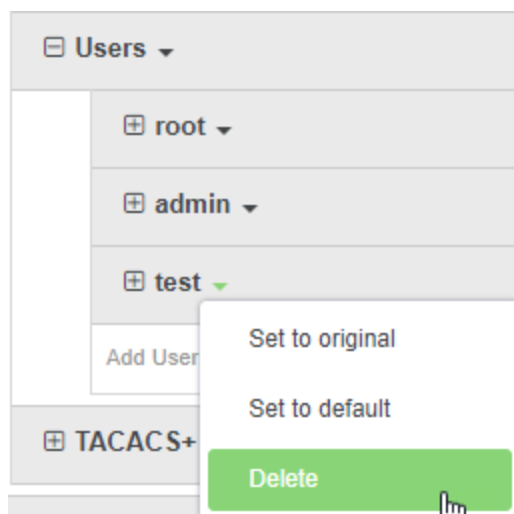
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a local user

To delete a user from your IX14:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Users**.
4. Click the down arrow (▼) next to the name of the user to be deleted and select **Delete**.



5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. At the config prompt, type:

```
(config)> del auth user username
```

4. Save the configuration and apply the change:

---

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

---

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

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



## Terminal Access Controller Access-Control System Plus (TACACS+)

Your IX14 device supports Terminal Access Controller Access-Control System Plus (TACACS+), a networking protocol that provides centralized authentication and authorization management for users who connect to the device.

With TACACS+ support, the IX14 device acts as a TACACS+ client, which sends user credentials and connection parameters to a TACACS+ server over TCP. The TACACS+ server then authenticates the TACACS+ client requests and sends back a response message to the device.

When you are using TACACS+ authentication, you can have both local users and TACACS+ users able to log in to the device.

To use TACACS+ authentication, you must set up a TACACS+ server that is accessible by the IX14 device prior to configuration. The process of setting up a TACACS+ server varies by the server environment.

### TACACS+ user configuration

After setting up the TACACS+ server, you will need to configure one or more users on the server. When configured with TACACS+ support, the IX14 device uses the TACACS+ server for authentication (password verification) and authorization (assigning the access level of the user).

#### Example TACACS+ Configuration

With TACACS+, users are defined in the server configuration file. On Ubuntu, the default location and filename for the server configuration file is **/etc/tacacs+/tac\_plus.conf**.

---

**Note** TACACS+ configuration, including filenames and locations, may vary depending on your platform and installation. This example assumes a Ubuntu installation.

---

To define users:

1. Open the TACACS+ server configuration file in a text editor. For example:

---

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

---

2. Add users to the file using the following format. This example will create two users, one with admin and serial access, and one with only serial access.

---

```
user = user1 {
    name = "User1 for IX14"
    pap = cleartext password1
    service = system {
        groupname = admin,serial
    }
}
user = user2 {
    name = "User2 for IX14"
    pap = cleartext password2
    service = system {
        groupname = serial
    }
}
```

---

The value of the `groupname` attribute must correspond to authentication groups configured on your IX14 device. See [Configure authentication groups](#) for more information about authentication groups. The `groupname` attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

---

```
sudo tac_plus -C /etc/tacacs+/tac_plus.conf -P
```

---

If successful, this command will echo the configuration file to standard out. If the command encounters any syntax errors, a message similar to this will display:

---

```
Error: Unrecognised token on line 1
```

---

5. Restart the TACACS+ server:

---

```
sudo /etc/init.d/tacacs_plus restart
```

---

## TACACS+ server failover and fallback to local authentication

In addition to the primary TACACS+ server, you can also configure your IX14 device to use backup TACACS+ servers. Backup TACACS+ servers are used for authentication requests when the primary TACACS+ server is unavailable.

### *Falling back to local authentication*

With user authentication methods, you can configure your IX14 device to use multiple types of authentication. For example, you can configure both TACACS+ authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup TACACS+ servers are unavailable. Additionally, users who are configured locally but are not configured on the TACACS+ are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the RADIUS server, and only authenticated locally if the RADIUS server is unavailable or if the user is not defined on the RADIUS server, then you should list RADIUS as the first authentication method and Local users as a subsequent authentication method. See [Configure user authentication methods](#) for more information about authentication methods.

If the TACACS+ servers are unavailable and the IX14 device falls back to local authentication, only users defined locally on the device are able to log in. TACACS+ users cannot log in until the TACACS+ servers are brought back online.

## Configure your IX14 device to use a TACACS+ server

This section describes how to configure a IX14 device to use a TACACS+ server for authentication and authorization.

### Required configuration items

- Define the TACACS+ server IP address or domain name.
- Define the TACACS+ server port. It is configured to 49 by default.
- Define the TACACS+ server shared secret.
- The group attribute configured in the TACACS+ server configuration.

- The service field configured in the TACACS+ server configuration.
- Add TACACS+ as an authentication method for your IX14 device.

#### Additional configuration items

- Add additional TACACS+ servers in case the first TACACS+ server is unavailable.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > TACACS+ > Servers**.
4. Click **Add**.
5. For **Hostname**, type the hostname or IP address of the TACACS+.
6. (Optional) Change the default **Port** setting to the appropriate port.
7. For **Secret**, type the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's tac\_plus.conf file, for example:

---

```
key = testing123
```

---

8. (Optional) For **Group attribute**, type the name of the attribute used in the TACACS+ server's configuration to identify the IX14 authentication group or groups that the user is a member of. For example, in [TACACS+ user configuration](#), the group attribute in the sample tac\_plus.conf file is **groupname**, which is also the default setting in the IX14 configuration.
9. (Optional) For **Service**, type the value of the **service** attribute in the the TACACS+ server's configuration. For example, in [TACACS+ user configuration](#), the value of the **service** attribute in the sample tac\_plus.conf file is **system**, which is also the default setting in the IX14 configuration.
10. (Optional) Click **Add** again to add additional TACACS+ servers.
11. Add TACACS+ to the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. Click **Add**.
  - c. Select **TACACS+** for the new method from the **Method** drop-down.

Authentication methods are attempted in the order they are listed until the first successful authentication result is returned.
12. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. Add a TACACS+ server:

---

```
(config)> add auth tacacs+ server end
(config auth tacacs+ server 0)>
```

---

4. Enter the server IP address or hostname:

---

```
(config auth tacacs+ server 0)> hostname hostname|ip-address
(config auth tacacs+ server 0)>
```

---

5. (Optional) Change the default port setting to the appropriate port:

---

```
(config auth tacacs+ server 0)> port port
(config auth tacacs+ server 0)>
```

---

6. Enter the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's `tac_plus.conf` file. For example:

---

```
(config auth tacacs+ server 0)> secret testing123
(config auth tacacs+ server 0)>
```

---

7. Return to the config prompt by typing three periods:

---

```
(config auth tacacs+ server 0)> ...
(config)>
```

---

8. (Optional) Configure the `group_attribute`. This is the name of the attribute used in the TACACS+ server's configuration to identify the IX14 authentication group or groups that the user is a member of. For example, in [TACACS+ user configuration](#), the group attribute in the sample `tac_plus.conf` file is **groupname**, which is also the default setting for the `group_attribute` in the IX14 configuration.

---

```
(config)> auth tacacs+ group_attribute attribute-name
(config)>
```

---

9. (Optional) Configure the type of service. This is the value of the **service** attribute in the the TACACS+ server's configuration. For example, in [TACACS+ user configuration](#), the value of the **service** attribute in the sample `tac_plus.conf` file is **system**, which is also the default setting in the IX14 configuration.

---

```
(config)> auth tacacs+ service service-name
(config)>
```

---

10. (Optional) Repeat the above steps to add additional TACACS+ servers.
11. Add TACACS+ to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add TACACS+ to the end of the list. See [Configure user authentication methods](#) for information about adding methods to the beginning or middle of the list.

---

```
(config)> add auth method end tacacs+
(config)>
```

---

12. Save the configuration and apply the change:

---

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

---

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

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

## Remote Authentication Dial-In User Service (RADIUS)

Your IX14 device supports Remote Authentication Dial-In User Service (RADIUS), a networking protocol that provides centralized authentication and authorization management for users who connect to the device.

With RADIUS support, the IX14 device acts as a RADIUS client, which sends user credentials and connection parameters to a RADIUS server over UDP. The RADIUS server then authenticates the RADIUS client requests and sends back a response message to the device.

When you are using RADIUS authentication, you can have both local users and RADIUS users able to log in to the device.

To use RADIUS authentication, you must set up a RADIUS server that is accessible by the IX14 device prior to configuration. The process of setting up a RADIUS server varies by the server environment. An example of a RADIUS server is FreeRADIUS.

### RADIUS user configuration

After setting up the RADIUS server, you will need to configure one or more users on the server. When configured with RADIUS support, the IX14 device uses the RADIUS server for authentication (password verification) and authorization (assigning the access level of the user).

#### Example FreeRADIUS Configuration

With FreeRADIUS, users are defined in the **users** file in your FreeRADIUS installation. To define users:

1. Open the FreeRadius user file in a text editor. For example:

---

```
$ sudo gedit /etc/freeradius/3.0/users
```

---

2. Add users to the file using the following format:

---

```
user1 Cleartext-Password := "user1"  
      Unix-FTP-Group-Names := "admin"  
  
user2 Cleartext-Password := "user2"  
      Unix-FTP-Group-Names := "serial"
```

---

The value of the Unix-FTP-Group-Names attribute must correspond to authentication groups configured on your IX14. See [Configure authentication groups](#) for more information about authentication groups. The groupname attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

---

```
sudo freeradius -CX
```

---

This should return a message that completes similar to:

---

```
...  
Configuration appears to be OK
```

---

5. Restart the FreeRADIUS server:

---

```
sudo /etc/init.d/freeradius restart
```

---

## RADIUS server failover and fallback to local configuration

In addition to the primary RADIUS server, you can also configure your IX14 device to use backup RADIUS servers. Backup RADIUS servers are used for authentication requests when the primary RADIUS server is unavailable.

### *Falling back to local authentication*

With user authentication methods, you can configure your IX14 device to use multiple types of authentication. For example, you can configure both RADIUS authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup RADIUS servers are unavailable. Additionally, users who are configured locally but are not configured on the RADIUS are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the RADIUS server, and only authenticated locally if the RADIUS server is unavailable or if the user is not defined on the RADIUS server, then you should list RADIUS as the first authentication method and Local users as a subsequent authentication method.

See [Configure user authentication methods](#) for more information about authentication methods.

If the RADIUS servers are unavailable and the IX14 device falls back to local authentication, only users defined locally on the device are able to log in. RADIUS users cannot log in until the RADIUS servers are brought back online.

## Configure your IX14 device to use a RADIUS server

This section describes how to configure a IX14 device to use a RADIUS server for authentication and authorization.

### Required configuration items

- Define the RADIUS server IP address or domain name.
- Define the RADIUS server port. It is configured to 1812 by default.
- Define the RADIUS server shared secret.
- Add RADIUS as an authentication method for your IX14 device.

### Additional configuration items

- Add additional RADIUS servers in case the first RADIUS server is unavailable.
- The server NAS ID. If left blank, the default value is used:
  - If you are access the IX14 device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are access the IX14 device by using ssh, the default value is **sshd**.
- Time in seconds before the request to the server times out. The default is 3 seconds and the maximum possible value is 60 seconds.
- Enable additional debug messages from the RADIUS client.

## WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > RADIUS > Servers**.
4. Click **Add**.
5. For **Hostname**, type the hostname or IP address of the RADIUS.
6. (Optional) Change the default **Port** setting to the appropriate port.
7. For **Secret**, type the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file, for example:

---

```
secret=testing123
```

---

8. For **Timeout**, type or select amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.
9. (Optional) Click the checkbox next to **RADIUS debug** to enable additional debug messages from the RADIUS client.
10. (Optional) For **NAS ID**, type the unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:
  - If you are accessing the IX14 device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are accessing the IX14 device by using ssh, the default value is **sshd**.
11. (Optional) Click **Add** again to add additional RADIUS servers.
12. Add RADIUS to the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. Click **Add**.
  - c. Select **RADIUS** for the new method from the **Method** drop-down.

Authentication methods are attempted in the order they are listed until the first successful authentication result is returned.
13. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

## Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---



3. Add a RADIUS server:

---

```
(config)> add auth radius server end
(config auth radius server 0)>
```

---

4. Enter the server IP address or hostname:

---

```
(config auth radius server 0)> hostname hostname|ip-address
(config auth radius server 0)>
```

---

5. (Optional) Change the default port setting to the appropriate port:

---

```
(config auth radius server 0)> port port
(config auth radius server 0)>
```

---

6. Enter the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file. For example:

---

```
(config auth radius server 0)> secret testing123
(config auth radius server 0)>
```

---

7. Configure the amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.

---

```
(config auth radius server 0)> timeout value
(config)>
```

---

8. Return to the config prompt by typing three periods:

---

```
(config auth radius server 0)> ...
(config)>
```

---

9. (Optional) Enable debug messages from the RADIUS client:

---

```
(config)> auth radius debug true
```

---

10. (Optional) Configure the NAS ID. This is a unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:

- If you are accessing the IX14 device by using the WebUI, the default value is for NAS ID is **httpd**.
- If you are accessing the IX14 device by using ssh, the default value is **sshd**.

---

```
(config)> auth radius nas_id id
(config)>
```

---

11. (Optional) Repeat the above steps to add additional RADIUS servers.
12. Add RADIUS to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add RADIUS to the end of the list. See [Configure user authentication methods](#) for information about adding methods to the beginning or middle of the list.

---

```
(config)> add auth method end radius
(config)>
```

---

13. Save the configuration and apply the change:

---

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

---

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

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

## Set the idle timeout for IX14 users

To configure the amount of time that the user's active session can be inactive before it is automatically disconnected, set the **Idle timeout** parameter.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication**.
4. For **Idle timeout**, enter the amount of time that the active session can be idle before the user is automatically logged out.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, type:

---

```
(config)# auth idle_timeout value
```

---

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

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

---

```
(config)> auth idle_timeout 600s
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

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

## Example user configuration

### Example 1: Administrator user with local authentication

Goal: To create a user with administrator rights who is authenticated locally on the device.

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Users**.
4. In **Add User**: enter a name for the user and click **Add**.
5. Enter a **Password** for the user.
6. Assign the user to the **admin** group:
  - a. Click **Groups**.
  - b. Click **Add**.
  - c. For **Group**, select the **admin** group.
  - d. Verify that the **admin** group has administrator rights:
    - i. Click **Authentication > Groups**.
    - ii. Click **admin**.
    - iii. Verify that the admin group has **Admin access** selected. If not, click the **Admin access** checkbox to select it.
  - e. Verify that **Local users** is one of the configured authentication methods:
    - i. Click **Authentication > Methods**.
    - ii. Verify that **Local users** is one of the methods listed in the list. If not:
      - i. Click **Add**.
      - ii. For **Method**, select **Local users**.
7. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---
3. Verify that the **admin** group has administrator rights:

---

```
(config)> show auth group admin acl
admin
    enable true
...
(config)>
```

---

If **admin > enable** is set to false:

---

```
(config)> auth group admin acl admin enable true
```

---

4. Verify that **local** is one of the configured authentication methods:

---

```
(config)> show auth method
0 local
(config)>
```

---

If **local** is not listed:

---

```
(config)> add auth method end local
(config)>
```

---

5. Create the user. In this example, the user is being created with the username **adminuser**:

---

```
(config)> add auth user adminuser
(config auth user adminuser)>
```

---

6. Assign a password to the user:

---

```
(config auth user adminuser)> password pwd
(config auth user adminuser)>
```

---

7. Assign the user to the **admin** group:

---

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

---

8. Save the configuration and apply the change:

---

```
(config auth user adminuser)> save
Configuration saved.
>
```

---

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

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

## Example 2: RADIUS, TACACS+, and local authentication for one user

Goal: To create a user with administrator rights who is authenticated by using all three authentication methods.

In this example, when the user attempts to log in to the IX14 device, user authentication will occur in the following order:

1. The user is authenticated by the RADIUS server. If the RADIUS server is unavailable,
2. The user is authenticated by the TACACS+ server. If both the RADIUS and TACACS+ servers are unavailable,
3. The user is authenticated by the IX14 device using local authentication.

This example uses a FreeRadius 3.0 server running on ubuntu, and a TACACS+ server running on ubuntu. Server configuration may vary depending on the platforms or type of servers used in your environment.

## WebUI

1. Configure a user on the RADIUS server:
  - a. On the ubuntu machine hosting the FreeRadius server, open the **/etc/freeradius/3.0/users** file:

```
$ sudo gedit /etc/freeradius/3.0/users
```

- b. Add a RADIUS user to the **users** file:

```
admin1 Cleartext-Password := "password1"
      Unix-FTP-Group-Names := "admin"
```

In this example:

- The user's username is **admin1**.
  - The user's password is **password1**.
  - The authentication group on the IX14 device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.
- c. Save and close the **users** file.
2. Configure a user on the TACACS+ server:
    - a. On the ubuntu machine hosting the TACACS+ server, open the **/etc/tacacs+/tac\_plus.conf** file:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

- b. Add a TACACS+ user to the **tac\_plus.conf** file:

```
user = admin1 {
    name = "Admin1 for TX64"
    pap = cleartext password1
    service = system {
        groupname = admin
    }
}
```

In this example:

- The user's username is **admin1**.
  - The user's password is **password1**.
  - The authentication group on the IX14 device, **admin**, is identified in the **groupname** parameter.
- c. Save and close the **tac\_plus.conf** file.

3. Log into the IX14 WebUI as a user with Admin access.
4. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
5. Configure the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. For **1. Method**, select **RADIUS**.
  - c. Click **Add**.
  - d. For **2. Method**, select **TACACS+**.
  - e. Click **Add**.
  - f. For **3. Method**, select **Local users**.
6. Create the local user:
  - a. Click **Authentication > Users**.
  - b. In **Add User:**, type **admin1** and click **Add**.
  - c. For **password**, type **password1**.
  - d. Assign the user to the **admin** group:
    - i. Click **Groups**.
    - ii. Click **Add**.
    - iii. For **Group**, select the **admin** group.

Verify that the **admin** group has administrator rights:

  - i. Click **Authentication > Groups**.
  - ii. Click **admin**.
  - iii. Verify that the admin group has **Admin access** selected. If not, click the **Admin access** checkbox to select it.
7. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Configure a user on the RADIUS server:
  - a. On the ubuntu machine hosting the FreeRadius server, open the **/etc/freeradius/3.0/users** file:

---

```
$ sudo gedit /etc/freeradius/3.0/users
```

---

- b. Add a RADIUS user to the **users** file:

---

```
admin1 Cleartext-Password := "password1"
      Unix-FTP-Group-Names := "admin"
```

---

In this example:

- The user's username is **admin1**.
- The user's password is **password1**.
- The authentication group on the IX14 device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.

- c. Save and close the **users** file.
2. Configure a user on the TACACS+ server:
  - a. On the ubuntu machine hosting the TACACS+ server, open the **/etc/tacacs+/tac\_plus.conf** file:

---

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

---

- b. Add a TACACS+ user to the **tac\_plus.conf** file:

---

```
user = admin1 {
    name = "Admin1 for TX64"
    pap = cleartext password1
    service = system {
        groupname = admin
    }
}
```

---

In this example:

- The user's username is **admin1**.
  - The user's password is **password1**.
  - The authentication group on the IX14 device, **admin**, is identified in the **groupname** parameter.
- c. Save and close the **tac\_plus.conf** file.
  3. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
  4. At the command line, type **config** to enter configuration mode:

---

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

---

5. Configure the authentication methods:
  - a. Determine the current authentication method configuration:

---

```
(config)> show auth method
0 local
(config)>
```

---

This output indicates that on this example system, only local authentication is configured.

- b. Add RADIUS authentication to the beginning of the list:

---

```
(config)> add auth method 0 radius
(config)>
```

---

- c. Add TACACS+ authentication second place in the list:

---

```
(config)> add auth method 1 tacacs+(config)>
```

---



- d. Verify that authentication will occur in the correct order:

```
(config)> show auth method
0 radius
1 tacacs+
2 local
(config)>
```

6. Verify that the **admin** group has administrator rights:

```
(config)> show auth group admin acl
admin
    enable true
...
(config)>
```

If **admin > enable** is set to false:

```
(config)> auth group admin acl admin enable true
```

7. Configure the local user:

- a. Create a local user with the username **admin1**:

```
(config)> add auth user admin1
(config auth user admin1)>
```

- b. Assign a password to the user:

```
(config auth user adminuser)> password password1
(config auth user adminuser)>
```

- c. Assign the user to the **admin** group:

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

8. Save the configuration and apply the change:

```
(config auth user adminuser)> save
Configuration saved.
>
```

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

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

## Firewall

---

Firewall configuration .....	91
Create a custom firewall zone .....	91
Configure the firewall zone for a network interface .....	92
Show firewall zones .....	93
Delete a custom firewall zone .....	95
Configure port forwarding .....	96
Enable or disable a port forwarding rule .....	99
Show port forwarding rules .....	101
Delete a port forwarding rule .....	102
Configure packet filtering .....	104
Enable or disable a packet filtering rule .....	107
Show packet filtering rules .....	108
Delete a packet filtering rule .....	109
Configure custom firewall rules .....	111
Configure Quality of Service options .....	112

## Firewall configuration

Firewall configuration includes the following configuration options:

- **Zones:** A zone is a firewall access group to which network interfaces can be added. You then use zones to configure packet filtering and access control lists for interfaces that are included in the zone. Preconfigured zones include:
  - **Any:** Matches any network interface, even if they are not assigned to this zone.
  - **Loopback:** Zone for interfaces that are used for communication between processes running on the device.
  - **Internal:** Used for interfaces connected to trusted networks. By default, the firewall will allow most access from this zone.
  - **External:** Used for interfaces connect to untrusted zones, such as the internet. This zone has Network Address Translation (NAT) enabled by default. By default, the firewall will block most access from this zone.
  - **Setup:** Used for interfaces involved in the initial setup of the device. By default, the firewall will only allow this zone to access administration services.
  - **IPsec:** The default zone for IPsec tunnels.
  - **Dynamic routes:** Used for routes learned using routing services.
- **Port forwarding:** A list of rules that allow network connections to the 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 IX14.
- **Custom rules:** A script that is run to install advanced firewall rules beyond the scope/capabilities of the standard device configuration.
- **Quality Of Service:** Quality of Service (QOS) options for bandwidth allocation and policy-based traffic shaping and prioritizing.

## Create a custom firewall zone

In addition to the preconfigured zones, you can create your custom zones that can be used to configure packet filtering and access control lists for network interfaces.

To create a zone:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Zones**.
4. In **Add Zone**, enter a name for the zone and click **Add**.
5. (Optional) Expand the new zone to enable Network Address Translation (NAT).
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

See [Configure the firewall zone for a network interface](#) for information about how to configure network interfaces to use a zone.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Add the new zone. For example, to add a zone named **my\_zone**:

```
(config)> add firewall zone my_zone
(config firewall zone my_zone)>
```

4. (Optional) Enable Network Address Translation (NAT):

```
(config firewall zone my_zone)> src_nat true
(config firewall zone my_zone)>
```

5. Save the configuration and apply the change:

```
(config firewall zone my_zone)> save
Configuration saved.
>
```

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

See [Configure the firewall zone for a network interface](#) for information about how to configure network interfaces to use a zone.

## Configure the firewall zone for a network interface

Firewall zones allow you to group network interfaces for the purpose of packet filtering and access control. There are several preconfigured firewall zones, and you can create custom zones as well. The firewall zone that a network interfaces uses is selected during interface configuration.

This example procedure uses an existing network interface named **LAN** and changes the firewall zone from the default zone, Internal, to a custom zone called **my\_zone**.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Network > Interfaces > LAN**.

4. For **Zone**, select **my\_zone**.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, type:

---

```
(config)> network interface lan zone my_zone
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

## Show firewall zones

To display information about configured firewall zones:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Zones**.
4. Click to expand each zone to view further information.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. Use the **show** command to display firewall zones:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

4. Type **cancel** to exit configuration mode:

---

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

---

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

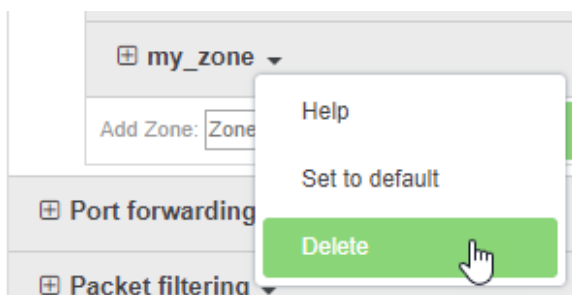
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a custom firewall zone

You cannot delete preconfigured firewall zones. To delete a custom firewall zone:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Zones**.
4. Click the down caret (▼) next to the appropriate custom firewall zone and select **Delete**.



5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Use the **del** command to delete a custom firewall rule. For example:

```
(config)> del firewall zone my_zone
```

4. Save the configuration and apply the change:

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

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

## Configure port forwarding

Most computers are protected by a firewall that prevents users on a public network from accessing servers on the private network. To allow a computer on the Internet to connect to a specific server on a private network, set up one or more port forwarding rules. Port forwarding rules provide mapping instructions that direct incoming traffic to the proper device on a LAN.

To configure a port forwarding rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Port forwarding**.
4. Click **Add**.  
Port forwarding rules are enabled by default.
5. (Optional) Type a **Label** that will be used to identify the rule.
6. For **Interface**, select the network interface for the rule.  
Network connections will only be forwarded if their destination address matches the IP address of the selected network interface.
7. For **IP version**, select either **IPv4** or **IPv6**.  
Network connections will only be forwarded if they match the selected IP version.
8. For **Protocol**, select the type of internet protocol.  
Network connections will only be forwarded if they match the selected protocol.
9. For **Port**, type the public-facing port number that network connections must use for their traffic to be forwarded.
10. For **To Address**, type the IP address of the server to which traffic should be forwarded.
11. For **To port**, type the port number of the port on the server to which traffic should be forwarded.
12. (Optional) Click **Access control list** to create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone:
  - To white list IP addresses:
    - a. Click **Addresses**.
    - b. For **Add Address**, enter an IP address and click **Add**.
    - c. Repeat for each additional IP address that should be white listed.
  - To specify firewall zones for white listing:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate zone.
    - d. Repeat for each additional zone.
13. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.



 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, type:

---

```
(config)> add firewall dnat end
(config firewall dnat 0)>
```

---

Port forwarding rules are enabled by default. To disable the rule:

---

```
(config firewall dnat 0)> enable false
(config firewall dnat 0)>
```

---

4. Set the network interface for the rule.

---

```
(config firewall dnat 0)> interface lan
(config firewall dnat 0)>
```

---

Network connections will only be forwarded if their destination address matches the IP address of this network interface.

To view a list of available interfaces, use the **?**:

---

```
(config firewall dnat 0)> interface ?
```

Interface: Network connections will only be forwarded if their destination address matches the IP address of this network interface.

Format:

```
aview
defaultip
defaultlinklocal
lan
loopback
modem
Current value:
```

---

```
(config firewall dnat 0)>
```

---

5. Set the IP version. Allowed values are **ipv4** and **ipv6**. The default is **ipv4**.

---

```
(config firewall dnat 0)> ip_version ipv6
(config firewall dnat 0)>
```

---

6. Set the public-facing port number that network connections must use for their traffic to be forwarded.

---

```
(config firewall dnat 0)> port port
(config firewall dnat 0)>
```

---

7. Set the type of internet protocol.

---

```
(config firewall dnat 0)> protocol value
(config firewall dnat 0)>
```

---

Network connections will only be forwarded if they match the selected protocol. Allowed values are **custom**, **tcp**, **tcpudp**, or **udp**. The default is **tcp**.

8. Set the IP address of the server to which traffic should be forwarded:

- For IPv4 addresses:

---

```
(config firewall dnat 0)> to_address ip-address
(config firewall dnat 0)>
```

---

- For IPv6 addresses:

---

```
(config firewall dnat 0)> to_address6 ip-address
(config firewall dnat 0)>
```

---

9. Set the public-facing port number that network connections must use for their traffic to be forwarded.

---

```
(config firewall dnat 0)> to_port port
(config firewall dnat 0)>
```

---

10. (Optional) To create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone, change to the `acl` node:

---

```
(config firewall dnat 0)> acl
(config firewall dnat 0 acl)>
```

---

- To white list an IP address:

- For IPv4 addresses:

---

```
(config firewall dnat 0 acl> add address end ip-address
(config firewall dnat 0 acl)>
```

---

- For IPv6 addresses:

---

```
(config firewall dnat 0 acl> add address6 end ip-address
(config firewall dnat 0 acl)>
```

---

Repeat for each appropriate IP address.

- To specify the firewall zone for white listing:

---

```
(config firewall dnat 0 acl)> add zone end zone
```

---

Repeat for each appropriate zone.

To view a list of available zones:

---

```
(config firewall dnat 0 acl)> .. .. zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----  
----

any	Any
dynamic_routes	Dynamic routes
external	External
internal	Internal
ipsec	IPsec
loopback	Loopback
setup	Setup

```
(config firewall dnat 0 acl)>
```

---

11. Save the configuration and apply the change:

---

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

---

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

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

## Enable or disable a port forwarding rule

To enable or disable a port forwarding rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Port forwarding**.
4. Click the appropriate port forwarding rule.
5. Click **Enable** to toggle the rule between enabled and disabled.
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Determine the index number of the appropriate port forwarding rule:

---

```
(config)> show firewall dnat
0
    acl
        no address
        no zone
    enable true
    interface
    ip_version ipv4
    label IPv4 port forwarding rule
    port 10000
    protocol tcp
    to_address6 10.10.10.10
    to_port 10001

1
    acl
        no address6
        no zone
    enable false
    interface
    ip_version ipv6
    label IPv6 port forwarding rule
    port 10002
    protocol tcp
    to_address6 c097:4533:bd63:bb12:9a6f:5569:4b53:c29a
    to_port 10003
(config)>
```

---

4. To enable a port forwarding rule, use the index number with the **enable true** command. For example:

---

```
(config)> firewall dnat 1 enable true
```

---

5. To disable a port forwarding rule, use the index number with the **enable false** command. For example:

---

```
(config)> firewall dnat 0 enable false
```

---

6. Save the configuration and apply the change:

---

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

---

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

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

## Show port forwarding rules

To show port forwarding rules:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Port forwarding**.
4. Click to expand each port forwarding rule to view the rule.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Use the show command to display the port forwarding rules:

---

```
(config)> show firewall dnat
0
    acl
        no address
        no zone
    enable true
    interface
    ip_version ipv4
    label IPv4 port forwarding rule
    port 10000
    protocol tcp
    to_address6 10.10.10.10
    to_port 10001
```

---

```

1
  acl
      no address6
      no zone
  enable true
  interface
  ip_version ipv6
  label IPv6 port forwarding rule
  port 10002
  protocol tcp
  to_address6 c097:4533:bd63:bb12:9a6f:5569:4b53:c29a
  to_port 10003
(config)>
    
```

4. Type **cancel** to exit configuration mode:

```

(config)> cancel
>
    
```

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

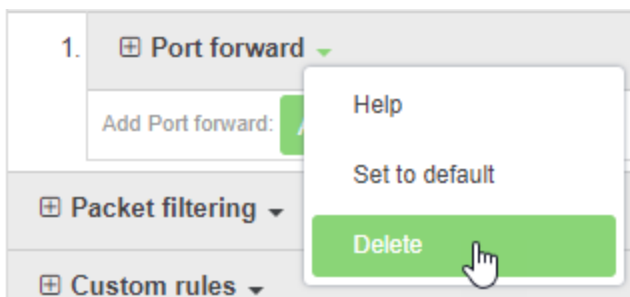
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a port forwarding rule

To delete a port forwarding rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Port forwarding**.
4. Click the down caret (▼) next to the appropriate port forwarding rule and select **Delete**.



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

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Determine the index number of the port forwarding rule you want to delete:

---

```
(config)> show firewall dnat
0
    acl
        no address
        no zone
    enable true
    interface
    ip_version ipv4
    label IPv4 port forwarding rule
    port 10000
    protocol tcp
    to_address6 10.10.10.10
    to_port 10001

1
    acl
        no address6
        no zone
    enable false
    interface
    ip_version ipv6
    label IPv6 port forwarding rule
    port 10002
    protocol tcp
    to_address6 c097:4533:bd63:bb12:9a6f:5569:4b53:c29a
    to_port 10003
(config)>
```

---

4. To delete the rule, use the index number with the **del** command. For example:

---

```
(config)> del firewall dnat 1
```

---

5. Save the configuration and apply the change:

---

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

---

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

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

## Configure packet filtering

By default, one packet filtering rule, **Allow all outgoing traffic**, is enabled and monitors traffic going to and from the IX14 device. The predefined settings are intended to block unauthorized inbound traffic while providing an unrestricted flow of outgoing data. You can modify the default packet filtering rule and create additional rules to define how the device accepts or rejects traffic that is forwarded through the device.

To configure a packet filtering rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Packet filtering**.
  - To edit the default packet filtering rule or another existing packet filtering rule, click to expand the rule.
  - To create a new packet filtering rule, click **Add**.

Packet filters are enabled by default.

4. (Optional) Type a **Label** that will be used to identify the rule.
5. For **Action**, select one of:
  - **Accept**: Allows matching network connections.
  - **Reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
  - **Drop**: Blocks matching network connections, and does not send a reply.
6. Select the **IP version**.
7. Select the **Protocol**.
8. For **Source zone**, select the firewall zone to limit this rule to incoming connections from network interfaces it that are a member of this zone.  
See [Firewall configuration](#) for more information about firewall zones.
9. For **Destination zone**, select the firewall zone to limit this rule to outgoing connections from network interfaces it that are a member of this zone.  
See [Firewall configuration](#) for more information about firewall zones.
10. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.



 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

To edit the default packet filtering rule or another existing packet filtering rule:

- a. Determine the index number of the appropriate packet filtering rule:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
  dst_zone internal
  enable true
  ip_version any
  label myfilter
  protocol any
  src_zone external
(config)>
```

---

- b. Select the appropriate rule by using its index number:

---

```
(config)> firewall filter 1
(config firewall filter 1)>
```

---

To create a new packet filtering rule:

---

```
(config)> add firewall filter end
(config firewall filter 1)>
```

---

3. Packet filtering rules are enabled by default. To disable the rule:

---

```
(config firewall filter 1)> enable false
(config firewall filter 1)>
```

---

4. (Optional) Set the label for the rule.

---

```
(config firewall filter 1)> label "My filter rule"
(config firewall filter 1)>
```

---

5. Set the action to be performed by the filter rule.

---

```
(config firewall filter 1)> action value
(config firewall filter 1)>
```

---

where *value* is one of:

- **accept**: Allows matching network connections.
  - **reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
  - **drop**: Blocks matching network connections, and does not send a reply.
6. Set the firewall zone to limit this rule to incoming connections from network interfaces it that are a member of this zone.

See [Firewall configuration](#) for more information about firewall zones.

---

```
(config firewall filter 1)> src_zone my_zone
(config firewall filter 1)>
```

---

7. Set the firewall zone to limit this rule to outgoing connections from network interfaces it that are a member of this zone.

See [Firewall configuration](#) for more information about firewall zones.

---

```
(config firewall filter 1)> dst_zone my_zone
(config firewall filter 1)>
```

---

8. Set the IP version.

---

```
(config firewall filter 1)> ip_version value
(config firewall filter 1)>
```

---

where *value* is one of:

- **any**
  - **ipv4**
  - **ipv6**
  - The default is **any**.
9. Set the protocol.

---

```
(config firewall filter 1)> protocol value
(config firewall filter 1)>
```

---

where *value* is one of:

- **any**
- **icmp**
- **icmpv6**
- **tcp**
- **udp**

The default is **any**.

10. Save the configuration and apply the change:

---

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

---

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

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

## Enable or disable a packet filtering rule

To enable or disable a packet filtering rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Packet filtering**.
4. Click the appropriate packet filtering rule.
5. Click **Enable** to toggle the rule between enabled and disabled.
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Determine the index number of the appropriate port forwarding rule:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
```

---

---

```

action drop
dst_zone internal
enable true
ip_version any
label My packet filter
protocol any
src_zone external
(config)>

```

---

- To enable a packet filtering rule, use the index number with the **enable true** command. For example:

---

```
(config)> firewall filter 1 enable true
```

---

- To disable a packet filtering rule, use the index number with the **enable false** command. For example:

---

```
(config)> firewall filter 1 enable false
```

---

- Save the configuration and apply the change:

---

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

---

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

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

## Show packet filtering rules

To show packet filtering rules:

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- Click **Firewall > Packet filtering**.
- Click to expand each packet filtering rule to view the rule.

### Command line

- Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

---

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

---

3. Use the show command to display the packet filtering rules:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
  dst_zone internal
  enable true
  ip_version any
  label My packet filter
  protocol any
  src_zone external
(config)>
```

---

4. Type **cancel** to exit configuration mode:

---

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

---

5. Type exit to exit the Admin CLI.

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

## Delete a packet filtering rule

To delete a packet filtering rule:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Packet filtering**.
4. Click the down caret (▼) next to the appropriate packet filtering rule and select **Delete**.
5. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Determine the index number of the packet filtering rule you want to delete:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
  dst_zone internal
  enable true
  ip_version any
  label My packet filter
  protocol any
  src_zone external
(config)>
```

---

4. To delete the rule, use the index number with the **del** command. For example:

---

```
(config)> del firewall filter 1
```

---

5. Save the configuration and apply the change:

---

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

---

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

## Configure custom firewall rules

Custom firewall rules consist of a script of shell commands that can be used to install firewall rules, ipsets, and other system configuration. These commands are run whenever system configuration changes occur that might cause changes to the firewall.

To configure custom firewall rules:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Custom rules**.
4. **Enable** the custom rules.
5. (Optional) Enable **Override** to override all preconfigured firewall behavior and rely solely on the custom firewall rules.
6. For **Rules**, type the shell command that will execute the custom firewall rules script.
7. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable custom firewall rules:

---

```
(config)> firewall custom enable true
(config)>
```

---

4. (Optional) Instruct the device to override all preconfigured firewall behavior and rely solely on the custom firewall rules:

---

```
(config)> firewall custom override true
(config)>
```

---

5. Set the shell command that will execute the custom firewall rules script:

---

```
(config)> firewall custom rules shell-command
(config)>
```

---

- Save the configuration and apply the change:

---

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

---

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

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

## Configure Quality of Service options

Quality of Service (QoS) options for bandwidth allocation and policy-based traffic shaping and prioritizing. There are two preconfigured QoS bindings: **Outbound**, and **Inbound**. You can enable either of these preconfigured bindings, or create your own.

### Enable the preconfigured bindings

#### WebUI

- Log into the IX14 WebUI as a user with Admin access.

- On the menu, click **Configuration**.

The **System Configuration** pane is displayed.

- Click **Firewall > Quality of Service**.

- Click to expand either **Outbound** or **Inbound**.

- Enable** the binding.

- Select an **Interface**.

- Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

- Log into the IX14 command line as a user with Admin access.

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

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

---

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

---

- Enable one of the preconfigured bindings:

- To enable the Outbound binding:

---

```
(config)> firewall qos 0 enable true
(config)>
```

---



- To enable the Inbound binding:

---

```
(config)> firewall qos 1 enable true
(config)>
```

---

4. Set the interface for the binding. Use the index number of the binding; for example, to set the interface for the Outbound binding:

---

```
(config)> firewall qos 0 interface /network/interface/
(config)>
```

---

To view a list of available interfaces, use the **?**:

---

```
(config)> firewall qos 0 interface ?
```

Interface: The network interface.

Format:

```
/network/interface/aview
/network/interface/defaultip
/network/interface/defaultlinklocal
/network/interface/lan
/network/interface/loopback
/network/interface/modem
```

Current value:

---

```
(config)>
```

---

5. Save the configuration and apply the change:

---

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

---

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

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

## Create a new binding

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Firewall > Quality of Service**.
4. Click **Add**.
5. **Enable** the binding.
6. Select an **Interface**.
7. Set other parameters for the binding as appropriate. For information about each parameter, click the down caret (▼) next to the parameter and select **Help**.
8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Add a binding:

---

```
(config)> add firewall qos end
(config firewall qos 2)>
```

---

4. Enable the new binding:

---

```
(config firewall qos 2)> enable true
(config firewall qos 2)>
```

---

5. Set the interface for the binding. Use the index number of the binding; for example, to set the interface for the Outbound binding:

---

```
(config firewall qos 2)> interface /network/interface/
(config firewall qos 2)>
```

---

To view a list of available interfaces, use the **?**:

---

```
(config firewall qos 2)> interface ?
```

---

---

Interface: The network interface.

Format:

```
/network/interface/aview
/network/interface/defaultip
/network/interface/defaultlinklocal
/network/interface/lan
/network/interface/loopback
/network/interface/modem
```

Current value:

```
(config)>
```

---

6. Set other parameters for the binding.
7. Save the configuration and apply the change:

---

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

---

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

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

## System administration

---

Review device status .....	117
Configure system information .....	118
Update system firmware .....	119
Update cellular module firmware .....	122
Reboot your IX14 device .....	122
Reset the device to factory defaults .....	124
Configuration files .....	126
Schedule system maintenance tasks .....	130
Create a Virtual LAN (VLAN) route .....	135
Example: Configure VPN access with IPSec tunnels .....	137
Serial port .....	143

## Review device status

You can review the system of your device from either the **Status** page of the Web interface, or from the command line:

### WebUI

To display system information:

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **Status**.  
A secondary menu appears, along with a status panel.
3. On the secondary menu, click to display the details panel for the status you want to view.

### Command line

To display system information, use the `show system` command.

- Show basic system information:

1. Log into the IX14 command line as a user with Admin access.

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

2. Enter **show system** at the prompt:

---

```
> show system

Hostname           : IX14
FW Version         : 19.8.1.30
MAC                : 0040D0133536
Model              : Digi IX14
Current Time       : Tue, 16 July 2019 21:14:12 +0000
Uptime             : 21 days, 21 hours, 22 minutes, 44 seconds
(336164s)

>
```

---

- Show more detailed system information:

1. Log into the IX14 command line as a user with Admin access.

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

2. Enter **show system verbose** at the prompt:

---

```
> show system verbose

Hostname           : IX14 FW Version           : 19.5.166.0
FW Build Date      : Tue, 16 July 2019 21:14:12 +0000
Schema Version     : 445
MAC                : 0040D0133536
Model              : Digi IX14
Timezone           : UTC
Current Time       : Tue, 16 July 2019 21:14:12 +0000
```

---

---

```
Uptime                : 21 days, 21 hours, 23 minutes, 44 seconds
(336224s)
```

```
Disk
----
```

```
Load Average          : 0.15, 0.11, 0.03
RAM Usage              : 266.580MB/1926.688MB (13%)
Disk /etc/config Usage : 10.920MB/5309.752MB (0%)
Disk /opt Usage        : 10.920MB/5309.752MB (0%)
Disk /overlay Usage    : MB/MB(%)
Disk /tmp Usage         : 0.004MB/262.144MB (0%)
Disk /var Usage         : 1.132MB/262.144MB (0%)
```

```
>
```

---

## Configure system information

You can configure information related to your IX14 device, such as providing a name and location for the device.

### Configuration items

- A name for the device.
- The name of a contact for the device.
- The location of the device.
- A description of the device.
- A banner that will be displayed when users access terminal services on the device.

To enter system information:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System**.
4. For **Name**, type a name for the device. This name will appear in log messages and at the command prompt.
5. For **Contact**, type the name of a contact for the device.
6. For **Location**, type the location of the device.
7. For **Banner**, type a banner message that will be displayed when users log into terminal services on the device.
8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Set a name for the device. This name will appear in log messages and at the command prompt.

---

```
(config)> system name 192.168.3.1
192.168.3.1(config)>
```

---

4. Set the contact for the device:

---

```
192.168.3.1(config)> system contact "Jane User"
192.168.3.1(config)>
```

---

5. Set the location for the device:

---

```
192.168.3.1(config)> system location "9350 Excelsior Blvd., Suite 700, Hopkins,
MN"
192.168.3.1(config)>
```

---

6. Set the banner for the device. This is displayed when users access terminal services on the device.

---

```
192.168.3.1(config)> system banner "Welcome to the Digi IX14."
192.168.3.1(config)>
```

---

7. Save the configuration and apply the change:

---

```
192.168.3.1(config)> save
Configuration saved.
192.168.3.1>
```

---

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

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

## Update system firmware

The IX14 operating system firmware images consist of a single file with the following naming convention:

***platform-version.bin***

For example, **IX14-19.8.1.30.bin**.

## Manage firmware updates using Digi Remote Manager

If you have a network of many devices, you can use Digi Remote Manager **Profiles** to manage firmware updates. Profiles ensure all your devices are running the correct firmware version and that

all newly installed devices are updated to that same version. For more information, see the **Profiles** section of the [Digi Remote Manager User Guide](#).

## Certificate management for firmware images

The system firmware files are signed to ensure that only Digi-approved firmware load onto the device. The IX14 device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

## Update the system firmware from the WebUI

### WebUI

1. Download the IX14 operating system firmware from the Digi Support FTP site to your local machine.
2. Log into the IX14 WebUI as a user with Admin access.
3. On the main menu, click **System**.
4. In the **Device Firmware** section, for **Firmware Image**, click **Choose File**.
5. Browse to the system firmware file location and select the file.
6. Click **Update Firmware**.

### Command line

1. Download the IX14 operating system firmware from the Digi Support FTP site to your local machine.
2. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
3. Load the firmware image onto the device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/IX14-19.8.1.30.bin local /etc/config/ to local
admin@192.168.4.1's password: adminpwd
IX14->19.8.1.30.bin          100%   36MB   11.1MB/s   00:03
>
```

---



4. Verify that the firmware file has been successfully uploaded to the device:

---

```
> ls /etc/config/
-rw-r--r--  1 root    root      37511229 May 16 20:10 IX14-19.8.1.30.bin
-rw-r--r--  1 root    root        2580 May 16 16:44 accns.json
drw-----  2 root    root      4096 Apr 29 18:51 analyzer
-rw-r--r--  1 root    root         47 Apr 30 06:59 dhcp.leases
drwxr-xr-x  2 root    root      4096 May 15 17:53 fcron
...
>
```

---

5. Update the firmware by entering the [update firmware](#) command, specifying the firmware file name:

---

```
> update firmware file IX14-19.8.1.30.bin
36632K
netflash: got "/etc/config/IX14-19.8.1.30", length=37511229
netflash: authentication successful
netflash: programming FLASH device /dev/flash/image
36633K 100%
Firmware update completed, reboot device
>
```

---

6. Reboot the device to run the new firmware image using the [reboot](#) command.

---

```
> reboot
Rebooting system
>
```

---

7. Once the device has rebooted, log into the IX14's command line as a user with Admin access and verify the running firmware version by entering the [show system](#) command.

---

```
> show system

Hostname           : IX14
FW Version         : 19.8.1.30
MAC                : 0040FF800120
Model              : Digi IX14
Current Time       : Tue, 16 July 2019 21:14:12 +0000
Uptime             : 42 seconds (42s)

>
```

---

## Update cellular module firmware

Digi provides the cellular module files for all certified cellular carriers for IX14 devices on the [Digi repository of cellular module firmware files](#).

### WebUI

This operation is available from the WebUI only. There is no equivalent functionality at the CLI.

1. Download the appropriate modem firmware from the Digi repository to your local machine.
2. Log into the IX14 WebUI as a user with Admin access.
3. From the main menu, click **System**.
4. In the **Modem Firmware** section, for **Firmware Image**, click **Choose File**.
5. Browse to the system firmware file location and select the file.
6. Click **Upload & Install Firmware**.

## Reboot your IX14 device

You can reboot the IX14 device immediately or schedule a reboot for a specific time every day.

---

**Note** You may want to save your configuration settings to a file before rebooting. See [Save configuration to a file](#).

---

### Reboot your device immediately

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. From the main menu, click **System**.
3. Click **Reboot**.
4. Click **OK** to confirm that you want to reboot the device.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

---

```
> reboot
```

---

## Schedule reboots of your device

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Select **Configuration > System > Scheduled tasks**.
4. For **Reboot time**, enter the time of the day that the device should reboot, using the format *HH:MM*.  
The device will reboot at this time every day.  
If a value is set for **Reboot time** but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See [System time](#) for information about configuring NTP servers.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Set the reboot time:

---

```
(config>> system schedule reboot_time time
(config)>
```

---

where *time* is the time of the day that the device should reboot, using the format *HH:MM*. For example, the set the device to reboot at two in the morning every day:

---

```
(config>> system schedule reboot_time 02:00
(config)>
```

---

If a value is set for **reboot\_time** but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See [System time](#) for information about configuring NTP servers.

4. Save the configuration and apply the change:

---

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

---

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

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

## Reset the device to factory defaults

Resetting the device to factory defaults performs the following actions:

- Clears all configuration settings. When the device restarts, it uses the default configuration.
- Deletes all user files including Python scripts.
- Erases all automatically generated keys.
- Clears event and system log files.

You can reset the device in the WebUI, at the command line, or by using the **Reset** button on the device. You can also reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **System**.
3. Under **Configuration Management**, click **Erase Config**.
4. Click **OK** to confirm.

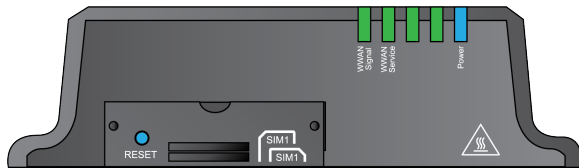
### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

```
> system factory-erase
```

### Reset the device by using the Reset button.

1. Short press and release the **Reset** button located under the SIM gasket cover:



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

### Reset the device with the revert command

You can reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command:

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. At the config prompt, enter **revert**:

---

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

---

4. Set the password for the root user prior to saving the changes:

---

```
(config)> auth user root password pwd
(config)>
```

---

5. Save the configuration and apply the change:

---

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

---

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

## Configuration files

The IX14 configuration file, `/etc/config/accns.json`, contains all configuration changes that have been made to the device. It does not contain the complete device configuration; it only contains changes to the default configuration. Both the default configuration and the changes contained in the `accns.json` file are applied when the device reboots.

### Save configuration changes

When you make changes to the IX14 configuration, the changes are not automatically saved. You must explicitly save configuration changes, which also applies to changes. If you do not save configuration changes, the system discards the changes.

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.

2. On the menu, click **Configuration**.

The **System Configuration** pane is displayed.

3. Make any necessary configuration changes.
4. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.

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

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

---

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

---

3. Make any necessary configuration changes.
4. Save the configuration and apply the change:

---

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

---

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

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

## Save configuration to a file

You can save your IX14 device's configuration to a file and use this file to restore the configuration, either to the same device or to similar devices.

### WebUI

This procedure creates a binary archive file containing the device's configuration, certificates and keys, and other information.

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **System**.
3. (Optional) Encrypt the configuration using a passphrase:
  - In the **Configuration Management** section, for **Passphrase (save/restore)**, enter the passphrase.
4. In the **Configuration Management** section, click **Save Config**.  
The file will be downloaded using your browser's standard download process.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

---

```
> system backup path [passphrase passphrase] type type
```

---

where

- *path* is the location on the IX14's filesystem where the configuration backup file should be saved.
- *passphrase* (optional) is a passphrase used to encrypt the configuration backup.
- *type* is the type of backup, either:
  - **archive**: Creates a binary archive file containing the device's configuration, certificates and keys, and other information.
  - **cli-config**: Creates a text file containing only the configuration changes.

For example:

---

```
> system backup /etc/config/ type archive
```

---

3. (Optional) Use **scp** to copy the file from your device to another host:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.

- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX14 device.

For example:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/ local
/etc/config/backup-archive-0040FF800120-19.05.17-19.01.17.bin to remote
```

---

## Restore the device configuration

You can restore a configuration file to your IX14 device by using a backup from the device, or a backup from a similar device.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **System**.
3. If a passphrase was used to create the configuration backup:
  - In the **Configuration Management** section, for **Passphrase (save/restore)**, enter the passphrase.
4. Under **Configuration Management**, click **Choose File**.
5. Browse to the system firmware file location and select the file.
6. Click **Restore Config**.
7. Click **OK** to confirm.

The configuration will be restored and the device will be rebooted.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. If the configuration backup is on a remote host, use **scp** to copy the file from the host to your device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
local
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:



---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/backup-archive-0040FF800120-19.05.17-19.01.17.bin local /etc/config/ to local
```

---

3. Enter the following:

---

```
> system restore path [passphrase passphrase]
```

---

where

- *path* is the location on the IX14's filesystem where the configuration backup file should be saved.
- *passphrase* (optional) is the passphrase to restore the configuration backup, if a passphrase was used when the backup was created.

For example:

---

```
> system restore /etc/config/
```

---

## Schedule system maintenance tasks

You can configure tasks and custom scripts to be run during a specified maintenance window.

### Required configuration items

- The time that the system maintenance tasks will start.
- The duration window during which the system maintenance tasks can run.
- The frequency (either daily or weekly) that the tasks will run.
- The tasks to be performed. Options are:
  - Modem firmware update.
  - Configuration check.

### Additional configuration items

- Custom scripts that should be run as part of the configuration check.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System > Scheduled tasks > System maintenance**.
4. For **Start time**, type the time of day that the maintenance window should start, using the syntax *HH:MM*. If **Start time** is not set, maintenance tasks are not scheduled and will not be run.  
The behavior of **Start time** varies depending on the setting of **Duration window**, which is configured in the next step.
  - If **Duration window** is set to **Immediately**, all scheduled tasks will begin at the exact time specified in **Start time**.
  - If **Duration window** is set to **24 hours**, **Start time** is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting **Duration window** to **24 hours** can potentially overstress the device and should be used with caution.
  - If **Duration window** is set to any value other than to **Immediately** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
  - If **Duration window** is set to one or more hours, the minutes field in **Start time** is ignored and the duration window will begin at the beginning of the specified hour.
5. For **Duration window**, select the amount of time that the maintenance tasks will be run. If **Immediately** is selected, all scheduled tasks will begin at the exact time specified in **Start time**.
6. For **Frequency**, select either **Daily** or **Weekly** for the frequency that the maintenance tasks should be run.
7. Click the checkbox for **Modem firmware update** to instruct the system to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. **Modem firmware update** looks for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

8. Click the checkbox for **Configuration check** to allow for the configuration to be updated, including by custom scripts, during the maintenance window.
9. (Optional) To schedule custom scripts:
  - a. Click **Custom scripts**.

---

**Note** This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care. Scripts created here are also automatically entered in **Configuration > Applications**.

---

- b. Click **Add**.
- c. **Enable** the script.
- d. (Optional) For **Label**, provide a label for the script.
- e. For **Run mode**, select the mode that will be used to run the script. Available options are:
  - **On boot**: The script will run once each time the device boots.
    - If **On boot** is selected, select the action that will be taken when the script completes in **Exit action**. Available options are:
      - **None**: Action taken when the script exits.
      - **Restart script**: Runs the script repeatedly.
      - **Reboot**: The device will reboot when the script completes.
  - **Interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **Interval** is selected:
    - For **Interval**, type the interval.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number*{w|d|h|m|s}.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
    - Click the checkbox for **Run single** to run only a single instance of the script at a time.  
If **Run single** is not selected, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.
  - **Set time**: Runs the script at a specified time of the day.
    - If **Set Time** is selected, specify the time that the script should run in **Run time**, using the format *HH:MM*.
  - **During system maintenance**: The script will run during the system maintenance time window.
- f. For **Commands**, enter the commands that will execute the script.  
If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).
- g. Script logging options:
  - i. Check the box for **Log script output** to log the script's output to the system log.
  - ii. Check the box for **Log script errors** to log script errors to the system log.
 If neither option is selected, only the script's exit code is written to the system log.
- h. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}.

- i. Check the box for **Once** to configure the script to run only once at the specified time.  
If **Once** is selected, rebooting the device will cause the script to not run again. The only way to re-run the script is to:
  - Remove the script from the device and add it again.
  - Make a change to the script.
  - Uncheck **Once**.

10. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Schedule system maintenance:
  - a. Configure the time of day that the maintenance window should start, using the syntax *HH:MM*. If the start time is not set, maintenance tasks are not scheduled and will not be run.

---

```
(config)> system schedule maintenance from HH:MM
(config)>
```

---

The behavior of the start time varies depending on the setting of the duration length, which is configured in the next step.

- If the duration length is set to **0**, all scheduled tasks will begin at the exact time specified in the start time.
  - If the duration length is set to **24 hours**, the start time is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting the duration length to **24 hours** can potentially overstress the device and should be used with caution.
  - If the duration length is set to any value other than to **0** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
  - If the duration length is set to one or more hours, the minutes field in the start time is ignored and the duration window will begin at the beginning of the specified hour.
- b. Configure the duration length (the amount of time that the maintenance tasks will be run). If **0** is used, all scheduled tasks will begin at the start time, defined in the previous step.

---

```
system schedule maintenance length num
(config)>
```

---

where *num* is any whole number between **0** and **24**.

- c. Configure the frequency that the maintenance tasks should be run:

---

```
system schedule maintenance frequency value
(config)>
```

---

where *value* is either **daily** or **weekly**. **Daily** is the default.

- d. Configure the device to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. The device will look for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

---

```
system schedule maintenance modem_fw_update value
(config)>
```

---

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

- e. Allow for the configuration to be updated, including by custom scripts, during the maintenance window:

---

```
system schedule maintenance config_check value
(config)>
```

---

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

4. (Optional) Schedule custom scripts:

- a. Add a script:

---

```
(config)> add system schedule script end
(config system schedule script 0)>
```

---

- b. Enable the application:

---

```
(config system schedule script 0)> enable true
(config system schedule script 0)>
```

---

- c. (Optional) Provide a label for the script.

---

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

---

where *value* is any string. if spaces are used, enclose *value* within double quotes.

- d. Set the mode that will be used to run the script:

---

```
(config system schedule script 0)> when mode
(config system schedule script 0)>
```

---

where *mode* is one of the following:

- **boot**: The script will run once each time the device boots.
  - If **boot** is selected, set the action that will be taken when the script completes:

---

```
(config system schedule script 0)> exit_action action
(config system schedule script 0)>
```

---

where *action* is one of the following:

- **none**: Action taken when the script exits.
- **restart**: Runs the script repeatedly.
- **reboot**: The device will reboot when the script completes.
- **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected:

- Set the interval:

---

```
(config system schedule script 0)> on_interval value
(config system schedule script 0)>
```

---

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

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

---

```
(config system schedule script 0)> on_interval 600s
(config system schedule script 0)>
```

---

- (Optional) Configure the script to run only a single instance at a time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is set to **false**, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.

- **set\_time**: Runs the script at a specified time of the day.
  - If **Set Time** is selected, set the time that the script should run, using the format *HH:MM*:

---

```
(config system schedule script 0)> run_time HH:MM
(config system schedule script 0)>
```

---

- **maintenance\_time**: The script will run during the system maintenance time window.

- e. Set the commands that will execute the script:

---

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

---

where *filename* is the path and filename of the script, and any related command line information.

If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

- f. Script logging options:

- To log the script's output to the system log:

---

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

---

- To log script errors to the system log:

---

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

---

If **syslog\_stdout** and **syslog\_stderr** are not enabled, only the script's exit code is written to the system log.

- g. Set the maximum amount of memory available to be used by the script and its subprocesses:

---

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

---

where *value* uses the syntax **number{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}**.

- h. To run the script only once at the specified time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:

- Remove the script from the device and add it again.
- Make a change to the script.
- Disable **once**.

5. Save the configuration and apply the change:

---

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

---

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

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

## Create a Virtual LAN (VLAN) route

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

### Required configuration items

- Device to be assigned to the VLAN.
- The VLAN ID. The TCP header uses the VLAN ID to identify the destination VLAN for the packet.

To create a VLAN:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Network > Virtual LAN**.
4. Type a name for the VLAN and click **Add**.
5. Select the **Device**.

6. Type or select a unique numeric **ID** for the VLAN ID.
7. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Add the VLAN:

```
(config)> add network vlan name
(config)>
```

4. Set the device to be used by the VLAN:

- a. View a list of available devices:

```
(config network vlan vlan1)> device ?

Device: The Ethernet device to use for this virtual LAN
Format:
  /network/device/lan
  /network/device/loopback
  /network/vlan/vlan1
Current value:
```

```
(config network vlan vlan1)>
```

- b. Add the device:

```
(config network vlan vlan1)> device /network/device/lan
(config network vlan vlan1)>
```

5. Set the VLAN ID:

```
(config network vlan vlan1)> id value
```

where *value* is an integer between **1** and **4095**.

6. Save the configuration and apply the change:

```
(config network vlan vlan1)> save
Configuration saved.
>
```



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

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

## Example: Configure VPN access with IPsec tunnels

This example demonstrates how to build an IPsec tunnel through the 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 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 IX14 with a tunnel to a VPN server at 12.13.14.15 through its cellular modem. The client laptop connected to the IX14 WAN/ETH1 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 IX14:

### WebUI

#### Task One: Configure the Tunnel

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **VPN > IPsec > Tunnels**.
4. Add a new tunnel named **my\_tunnel** and configure the following options:
  - a. **Pre-shared key:** Enter the pre-shared key to authenticate with the peer.
  - b. (Optional) **XAUTH client**, check **Enable** and enter the XAUTH client **Username** and **Password**.
  - c. **Enable MODECFG client:** Enable this option to allow receipt of the MODECFG attributes to configure the IP address and DNS server for the tunnel.
  - d. **Local endpoint:** Do one of the following:
    - To build the tunnel only through the cellular modem WAN interface:
      - i. For **Type**, select **Interface**.
      - ii. For **Interface**, select **Modem**.
    - To build the tunnel through any available WAN interface:
      - i. Click to expand **ID**.
      - ii. For **ID Type**, selected **KeyID**
      - iii. Set the **KeyID value**.

- e. For **Remote endpoint**:
  - i. Click to expand **Remote endpoint**.
  - ii. For **Hostname**, type the hostname or IP address of the remote endpoint.
  - iii. Click to expand **ID**.
  - iv. For **ID Type**, select **IPv4**.
  - v. For **IPv4 ID value**, type an IPv4 formatted ID. This should take the form of a hostname or IP address.
- f. For **IKE**:
  - i. Click to expand **IKE**.
  - ii. For **Mode**, select **Aggressive mode**.
  - iii. For both **Phase 1 Proposals** and **Phase 2 Proposals**:
    - i. Click to expand each node.
    - ii. Click **Add**.
    - iii. Configure the settings to match the IKE settings required by the IPsec server. In this example, both proposals are set to **AES128, SHA1, MOD768**.
5. Add a **Policy**:
  - a. Click to expand **Policies**.
  - b. Click **Add**.
  - c. Click to expand **Policy**.
  - d. For **Remote network**, type 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**.

---

- e. Click to expand **Local network**.
- f. For **Type**, select **Request a network**.
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

## Task two: Configure the firewall

1. Click **Configuration > Firewall > Packet Filtering**.
2. Click **Add**.
3. For **Label**, type "Allow all incoming traffic to IPsec tunnel."
4. For **Source Zone**, select **IPsec**.
5. For **Destination Zone**, select **Internal**.
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.

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

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

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

3. Add a new IPsec tunnel named **my\_tunnel**:

```
(config)> add vpn ipsec tunnel my_tunnel
(config vpn ipsec tunnel my_tunnel)>
```

4. Set the preshared key to authenticate with the peer:

```
(config vpn ipsec tunnel my_tunnel)> auth secret key
(config vpn ipsec tunnel my_tunnel)>
```

5. (Optional) Enable XAUTH client functionality:

- a. Enable XAUTH client:

```
(config vpn ipsec tunnel my_tunnel)> xauth_client enable true
(config vpn ipsec tunnel my_tunnel)>
```

- b. Set the XAUTH client username:

```
(config vpn ipsec tunnel my_tunnel)> xauth_client username name
(config vpn ipsec tunnel my_tunnel)>
```

- c. Set the XAUTH client password:

```
(config vpn ipsec tunnel my_tunnel)> xauth_client password pwd
(config vpn ipsec tunnel my_tunnel)>
```

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

```
(config vpn ipsec tunnel my_tunnel)> modecfg_client enable true
(config vpn ipsec tunnel my_tunnel)>
```

7. Set the 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.

```
(config vpn ipsec tunnel my_tunnel)> local id type keyid
(config vpn ipsec tunnel my_tunnel)>
```

- Set the local endpoint type to **interface** and set the local endpoint interface to **modem**. This builds the tunnel only through the cellular modem interface.

---

```
(config vpn ipsec tunnel my_tunnel)> local type interface
(config vpn ipsec tunnel my_tunnel)> local interface modem
```

---

## 8. Configure the remote endpoint:

- a. Set the ID type to ipv4:

---

```
(config vpn ipsec tunnel my_tunnel)> remote id type ipv4
(config vpn ipsec tunnel my_tunnel)>
```

---

- b. Set the IPv4 ID value using either the fully-qualified domain name or an IP address:

---

```
(config vpn ipsec tunnel my_tunnel)> remote id ipv4_id hostname
(config vpn ipsec tunnel my_tunnel)>
```

---

## 9. Configure IKE settings:

- a. Set the IKE mode to
- aggressive**
- :

---

```
(config vpn ipsec tunnel my_tunnel)> ike mode aggressive
(config vpn ipsec tunnel my_tunnel)>
```

---

- b. Add an IKE phase 1 proposal:

---

```
(config vpn ipsec tunnel my_tunnel)> add ike phase1_proposal end
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)>
```

---

- c. Set the IKE Phase 1 proposals to match the IKE settings required by the IPsec server. In this example, both proposals are set to:

- cipher: **aes128**
- dh\_group: **modp768**
- hash: **sha1** (the default setting)

---

```
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)> show
cipher 3des
dh_group modp1024
hash sha1
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)> cipher aes128
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)> dhgroup modp768
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)>
```

---

- d. Add an IKE phase 2 proposal:

---

```
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)> .. ..
(config vpn ipsec tunnel my_tunnel ike)> add phase2_proposal end
(config vpn ipsec tunnel my_tunnel ike phase2_proposal 0)> cipher aes128
(config vpn ipsec tunnel my_tunnel ike phase2_proposal 0)> dhgroup modp768
(config vpn ipsec tunnel my_tunnel ike phase2_proposal 0)>
```

---

## 10. Add a new policy and set the following options:

## a. Add a policy:

```
(config vpn ipsec tunnel my_tunnel ike phase1_proposal 0)> ...  
(config)> add vpn ipsec tunnel my_tunnel policy end  
(config vpn ipsec tunnel my_tunnel policy 1)>
```

## b. Set the local network type to request a network:

```
(config vpn ipsec tunnel my_tunnel policy 1)> local type request  
(config vpn ipsec tunnel my_tunnel policy 1)>
```

b. Set the IP address of the remote network. In this sample, the remote network is **10.255.0.0/16**.

```
(config vpn ipsec tunnel my_tunnel policy 1)> remote network 10.255.0.0/16  
(config vpn ipsec tunnel my_tunnel policy 1)>
```

**Note** If you want to have all outbound traffic go through this tunnel, set policy remote network to **0.0.0.0/0**.

## 11. Add a packet filtering rule to allow return traffic:

## a. Add a new packet filter:

```
(config vpn ipsec tunnel my_tunnel policy 1)> ...  
(config)> add firewall filter end  
(config firewall filter 1)>
```

b. Set the label to **Allow all incoming traffic to IPsec tunnel**:

```
(config firewall filter 1)> label "Allow all incoming traffic to IPsec tunnel"  
(config firewall filter 1)>
```

c. Leave action to at the default setting of **accept**, IP version at the default setting of **any**, and set Protocol at the default setting of **Any**.d. Set the source zone to **ipsec**:

```
(config firewall filter 1)> src_zone ipsec  
(config firewall filter 1)>
```

e. Set the destination zone to **internal**:

```
(config firewall filter 1)> dst_zone internal  
(config firewall filter 1)>
```

## 12. Save the configuration and apply the change:

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

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

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

## Serial port

IX14 devices have a single serial port that provides access to the command-line interface.

Use an RS-232 serial cable to establish a serial connection from your IX14 to your local laptop or PC. Use a terminal emulator program to establish the serial connection. The terminal emulator's serial connection must be configured to match the configuration of the IX14 device's serial port. The default serial port configuration for the IX14 is:

- Baud rate: **115200**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**
- Flow control: **None**

### Configure the serial port

By default, the IX14 serial port is configured as follows:

- **Enabled**
- **Serial mode:** Login
- **Label:** None
- **Baud rate:** 115200
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None

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

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Serial > Port 1**.
4. The serial port is enabled by default. To disable, deselect **Enable**.
5. For serial mode, select either **Login** or **Remote**.
  - **Login:** Allows the user to log into the device through the serial port.
  - **Remote:** Allows for remote access to another device that is connected to the serial port.The default is **Login**.
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. For **Baud rate**, type the baud rate used by the device to which you want to connect.
8. For **Data bits**, type the number of data bits used by the device to which you want to connect.

9. For **Parity**, select the type of parity used by the device to which you want to connect.
10. For **Stop bits**, select the number of stop bits used by the device to which you want to connect.
11. For **Flow control**, select the type of flow control used by the device to which you want to connect.
12. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

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

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
```

4. Set the mode:

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

where *mode* is either:

- **login**: Allows the user to log into the device through the serial port.
- **remote**: Allows for remote access to another device that is connected to the serial port.

The default is **login**.

5. (Optional) Set a label that will be used when referring to this port.

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

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

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

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

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

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

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

Allowed values are:

- **even**
- **odd**
- **none**



The default is **none**.

- Set the stop bits used by the device to which you want to connect:

---

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

---

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

---

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

---

Allowed values are:

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

The default is **none**.

- Save the configuration and apply the change:

---

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

---

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

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

## Show serial status and statistics

To show the status and statistics for the serial port:

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the main menu, click **Status**
- Click **Serial**.

### Command line

- Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- Use the [show serial](#) command:

---

```
> show serial
```

Label	Port	Enable	Mode	Baudrate
Serial 1	port1	true	login	115200

---

```
>
```

---

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

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

## Services

---

Allow remote access for web administration and SSH .....	148
Configure the web administration service .....	149
Configure SSH access .....	155
Use SSH with key authentication .....	160
Configure telnet access .....	162
Configure DNS .....	166
Simple Network Management Protocol (SNMP) .....	172
System time .....	176
Configure the system time .....	177
Network Time Protocol .....	179
Configure the device as an NTP server .....	179
Configure a multicast route .....	184
Enable service discovery (mDNS) .....	186

## Allow remote access for web administration and SSH

By default, only devices connected to the IX14's LAN have access to the device via web administration and SSH. To enable these services for access from remote devices:

- The IX14 device must have a publicly reachable IP address.
- The **External** firewall zone must be added to the web administration or SSH service. See [Firewall configuration](#) for information on zones.

To allow web administration or SSH for the External firewall zone:

### Add the External firewall zone to the web administration service

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > Web administration > Access Control List > Zones**.
4. Click **Add**.
5. Select **External**.
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Add the external zone to the web administration service:

```
(config)> add service web-admin acl zone end external
(config)>
```

4. Save the configuration and apply the change:

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

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

## Add the External firewall zone to the SSH service

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Configuration > Services > SSH > Access Control List > Zones**.
4. Click **Add**.
5. Select **External**.
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Add the **External** zone to the SSH service:

```
(config)> add service ssh acl zone end external
(config)>
```

4. Save the configuration and apply the change:

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

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

## Configure the web administration service

The web administration service allows you to monitor and configure the IX14 device by using the WebUI, a browser-based interface.

By default, the web administration service is enabled and uses the standard HTTPS port, 443. The default access control for the service uses the **internal** firewall zone, which means that only devices connected to the IX14's LAN can access the WebUI. If this configuration is sufficient for your needs, no further configuration is required. See [Allow remote access for web administration and SSH](#) for information about configuring the web administration service to allow access from remote devices.

### Required configuration items

- The web administration service is enabled by default.
- Configure access control for the service.

### Additional configuration items

- Port to use for web administration service communication.
- Multicast DNS (mDNS) support.
- An SSL certificate to use for communications with the service.
- Support for legacy encryption protocols.

### Enable or disable the web administration service

The web administration service is enabled by default. To disable the service, or enable it if it has been disabled:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > Web administration**.
4. Click **Enable**.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable or disable the web administration service:

- To enable the service:

---

```
(config)> service web_admin enable true
(config)>
```

---

- To disable the service:

---

```
(config)> service web_admin enable false
(config)>
```

---

- Save the configuration and apply the change:

---

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

---

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

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

## Configure the service

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- Click **Services > Web administration**.
- (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
- Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - Click **IPv4 Addresses**.
    - Click **Add**.
    - For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the web administration service.
    - Click **Add** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - Click **IPv6 Addresses**.
    - Click **Add**.
    - For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the web administration service.
    - Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - Click **Interfaces**.
    - Click **Add**.
    - For **Interface**, select the appropriate interface from the dropdown.
    - Click **Add** again to allow access through additional interfaces.

- To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
- 6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
- 7. For **SSL certificate**, if you have your own signed SSL certificate, type the certificate and private key in PEM format. If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
- 8. For **Allow legacy encryption protocols**, enable this option to allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.
- 9. **View** is set to **Auto** by default and normally should not be changed.
- 10. **Legacy port redirection** is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed. To disable legacy port redirection, click to expand **Legacy port redirection** and deselect **Enable**.
- 11. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service web_admin acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the web administration service.

Repeat this step to list additional IP addresses or networks.



- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service web_admin acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the web administration service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service web_admin acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
lan                 LAN
loopback            Loopback
modem               Modem
```

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service web_admin acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
```

---

---

```

        src_nat true
internal
        src_nat false
ipsec
        src_nat false
loopback
        src_nat false
setup
        src_nat false
(config)>

```

---

- Repeat this step to list additional firewall zones.
4. (Optional) If you have your own signed SSL certificate, set the certificate and private key in PEM format. If not set, the device will use an automatically-generated key.

---

```

(config)> service web_admin cert cert.pem
(config)>

```

---

5. (Optional) Configure Multicast DNS (mDNS):  
mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

- To enable the mDNS protocol:

---

```

(config)> service web_admin mdns enable true
(config)>

```

---

- To disable the mDNS protocol:

---

```

(config)> service web_admin mdns enable false
(config)>

```

---

6. (Optional) Set the port number for this service.  
The default setting of 443 normally should not be changed.

---

```

(config)> service web_admin port 444
(config)>

```

---

7. (Optional) Configure the device to allow legacy encryption protocols.  
Legacy encryption protocols allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.

To enable legacy encryption protocols:

---

```

(config)> service web_admin legacy_encryption true
(config)>

```

---

8. (Optional) Disable legacy port redirection.  
Legacy port redirection is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed.

To disable legacy port redirection:

```
(config)> service web_admin legacy enable false
(config)>
```

9. Save the configuration and apply the change:

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

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

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

## Configure SSH access

The IX14's default configuration has SSH access enabled, and allows SSH access to the device from authorized users within the **Internal** firewall zone. If this configuration is sufficient for your needs, no further configuration is required. See [Allow remote access for web administration and SSH](#) for information about configuring the SSH service to allow access from remote devices.

### Required configuration items

- Enable SSH access.
- Configure access control for the SSH service.

### Additional configuration items

- Port to use for communications with the SSH service.
- Multicast DNS (mDNS) support.
- A private key to use for communications with the SSH service.

### Enable or disable the SSH service

The SSH service is enabled by default. To disable the service, or enable it if it has been disabled:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.

The **System Configuration** pane is displayed.

3. Click **Services > SSH**.
4. Click **Enable**.
5. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.

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

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

---

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

---

- Enable or disable the SSH service:

- To enable the service:

---

```
(config)> service ssh enable true
(config)>
```

---

- To disable the service:

---

```
(config)> service ssh enable false
(config)>
```

---

- Save the configuration and apply the change:

---

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

---

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

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

## Configure the service

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- Click **Services > SSH**.
- (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
- Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - Click **IPv4 Addresses**.
    - Click **Add**.
    - For **Address**, enter the IPv4 address or network that can access the device's SSH service.  
Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - any**: No limit to IPv4 addresses that can access the SSH service.
    - Click **Add** again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's SSH service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the SSH service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
  7. For **Private key**, type the private key in PEM format. If **Private key** is blank, the device will use an automatically-generated key.
  8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:
 

---

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

---
3. Configure access control:
  - To limit access to specified IPv4 addresses and networks:
 

---

```
(config)> add service ssh acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the SSH service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service ssh acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the SSH service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service ssh acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
lan                 LAN
loopback            Loopback
modem               Modem
```

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service ssh acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.
4. (Optional) Set the private key in PEM format. If not set, the device will use an automatically-generated key.

---

```
(config)> service ssh key key.pem
(config)>
```

---

5. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

- To enable the mDNS protocol:

---

```
(config)> service ssh mdns enable true
(config)>
```

---

- To disable the mDNS protocol:

---

```
(config)> service ssh mdns enable false
(config)>
```

---

6. (Optional) Set the port number for this service.  
The default setting of 22 normally should not be changed.

---

```
(config)> service ssh port 24
(config)>
```

---

7. Save the configuration and apply the change:

---

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

---

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

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

## Use SSH with key authentication

Rather than using passwords, you can use SSH keys to authenticate users connecting via SSH, SFTP, or SCP. SSH keys provide security and scalability:

- **Security:** Using SSH keys for authentication is more secure than using passwords. Unlike a password that can be guessed by an unauthorized user, SSH key pairs provide more sophisticated security. A public key configured on the IX14 device is paired with a private key on the user's PC. The private key, once generated, remains on the user's PC.
- **Scalability:** SSH keys can be used on more than one IX14 device.

### Generating SSH key pairs

On a Microsoft Windows PC, you can generate SSH key pairs using a terminal emulator application, such as **PuTTY** or **Tera Term**.

On a Linux host, an SSH key pair is usually created automatically in the user's **.ssh** directory. The private and public keys are named **id\_rsa** and **id\_rsa.pub**. If you need to generate an SSH key pair, you can use the **ssh-keygen** application.

For example, the following entry generates an RSA key pair in the user's **.ssh** directory:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa
```

The private key file is named **id\_rsa** and the public key file is named **id\_rsa.pub**. (The **.pub** extension is automatically appended to the name specified for the private key output file.)

### Required configuration items

- Name for the user
- SSH public key for the user

### Additional configuration items

- If you want to access the IX14 device using SSH over a WAN interface, configure the access control list for the SSH service to allow SSH access for the **External** firewall zone.

## WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Authentication > Users**.
4. Select an existing user or create a new user. See [User authentication](#) for information about creating a new user.
5. Click **SSH keys**.
6. In **Add SSH key**, enter a name for the SSH key and click **Add**.



7. Enter the public SSH key by pasting or typing a public encryption key that this user can use for passwordless SSH login.
8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

You can add configure passwordless SSH login for an existing user or include the support when creating a new user. See [User authentication](#) for information about creating a new user. These instructions assume an existing user named **temp\_user**.

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Add an SSH key for the user by using the `ssh_key` command and pasting or typing a public encryption key:

---

```
(config)> add auth user maria ssh_key key_name key
(config)>
```

---

where:

- *key\_name* is a name for the key.
  - *key* is a public SSH key, which you can enter by pasting or typing a public encryption key that this user can use for passwordless SSH login
4. Save the configuration and apply the change:

---

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

---

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

## Configure telnet access

By default, the telnet service is disabled.

---

**Note** Telnet is an insecure protocol and should only be used for backward-compatibility reasons, and only if the network connection is otherwise secured.

---

### Required configuration items

- Enable telnet access.
- Configure access control for the telnet service.

### Additional configuration items

- Port to use for communications with the telnet service.
- Multicast DNS (mDNS) support.

### Enable the telnet service

The telnet service is disabled by default. To enable the service:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > telnet**.
4. Click **Enable**.
5. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable the telnet service:

---

```
(config)> service telnet enable true
(config)>
```

---

4. Save the configuration and apply the change:

---

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

---

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

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

### Configure the service

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > telnet**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's telnet service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the telnet service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's telnet service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the telnet service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.

- To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
- 6. Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
- 7. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service telnet acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the telnet service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service telnet acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the telnet service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service telnet acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
lan                 LAN
loopback            Loopback
modem               Modem
```

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service telnet acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.

#### 4. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

- To enable the mDNS protocol:

---

```
(config)> service telnet mdns enable true
(config)>
```

---

- To disable the mDNS protocol:

---

```
(config)> service telnet mdns enable false
(config)>
```

---

#### 5. (Optional) Set the port number for this service.

The default setting of 23 normally should not be changed.

---

```
(config)> service telnet port 25
(config)>
```

---

#### 6. Save the configuration and apply the change:

---

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

---

#### 7. Type **exit** to exit the Admin CLI.

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

## Configure DNS

The IX14 device includes a caching DNS server which forwards queries to the DNS servers that are associated with the network interfaces, and caches the results. This server is used within the device, and cannot be disabled. Use the access control list to restrict external access to this server.

### **Required configuration items**

- Configure access control for the DNS service.

### **Additional configuration items**

- Whether the device should cache negative responses.
- Whether the device should always perform DNS queries to all available DNS servers.
- Whether to prevent upstream DNS servers from returning private IP addresses.
- Additional DNS servers, in addition to the ones associated with the device's network interfaces.
- Specific host names and their IP addresses.

To configure the DNS server:

 **WebUI**

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > DNS**.
4. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's DNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the DNS service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's DNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the DNS service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
5. (Optional) **Cache negative responses** is enabled by default. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable, click **Cache negative responses**.
6. (Optional) **Query all servers** is enabled by default. This option is useful when only some DNS servers will be able to resolve hostnames. To disable, click **Query all servers**.

7. (Optional) **Rebind protection**, if enabled, prevents upstream DNS servers from returning private IP addresses. To enable, click **Rebind protection**.
8. (Optional) **Allow localhost rebinding** is enabled by default if **Rebind protection** is enabled. This is useful for Real-time Black List (RBL) servers.
9. (Optional) To add additional DNS servers:
  - a. Click **DNS servers**.
  - b. Click **Add**.
  - c. (Optional) Enter a label for the DNS server.
  - d. For **DNS server**, enter the IP address of the DNS server.
  - e. **Domain** restricts the device's use of this DNS server based on the domain. If no domain are listed, then all queries may be sent to this server.
10. (Optional) To add host names and their IP addresses that the device's DNS server will resolve:
  - a. Click **Additional DNS hostnames**.
  - b. Click **Add**.
  - c. Type the **IP address** of the host.
  - d. For **Name**, type the hostname.
11. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Configure access control:
  - To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service dns acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.



- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service dns acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service dns acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
lan                 LAN
loopback            Loopback
modem               Modem
```

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service dns acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
```

---

---

```
src_nat true
internal
src_nat false
ipsec
src_nat false
loopback
src_nat false
setup
src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.
4. (Optional) Cache negative responses  
By default, the device's DNS server caches negative responses. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable:

---

```
(config)> service dns cache_negative_responses false
(config)>
```

---

5. (Optional) Query all servers  
By default, the device's DNS server queries all available DNS servers. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable:

---

```
(config)> service dns query_all_servers false
(config)>
```

---

6. (Optional) Rebind protection  
By default, rebind protection is disabled. If enabled, this prevents upstream DNS servers from returning private IP addresses. To enable:

---

```
(config)> service dns stop_dns_rebind false
(config)>
```

---

7. (Optional) Allow localhost rebinding  
By default, localhost rebinding is enabled by default if rebind protection is enabled. This is useful for Real-time Black List (RBL) servers. To disable:

---

```
(config)> service dns rebind_localhost_ok false
(config)>
```

---

8. (Optional) Add additional DNS servers

- a. Add a DNS server:

---

```
(config)> add service dns server end
(config service dns server 0)>
```

---

- b. Set the IP address of the DNS server:

---

```
(config service dns server 0)> address ip-addr
(config service dns server 0)>
```

---

- c. To restrict the device's use of this DNS server based on the domain, use the **domain** command. If no domain are listed, then all queries may be sent to this server.

---

```
(config service dns server 0)> domain domain
(config service dns server 0)>
```

---

- d. (Optional) Set a label for this DNS server:

---

```
(config service dns server 0)> label label
(config service dns server 0)>
```

---

9. (Optional) Add host names and their IP addresses that the device's DNS server will resolve

- a. Add a host:

---

```
(config)> add service dns host end
(config service dns host 0)>
```

---

- b. Set the IP address of the host:

---

```
(config service dns host 0)> address ip-addr
(config service dns host 0)>
```

---

- c. Set the host name:

---

```
(config service dns host 0)> name host-name
(config service dns host 0)>
```

---

10. Save the configuration and apply the change:

---

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

---

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

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

## Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for remotely managing and monitoring network devices. Network administrators can use the SNMP architecture to manage nodes, including servers, workstations, routers, switches, hubs, and other equipment on an IP network, manage network performance, find and solve network problems, and plan for network growth.

### SNMP Security

By default, the IX14 device automatically blocks SNMP packets from being received over WAN and LAN interfaces. As a result, if you want a IX14 device to receive SNMP packets, you must configure the SNMP access control list to allow the device to receive the packets.

## Configure Simple Network Management Protocol (SNMP)

### Required configuration items

- Enable SNMP.
- The user name and password used to connect to the SNMP agent.

### Additional configuration items

- Access control configuration that allows remote connections to the SNMP agent.
- The port used by the SNMP agent.
- Authentication type (either MD5 or SHA).
- Privacy protocol (either DES or AES).
- Privacy passphrase, if different than the SNMP user password.
- Enable Multicast DNS (mDNS) support.

To configure the SNMP agent on your IX14 device:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > SNMP**.
4. Click **Enable**.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's SNMP agent.  
Allowed values are:

- A single IP address or host name.
  - A network designation in CIDR notation, for example, 192.168.1.0/24.
  - **any**: No limit to IPv4 addresses that can access the SNMP agent.
- d. Click **Add** again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's SNMP agent. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the SNMP agent.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
6. Type the **Username** used to connect to the SNMP agent.
  7. Type the **Password** used to connect to the SNMP agent.
  8. (Optional) For **Port**, type the port number. The default is **161**.
  9. (Optional) Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
  10. (Optional) Select the **Authentication type**, either **MD5** or **SHA**. The default is **MD5**.
  11. (Optional) Type the **Privacy passphrase**. If not set, the password, entered above, is used.
  12. (Optional) Select the **Privacy protocol**, either **DES** or **AES**. The default is **DES**.
  13. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.



### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. Enable the SNMP agent:

---

```
(config)> service location snmp true
(config)>
```

---

4. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service snmp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the SNMP service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service snmp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the SNMP service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service snmp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

---

```
defaultip           Default IP
defaultlinklocal    Default Link-local IP
```

---

---

```
lan          LAN
loopback    Loopback
modem       Modem
```

---

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service snmp acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- a. Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.

5. Set the name of the user that will be used to connect to the SNMP agent.

---

```
(config)> service snmp username name
(config)>
```

---

6. Set the password for the user that will be used to connect to the SNMP agent:

---

```
(config)> service snmp password pwd
(config)>
```

---

7. (Optional) Set the port number for the SNMP agent. The default is **161**.

---

```
(config)> service snmp port port
(config)>
```

---

8. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. For the SNMP agent, mDNS is disabled by default. To enable:

---

```
(config)> service snmp mdns enable true
(config)>
```

---

9. (Optional) Set the authentication type. Allowed values are **MD5** or **SHA**. The default is **MD5**.

---

```
(config)> service snmp auth_type SHA
(config)>
```

---

10. (Optional) Set the privacy passphrase. If not set, the password, entered above, is used.

---

```
(config)> service snmp privacy pwd
(config)>
```

---

11. (Optional) Set the privacy protocol, either **DES** or **AES**. The default is **DES**.

---

```
(config)> service snmp privacy_protocol AES
(config)>
```

---

12. Save the configuration and apply the change:

---

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

---

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

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

## Use the SNMP service

Once the SNMP service has been configured, you can connect your SNMP manager to the device's agent.

Since the agent is read-only, command changes to the device are not possible.

### Download default MIBs

This procedure is available from the WebUI only. To download the default MIBs provided by Digi:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **System**.
3. Under the **SNMP MIBS**, click **Download MIBs**.

## System time

By default, the IX14 device synchronizes the system time by periodically connecting to the Digi NTP server, **time.devicecloud.com**. In this mode, the device queries the time server based on following events and schedule:

- At boot time.
- Once a day.



The default configuration has the system time zone set to UTC. No additional configuration is required for the system time if the default configuration is sufficient. However, you can change the default time zone and the default NTP server, as well as configuring additional NTP servers. If multiple servers are configured, a number of time samples are obtained from each of the servers and a subset of the NTP clock filter and selection algorithms are applied to select the best of these. See [Configure the system time](#) for details about changing the default configuration.

The IX14 device can also be configured to use Network Time Protocol (NTP). In this configuration, the device serves as an NTP server, providing NTP services to downstream devices. See [Network Time Protocol](#) for more information about NTP server support.

## Configure the system time

This procedure is optional.

The IX14 device's default system time configuration uses the Digi NTP server, **time.devicecloud.com**, and has the time zone set to **UTC**. You can change the default NTP server and the default time zone, as well as configuring additional NTP servers.

### Required Configuration Items

- The time zone for the IX14 device.
- At least one upstream NTP server for synchronization.

### Additional Configuration Options

- Additional upstream NTP servers.

## WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System > Time**
4. (Optional) Select the **Timezone** for the location of your IX14 device.
5. (Optional) Add upstream NTP servers that the device will use to synchronize its time. The default setting is **time.devicecloud.com**.
  - To change the default value of the NTP server:
    - a. Click **NTP servers**.
    - b. For **Server**, type a new server name.
  - To add an NTP server:
    - a. Click **NTP servers**.
    - b. Click **Add**.
    - c. For **Server**, enter the hostname of the upstream NTP server that the device will use to synchronize its time.
    - d. Click **Add** to list additional NTP servers. If multiple servers are included, servers are tried in the order listed until one succeeds.

---

**Note** This list is synchronized with the list of servers included with NTP server configuration, and changes made to one will be reflected in the other. See [Configure the device as an NTP server](#) for more information about NTP server configuration.

---

- Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

- Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

---

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

---

- (Optional) Set the timezone for the location of your IX14 device. The default is **UTC**.

---

```
(config)> system time timezone value
(config)>
```

---

Where *value* is the timezone using the format specified with the following command:

---

```
(config)> system time timezone ?
```

```
Timezone: The timezone for the location of this device. This is used to adjust
the time for log
messages. It also affects actions that occur at a specific time of day.
```

```
Format:
```

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
```

---

```
(config)>
```

---

- (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.
  - To delete the default NTP server, **time.devicecloud.com**:

---

```
(config)> del service ntp server 0
```

---

- To add the NTP server to the beginning of the list, use the index value of **0** to indicate that it should be added as the first server:

---

```
(config)> add service ntp server 0 time.server.com
(config)>
```

---

- To add the NTP server to the end of the list, use the index keyword **end**:

---

```
(config)> add service ntp server end time.server.com
(config)>
```

---

- To add the NTP server in another location in the list, use an index value to indicate the appropriate position. For example:

---

```
(config)> add service ntp server 1 time.server.com
(config)>
```

---

**Note** This list is synchronized with the list of servers included with NTP server configuration, and changes made to one will be reflected in the other. See [Configure the device as an NTP server](#) for more information about NTP server configuration.

---

5. Save the configuration and apply the change:

---

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

---

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

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

## Network Time Protocol

Network Time Protocol (NTP) enables devices connected on local and worldwide networks to synchronize their internal software and hardware clocks to the same time source. The IX14 device can be configured as an NTP server, allowing downstream hosts that are attached to the device's Local Area Networks to synchronize with the device.

When the device is configured as an NTP server, it also functions as an NTP client. The NTP client will be consistently synchronized with one or more upstream NTP servers, which means that NTP packets are transferred every few seconds. A minimum of one upstream NTP server is required. Additional NTP servers can be configured. If multiple servers are configured, a number of time samples are obtained from each of the servers and a subset of the NTP clock filter and selection algorithms are applied to select the best of these.

See [Configure the device as an NTP server](#) for information about configuring your device as an NTP server.

## Configure the device as an NTP server

### **Required Configuration Items**

- Enable the NTP service.
- At least one upstream NTP server for synchronization. The default setting is the Digi NTP server, **time.devicecloud.com**.

### Additional Configuration Options

- Additional upstream NTP servers.
- Access control list to limit downstream access to the IX14 device's NTP service.
- The time zone setting, if the default setting of UTC is not appropriate.

To configure the IX14 device's NTP service:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > NTP**.
4. Enable the IX14 device's NTP service by clicking **Enable**.
5. (Optional) Configure the access control list to limit downstream access to the IX14 device's NTP service.
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's NTP service.  
Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the NTP service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's NTP service.  
Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the NTP service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.

- c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
- d. Click **Add** again to allow access through additional firewall zones.

---

**Note** By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the IX14 device can use the NTP service.

---

6. (Optional) Add upstream NTP servers that the device will use to synchronize its time. The default setting is **time.devicecloud.com**.
  - To change the default value of the NTP server:
    - a. Click **NTP servers**.
    - b. For **Server**, type a new server name.
  - To add an NTP server:
    - a. Click **NTP servers**.
    - b. Click **Add**.
    - c. For **Server**, enter the hostname of the upstream NTP server that the device will use to synchronize its time.
    - d. Click **Add** to list additional NTP servers. If multiple servers are included, servers are tried in the order listed until one succeeds.

---

**Note** This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See [Configure the system time](#) for more information about NTP client configuration.

---

7. (Optional) Configure the system time zone. The default is **UTC**.
  - a. Click **System > Time**
  - b. Select the **Timezone** for the location of your IX14 device.
8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:
 

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

---
3. Enable the NTP service:
 

```
(config)> service NTP enable true
(config)>
```

---
4. (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.

- To delete the default NTP server, **time.devicecloud.com**:

---

```
(config)> del service ntp server 0
```

---

- To add the NTP server to the beginning of the list, use the index value of **0** to indicate that it should be added as the first server:

---

```
(config)> add service ntp server 0 time.server.com
(config)>
```

---

- To add the NTP server to the end of the list, use the index keyword **end**:

---

```
(config)> add service ntp server end time.server.com
(config)>
```

---

- To add the NTP server in another location in the list, use an index value to indicate the appropriate position. For example:

---

```
(config)> add service ntp server 1 time.server.com
(config)>
```

---

**Note** This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See [Configure the system time](#) for more information about NTP client configuration.

---

5. (Optional) Configure the access control list to limit downstream access to the IX14 device's NTP service.

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service ntp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the NTP server agent.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service ntp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the NTP server agent.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

---

```
(config)> add service ntp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

---

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
lan                 LAN
loopback            Loopback
modem               Modem
```

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service ntp acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.

---

**Note** By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the IX14 device can use the NTP service.

---

6. (Optional) Set the timezone for the location of your IX14 device. The default is **UTC**.

```
(config)> system time timezone value
(config)>
```

---

Where *value* is the timezone using the format specified with the following command:

```
(config)> system time timezone ?
```

Timezone: The timezone for the location of this device. This is used to adjust the time for log messages. It also affects actions that occur at a specific time of day.

Format:

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
```

```
(config)>
```

---

7. Save the configuration and apply the change:

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

---

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

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

## Configure a multicast route

Multicast routing allows a device to transmit data to a single multicast address, which is then distributed to a group of devices that are configured to be members of that group.

To configure a multicast route:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Services > Multicast**.
4. Type a name for the route and click **Add**.
5. The new route is enabled by default. To disable, uncheck **Enable**.
6. Type the **Source address** for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.



7. Type the **Source port**. Ensure the port is not used by another protocol.
8. Select a **Source interface** where multicast packets will arrive.
9. Select a **Destination interface** that the IX14 device will use to send multicast packets.
10. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

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

3. Add the multicast route. For example, to add a route named **test**:

```
(config)> add service multicast test
(config service multicast test)>
```

4. The multicast route is enabled by default. If it has been disabled, enable the route:

```
(config service multicast test)> enable true
(config service multicast test)>
```

5. Set the source address for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.

```
(config service multicast test)> dst ip-address
(config service multicast test)>
```

6. Set the source port for the route. Ensure the port is not used by another protocol.

```
(config service multicast test)> port port
(config service multicast test)>
```

7. Set the source interface for the route where multicast packets will arrive:

```
(config service multicast test)> src_interface interface
(config service multicast test)>
```

Display a list of available interfaces:

Use **network interface ?** to display interface information:

```
(config service multicast test)> ... network interface ?
```

```
Interfaces
```

```
Additional Configuration
```

```

-----
defaultip           Default IP
defaultlinklocal   Default Link-local IP
lan                LAN
loopback           Loopback
modem              Modem

```

```
(config service multicast test)>
```

- Set the destination interface that the IX14 device will use to send mutlicast packets.

```
(config service multicast test)> interface interface
(config service multicast test)>
```

Display a list of available interfaces:

Use **network interface ?** to display interface information:

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```

-----
defaultip           Default IP
defaultlinklocal   Default Link-local IP
lan                LAN
loopback           Loopback
modem              Modem

```

```
(config)>
```

- Save the configuration and apply the change:

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

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

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

## Enable service discovery (mDNS)

Multicast DNS mDNS is a protocol that resolves host names in small networks that do not have a DNS server. You can enable the IX14 device to use mDNS.

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- Click **Services > Service Discovery (mDNS)**.

4. **Enable** the mDNS service.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's mDNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the mDNS service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. Click **Add**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's mDNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the mDNS service.
    - d. Click **Add** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the IX14 device:
    - a. Click **Interfaces**.
    - b. Click **Add**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **Add** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. Click **Add**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **Add** again to allow access through additional firewall zones.
6. Click **Save** to save the configuration and apply the change.

The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

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

- Enable the mDNS service:

```
(config)> service mdns enable true
(config)>
```

- Configure access control:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add service mdns acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- any**: No limit to IPv4 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service mdns acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- any**: No limit to IPv6 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the IX14 device:

```
(config)> add service mdns acl interface end value
(config)>
```

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use **network interface ?** to display interface information:

```
(config)> ... network interface ?
```

Interfaces

Additional Configuration

```
-----
defaultip           Default IP
defaultlinklocal    Default Link-local IP
```

---

```
lan                LAN
loopback          Loopback
modem             Modem
```

---

```
(config)>
```

---

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service mdns acl zone end value
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

- a. Type **show firewall zones** at the config prompt:

---

```
(config)> show firewall zone
any
    src_nat false
dynamic_routes
    src_nat false
external
    src_nat true
internal
    src_nat false
ipsec
    src_nat false
loopback
    src_nat false
setup
    src_nat false
(config)>
```

---

- Repeat this step to list additional firewall zones.

5. Save the configuration and apply the change:

---

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

---

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

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

## Applications

---

The 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 applications and other scripts to be run each time the device system restarts, at specific intervals, or at a specified time.

Configure applications to run automatically .....	191
Run a Python application at the shell prompt .....	196
Start an interactive Python session .....	197
Digidevice module .....	199

## Configure applications to run automatically

You can configure an application to run automatically when the system restarts, at specific intervals, or at a specified time.

### Required configuration items

- Upload or create the Python application.
- Enable the Python application to be run automatically.
- Select whether the application should run:
  - When the device boots.
  - At a specified time.
  - At a specified interval.
  - During system maintenance.

### Additional configuration items

- A label used to identify the application.
- The action to take if the Python application finishes. The actions that can be taken are:
  - None.
  - Restart the script.
  - Reboot the device.
- The arguments for the Python application.
- Whether to write the application output and errors to the system log.
- The memory available to be used by the application.
- Whether the script should run one time only.

## Task one: Upload the application

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. From the main menu, select **Applications**.
3. Click **Choose File** and select the application file you want to upload.
4. Click **Upload**.

The uploaded file is uploaded to the `/etc/config/scripts` directory.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the command line, use the `scp` command to upload the Python application script to the IX14 device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
local
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:

To upload a Python application from a remote host with an IP address of 192.168.4.1 to the `/etc/config/scripts` directory on the IX14 device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local
/etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                100%   36MB   11.1MB/s   00:03
>
```

---

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

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

---

**Note** You can also create Python applications by using the **vi** command when logged in with shell access.

---

## Task two: Configure the application to run automatically

---

**Note** This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

---

### WebUI

- Log into the IX14 WebUI as a user with Admin access.
- On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- Click **Applications**.  
Scripts created here are also automatically entered in **System > Scheduled tasks > Custom scripts**.
- Click **Add**.
- Enable** the script.
- (Optional) For **Label**, provide a label for the script.
- For **Run mode**, select the mode that will be used to run the script. Available options are:



- **On boot:** The script will run once each time the device boots.
  - If **On boot** is selected, select the action that will be taken when the script completes in **Exit action**. Available options are:
    - **None:** Action taken when the script exits.
    - **Restart script:** Runs the script repeatedly.
    - **Reboot:** The device will reboot when the script completes.
  - **Interval:** The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **Interval** is selected:
    - For **Interval**, type the interval.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number*{w|d|h|m|s}.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
    - Click the checkbox for **Run single** to run only a single instance of the script at a time.  
If **Run single** is not selected, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.
  - **Set time:** Runs the script at a specified time of the day.
    - If **Set Time** is selected, specify the time that the script should run in **Run time**, using the format *HH:MM*.
  - **During system maintenance:** The script will run during the system maintenance time window.
- 8. For **Commands**, enter the commands that will execute the script.  
If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).
- 9. Script logging options:
  - a. Check the box for **Log script output** to log the script's output to the system log.
  - b. Check the box for **Log script errors** to log script errors to the system log.
 If neither option is selected, only the script's exit code is written to the system log.
- 10. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}.
- 11. Check the box for **Once** to configure the script to run only once at the specified time.  
If **Once** is selected, rebooting the device will cause the script to not run again. The only way to re-run the script is to:
  - Remove the script from the device and add it again.
  - Make a change to the script.
  - Uncheck **Once**.
- 12. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.



### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

- Add a script:

---

```
(config)> add application end
(config system schedule script 0)>
```

---

- Enable the application:

---

```
(config system schedule script 0)> enable true
(config system schedule script 0)>
```

---

- (Optional) Provide a label for the script.

---

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

---

where *value* is any string. If spaces are used, enclose *value* within double quotes.

- Set the mode that will be used to run the script:

---

```
(config system schedule script 0)> when mode
(config system schedule script 0)>
```

---

where *mode* is one of the following:

- **boot**: The script will run once each time the device boots.
  - If **boot** is selected, set the action that will be taken when the script completes:

---

```
(config system schedule script 0)> exit_action action
(config system schedule script 0)>
```

---

where *action* is one of the following:

- **none**: Action taken when the script exits.
  - **restart**: Runs the script repeatedly.
  - **reboot**: The device will reboot when the script completes.
- **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected:
    - Set the interval:

---

```
(config system schedule script 0)> on_interval value
(config system schedule script 0)>
```

---

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

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

---

```
(config system schedule script 0)> on_interval 600s
(config system schedule script 0)>
```

---

- (Optional) Configure the script to run only a single instance at a time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is set to **false**, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.

- **set\_time**: Runs the script at a specified time of the day.
  - If **Set Time** is selected, set the time that the script should run, using the format *HH:MM*:

---

```
(config system schedule script 0)> run_time HH:MM
(config system schedule script 0)>
```

---

- **maintenance\_time**: The script will run during the system maintenance time window.

7. Set the commands that will execute the script:

---

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

---

where *filename* is the path and filename of the script, and any related command line information.

If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

8. Script logging options:

- To log the script's output to the system log:

---

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

---

- To log script errors to the system log:

---

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

---

If **syslog\_stdout** and **syslog\_stderr** are not enabled, only the script's exit code is written to the system log.

9. Set the maximum amount of memory available to be used by the script and its subprocesses:

---

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

---

where *value* uses the syntax **number{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}**.

10. To run the script only once at the specified time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:

- Remove the script from the device and add it again.
  - Make a change to the script.
  - Disable **once**.
11. Save the configuration and apply the change:

---

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

---

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

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

## Run a Python application at the shell prompt

Python applications can be run from a file at the shell prompt. The Python application will run until it completes, displaying output and prompting for additional user input if needed. To interrupt the application, enter **CTRL-C**.

**Note** Python applications cannot be run from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See [Configure authentication groups](#) for information about configuring authentication groups that include shell access.

1. Upload the Python application to the IX14 device:

### WebUI

- a. Log into the IX14 WebUI as a user with Admin access.
- b. From the main menu, select **Applications**.
- c. Click **Choose File** and select the application file you want to upload.
- d. Click **Upload**.

The uploaded file is uploaded to the `/etc/config/scripts` directory.

### Command line

- a. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- b. At the command line, use the `scp` command to upload the Python application script to the IX14 device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- `hostname-or-ip` is the hostname or ip address of the remote host.
- `username` is the name of the user on the remote host.

- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:

To upload a Python application from a remote host with an IP address of 192.168.4.1 to the `/etc/config/scripts` directory on the IX14 device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local
/etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                               100%   36MB   11.1MB/s   00:03
>
```

---

- c. Type **exit** to exit the Admin CLI.

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

---

**Note** You can also create Python applications by using the **vi** command when logged in with shell access.

---

2. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
3. Use the **python** command to run the Python application. In the following example, the Python application, **test.py**, takes 3 parameters: **120**, **ports** and **storage**:

---

```
# python test.py 120 ports storage
```

---

## Start an interactive Python session

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

---

**Note** The Python interactive session is not available from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See [Configure authentication groups](#) for information about configuring authentication groups that include shell access.

---

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
```

---

---

```
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Type Python commands at the Python prompt. For example, to view help for the digidevice module, type:

---

```
>>> help("digidevice")
Help on package digidevice:

NAME
    digidevice - Digi device python extensions

DESCRIPTION
    This module includes various extensions that allow Python
    to interact with additional features offered by the device.
...

```

---

4. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Digidevice module

The Python **digidevice** module provides platform-specific extensions that allow you to interact with the device's configuration and interfaces. The following submodules are included with the **digidevice** module:

Use digidevice.cli to execute CLI commands .....	200
Use digidevice.datapoint to upload custom datapoints to Remote Manager .....	201
Use digidevice.config for device configuration .....	203
Use Python to respond to DRM SCI requests .....	205
Use digidevice runtime to access the runtime database .....	212

## Use digidevice.cli to execute CLI commands

Use the **digidevice.cli** Python module to issue CLI commands from Python to retrieve status and statistical information about the device.

For example, to display the system status and statistics by using an interactive Python session, use the **show system** command with the **cli** module:

1. Log into the IX14 command line as a user with shell access.

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

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **cli** submodule:

---

```
>>> from digidevice import cli
>>>
```

---

4. Execute a CLI command using the **cli.execute(command)** function. For example, to print the system status and statistics to stdout using the **show system** command:

---

```
>>> response = cli.execute("show system")
>>>
>>> print (response)
```

Model	: Digi IX14
Serial Number	: IX14-000000
Hostname	: IX14
MAC	: 0040D0133536
Hardware Version	: 50001947-01 1P
Firmware Version	: 19.8.1.30
Bootloader Version	: 1
Current Time	: 19-05-21-13.22.15 +0000
CPU	: 0.9
Uptime	: 3 days, 0 hours, 49 minutes, 8 seconds (262148s)
Temperature	: 39C
Contact	: Techpubs

---

```
>>>
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### **Help for using Python to execute IX14 CLI commands**

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



1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **cli** submodule:

---

```
>>> from digidevice import cli
>>>
```

---

4. Use the help command with **cli.execute**:

---

```
>>> help(cli.execute)
Help on function execute in module digidevice.cli:

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

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Use digidevice.datapoint to upload custom datapoints to Remote Manager

Use the **datapoint** Python module to upload custom datapoints to Digi Remote Manager (DRM). The following characteristics can be defined for a datapoint:

- Stream ID
- Value
- (Optional) Data type
  - integer
  - long
  - float
  - double
  - string
  - binary
- Units (optional)
- Timestamp (optional)
- Location (optional)
  - Tuple of latitude, longitude and altitude
- Description (optional)

- Quality (optional)
  - An integer describing the quality of the data point

For example, to use an interactive Python session to upload datapoints related to velocity, temperature, and the state of the emergency door:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **datapoint** submodule and other necessary modules:

---

```
>>> from digidevice import datapoint
>>> import time
>>>
```

---

4. Upload the datapoints to DRM:

---

```
>>> datapoint.upload("Velocity", 69, units="mph")
>>> datapoint.upload("Temperature", 24, geo_location=(54.409469, -1.718836, 129))
>>> datapoint.upload("Emergency_Door", "closed", timestamp=time.time())
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Once the datapoints have been uploaded to DRM, they can be viewed via DRM or accessed using Web Services calls. See the [Digi Remote Manager Programmers Guide](#) for more information on web services and datapoints.

### ***Help for using Python to upload custom datapoints to Remote Manager***

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

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **datapoint** submodule and other necessary modules:

---

```
>>> from digidevice import datapoint
>>>
```

---

4. Use the help command with **datapoint.upload**:

---

```
>>> help(datapoint.upload)
Help on function upload in module digidevice.datapoint:

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

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Use digidevice.config for device configuration

Use the **config** Python module to access and modify the device configuration.

### Read the device configuration

Use the **get()** method to read the device configuration:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

4. Use **config.load()** and the **get()** method to return the device's configuration:

---

```
>>> cfg = config.load()
>>> print(cfg)
...
network.interface.lan1.device=/network/bridge/lan1
network.interface.lan1.enable=true
network.interface.lan1.ipv4.address=192.168.2.1/24
network.interface.lan1.ipv4.connection_monitor.attempts=3
...
```

---

---

```
>>> interfaces = cfg.get("network.interface")
>>> print(interfaces.keys())
['aview', 'defaultip', 'defaultlinklocal', 'lan1', 'loopback', 'wan1', 'wwan1',
'wwan2']
>>> print(interfaces.get("lan.ipv4.address"))
192.168.2.1/24
>>>
```

---

### **Modify the device configuration**

Use the **set()** and **commit()** methods to modify the device configuration:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

4. Use **config.load(writable=True)** to enable write mode for the configuration:

---

```
>>> cfg = config.load(writable=True)
>>>
```

---

5. Use the **set()** method to make changes to the configuration:

---

```
>>> cfg.set("system.name", "New-Name")
>>>
```

---

6. Use the **commit()** method to save the changes:

---

```
>>> cfg.commit()
True
>>>
```

---

7. Use the **get()** method to verify the change:

---

```
>>> print(cfg.get("system.name"))
New-Name
>>>
```

---

### **Help for using Python to read and modify device configuration**

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

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

4. Use the help command with **config**:

---

```
>>> help(config)
Help on module acl.config in acl:

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

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Use Python to respond to DRM SCI requests

The **device\_request** Python module allows you to interact with Digi Remote Manager (DRM) by using DRM's Server Command Interface (SCI), a web service that allows users to access information and perform commands that relate to their devices.

Use DRM's SCI interface to create SCI requests that are sent to your IX14 device, and use the **device\_request** module to send responses to those requests to DRM.

See the [Digi Remote Manager Programmers Guide](#) for more information on SCI.

### **Task one: Use the device\_request module on your IX14 device to create a response**

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **device\_request** module:

---

```
>>> from digidevice import device_request
>>>
```

---

4. Create a function to handle the request from DRM:

---

```
>>> def handler(target, request):
...     print ("received request %s for target %s" % (request, target))
...     return "OK"
...
>>>
```

---

5. Register a callback function that will be called when the device receives a SCI request from DRM:

---

```
>>> device_request.register("myTarget", handler)
>>>
```

---

**Note** Leave the interactive Python session active while completing task two, below. Once you have completed task two, exit the interactive session by using **Ctrl-D**. You can also exit the session using **exit()** or **quit()**.

---

### **Task two: Create and send an SCI request from DRM**

The second step in using the **device\_request** module is to create an SCI request that DRM will forward to the device. For example, you can create in SCI request a the DRM API explorer:

1. In DRM, click **Documentation > API Explorer**.
2. Select the device to use as the SCI target:
  - a. Click **SCI Targets**.
  - b. Click **Add Targets**.
  - c. Enter or select the device ID of the device.
  - d. Click **Add**.
  - e. Click **OK**.
3. Click **Examples > SCI > Data Service > Send Request**.

Code similar to the following will be displayed in the HTTP message body text box:

---

```
<sci_request version="1.0">
  <data_service>
    <targets>
      <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

---

---

**Note** The value of the **target\_name** parameter in the **device\_request** element must correspond to the **target** parameter of the **device\_request.register** function in the Python script. In this example, the two are the same.

---

4. Click **Send**.

Once that the request has been sent to the device, the handler on the device is executed.

- On the device, you will receive the following output:

---

```
>>> received request
      my payload string
      for target myTarget
```

---

- In DRM, you will receive a response similar to the following:

---

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    <requests>
      <device_request target_name="myTarget" status="0">OK</device_
request>
    </requests>
  </device>
</data_service>
</sci_request>
```

---

### Example: Use **digidevice.cli** with **digidevice.device\_request**

In this example, we will use the **digidevice.cli** module in conjunction with the **digidevice.device\_request** module to return information about multiple devices to DRM.

1. Create a Python application, called `showsystem.py`, that uses the **digidevice.cli** module to create a response containing information about device and the **device\_request** module to respond with this information to a request from DRM:

---

```
from digidevice import device_request
from digidevice import cli
import time

def handler(target, request):
    return cli.execute("show system verbose")

def status_cb(error_code, error_description):
    if error_code != 0:
        print("error handling showSystem device request: %s" % error_description)

device_request.register("showSystem", handler, status_callback = status_cb)

# Do not let the process finish so that it handles device requests
while True:
    time.sleep(10)
```

---

2. Upload the `showsystem.py` application to the `/etc/config/scripts` directory on two or more Digi devices. In this example, we will upload it to two devices, and use the same request in DRM to query both devices.

See [Configure applications to run automatically](#) for information about uploading Python applications to your device. You can also create the script on the device by using the **vi** command when logged in with shell access.

3. For both devices:
  - a. Configure the device to automatically run the `showsystem.py` application on reboot, and to restart the application if it crashes. This can be done from either the WebUI or the command line:

### WebUI

- i. Log into the IX14 WebUI as a user with Admin access.
- ii. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
- iii. Click **Applications**.
- iv. Click **Add**.
- v. Select the **Enable** checkbox to enable the script.
- vi. For **Label**, type **Show system application**.
- vii. For **Run mode**, select **On boot**.
- viii. For **Exit action**, select **Restart script**.
- ix. For **Commands**, type **python /etc/config/scripts/showsystem.py**.
- x. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

- i. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- ii. At the command line, type **config** to enter configuration mode:

---

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

---

- iii. Add an application entry:

---

```
(config)> add application end
(config system schedule script 0)>
```

---

- iv. Enable the application:

---

```
(config system schedule script 0)> enable true
(config system schedule script 0)>
```

---

- v. Provide a label for the script:

---

```
(config system schedule script 0)> label "Show system application"
```

---



- vi. Configure the application to run automatically when the device reboots:

---

```
(config system schedule script 0)> when boot
```

---

- vii. Configure the application to restart if it crashes:

---

```
(config system schedule script 0)> exit_action restart
```

---

- viii. Set the command that will execute the application:

---

```
(config system schedule script 0)> commands "python
/etc/config/scripts/showsystem.py"
```

---

- ix. Save the configuration and apply the change:

---

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

---

- b. Run the showsystem.py application. You can run the application by either rebooting the device, or by running it from the shell prompt.

- To reboot the device:

- i. From the WebUI:

- i. From the main menu, click **System**.

- ii. Click **Reboot**.

- ii. From the command line, at the Admin CLI prompt, type:

---

```
> reboot
```

---

- To run the application from the shell prompt:

- i. Log into the IX14 command line as a user with shell access.

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

- ii. Type the following at the shell prompt:

---

```
# python /etc/config/scripts/showsystem.py &
#
```

---

- iii. Exit the shell:

---

```
# exit
```

---

4. In DRM, click **Documentation > API Explorer**.

5. Select the devices to use as the SCI target:

- a. Click **SCI Targets**.
- b. Click **Add Targets**.
- c. Enter or select the device ID of one of the devices.
- d. Click **Add**.

- e. Enter or select the device ID of the second device and click **Add**.
  - f. Click **OK**.
6. Click **Examples > SCI > Data Service > Send Request**.

Code similar to the following will be displayed in the HTTP message body text box:

---

```
<sci_request version="1.0">
  <data_service>
    <targets>
      <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
      <device id="00000000-00000000-0000FFFF-485740BC"/>
    </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

---

7. For the **device\_request** element, replace the value of **target\_name** with **showSystem**. This matches the **target** parameter of the **device\_request.register** function in the showsystem.py application.

---

```
<device_request target_name="showSystem">
```

---

8. Click **Send**.

You should receive a response similar to the following:

---

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    <requests>
      <device_request target_name="showSystem" status="0">Model
: Digi IX14
  Serial Number      : IX14-000068
  Hostname           : IX14
  MAC                : 0040D0133536

  Hardware Version   : 50001959-01 A
  Firmware Version   : 19.8.1.30
  Bootloader Version : 1
  Firmware Build Date : Tue, 21 May 2019 13:22:15
  Schema Version     : 461

  Timezone           : UTC
  Current Time       : Tue, 16 July 2019 21:14:12
  CPU                : 1.1
  Uptime             : 1 day, 21 hours, 49 minutes, 47 seconds
(164987s)
  Temperature       : 39C

  Contact            : Jane Smith

  Disk
  ----
```

---

---

```

Load Average           : 0.10, 0.05, 0.00
RAM Usage              : 85.176MB/250.484MB (34%)
Disk /etc/config Usage : 0.068MB/13.416MB (1%)
Disk /opt Usage        : 47.724MB/5309.752MB (1%)
Disk /overlay Usage    : MB/MB (%)
Disk /tmp Usage        : 0.004MB/40.96MB (0%)
Disk /var Usage        : 0.820MB/32.768MB (3%)</device_request>
</requests>
</device>
<device id="00000000-00000000-0000FFFF-485740BC"/>
  <requests>
    <device_request target_name="showSystem" status="0">Model
: Digi IX14
    Serial Number       : IX14-000023
    Hostname            : IX14
    MAC                 : 0040D026791C

    Hardware Version    : 50001959-01 A
    Firmware Version    : 19.8.1.30
    Bootloader Version  : 1
    Firmware Build Date : Tue, 21 May 2019 13:22:15
    Schema Version      : 461

    Timezone            : UTC
    Current Time        : Tue, 16 July 2019 21:14:12
    CPU                 : 1.1
    Uptime              : 4 day, 13 hours, 43 minutes, 22 seconds
(395002s)
    Temperature        : 37C

    Contact             : Omar Ahmad
    Disk
    ----
    Load Average       : 0.10, 0.05, 0.00
    RAM Usage           : 85.176MB/250.484MB (34%)
    Disk /etc/config Usage : 0.068MB/13.416MB (1%)
    Disk /opt Usage     : 47.724MB/5309.752MB (1%)
    Disk /overlay Usage : MB/MB (%)
    Disk /tmp Usage     : 0.004MB/40.96MB (0%)
    Disk /var Usage     : 0.820MB/32.768MB (3%)</device_request>
  </requests>
</device>
</data_service>
</sci_request>

```

---

### **Help for using Python to respond to DRM SCI requests**

Get help for respond to Digi Remote Manager (DRM) Server Command Interface (SCI) requests by accessing help for **digidevice.device\_request**:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **device\_request** submodule:

---

```
>>> from digidevice import device_request
>>>
```

---

4. Use the help command with **device\_request**:

---

```
>>> help(device_request)
Help on module digidevice.device_request in digidevice:

NAME
digidevice.device_request - APIs for registering device request handlers
...
```

---

You can also use the help command with available **device\_request** functions:

- Use the help command with **device\_request.register**:

---

```
>>> help(device_request.register)
Help on function register in module digidevice.device_request:

register(target:str, response_callback:Callable[[str, str], str], status_
callback:Callable[[int, str], NoneType]=None, xml_encoding:str='UTF-8')
...
```

---

- Use the help command with **device\_request.unregister**:

---

```
>>> help(device_request.unregister)
Help on function unregister in module digidevice.device_request:

unregister(target:str) -> bool
...
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Use digidevice runtime to access the runtime database

Use the **runt** submodule to access and modify the device runtime database.

### *Read from the runtime database*

Use the **keys()** and **get()** methods to read the device configuration:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

4. Use **start()** method to open the runtime database:

---

```
>>> runt.start()
>>>
```

---

5. Display available keys in the runtime database:

---

```
>>> print(runt.keys(""))
['advanced', 'drm', 'firmware', 'location', 'manufacture', 'metrics', 'mm',
'network', 'pam', 'serial', 'system']
>>> print(runt.keys("system"))
['boot_count', 'chassis', 'cpu_temp', 'cpu_usage', 'disk', 'load_avg', 'local_
time', 'mac', 'mcu', 'model', 'ram', 'serial', 'uptime']
>>> print(runt.get("system.mac"))
0040D0133536
```

---

6. Close the runtime database:

---

```
>>> runt.stop()
>>>
```

---

### **Modify the runtime database**

Use the **set()** method to modify the runtime database:

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

4. Use **start()** method to open the runtime database:

---

```
>>> runt.start()
>>>
```

---

5. Use the **set()** method to make changes to the runtime database:

---

```
>>> runt.set("my-variable", "my-value")
>>>
```

---

6. Use the **get()** method to verify the change:

---

```
>>> print(runt.get("my-variable"))
my-variable
>>>
```

---

7. Close the runtime database:

---

```
>>> runt.stop()
>>>
```

---

8. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### ***Help for using Python to access the runtime database***

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

1. Log into the IX14 command line as a user with shell access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.
2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.6.4 (default, Tue, 16 July 2019 21:14:12)
[GCC 4.8.3] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

4. Use the help command with **runt**:

---

```
>>> help(runt)

Help on module acl.runt in digidevice:

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

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Central management with Digi Remote Manager

---

Digi Remote Manager support .....	217
Configure Digi Remote Manager .....	217
Collect device health data and set the sample interval .....	219
Log into Digi Remote Manager .....	220
Use Digi Remote Manager to view and manage your device .....	221
Add a device to Digi Remote Manager .....	222
View Digi Remote Manager configuration and connection status .....	222
Use the Digi Remote Manager mobile app .....	223
Configure multiple devices using profiles .....	224
Learn more .....	224



## Digi Remote Manager support

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

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

To learn more about DRM features and functions, see the [Digi Remote Manager User Guide](#).

## Configure Digi Remote Manager

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

### ***Additional configuration options***

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

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

To configure Digi Remote Manager:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Central management**.
4. Digi Remote Manager support is enabled by default. To disable, uncheck **Enable central management**.
5. (Optional) For **Management server**, type the URL for the central management server. The default is the Digi Remote Manager server, [my.devicecloud.com](http://my.devicecloud.com).
6. (Optional) For **Retry interval**, type the amount of time that the IX14 device should wait before reattempting to connect to the Digi Remote Manager server after being disconnected. The default is 30 seconds.  
Allowed values are any number of hours, minutes, or seconds, and take the format **number{h|m|s}**.  
For example, to set **Retry interval** to ten minutes, enter **10m** or **600s**.
7. (Optional) For **Keep-alive interval**, type the amount of time that the IX14 device should wait between sending keep-alive messages to the Digi Remote Manager when using a non-cellular interface. The default is 60 seconds.  
Allowed values are any number of hours, minutes, or seconds, and take the format **number{h|m|s}**.  
For example, to set **Keep-alive interval** to ten minutes, enter **10m** or **600s**.

8. (Optional) For **Cellular keep-alive interval**, type the amount of time that the IX14 device should wait between sending keep-alive messages to the Digi Remote Manager when using a cellular interface. The default is 290 seconds.  
Allowed values are any number of hours, minutes, or seconds, and take the format **number{h|m|s}**.  
For example, to set **Cellular keep-alive interval** to ten minutes, enter **10m** or **600s**.
9. (Optional) For **Allowed keep-alive misses**, type the number of allowed keep-alive misses. The default is **3**.
10. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

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

---

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

---

2. (Optional) Set the URL for the central management server. The default is the Digi Remote Manager server, [my.devicecloud.com](https://my.devicecloud.com).

---

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

---

3. (Optional) Set the amount of time that the IX14 device should wait before reattempting to connect to the Digi Remote Manager server after being disconnected. The minimum value is ten seconds. The default is 30 seconds.

---

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

---

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

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

---

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

---

4. (Optional) Set the amount of time that the IX14 device should wait between sending keep-alive messages to the Digi Remote Manager when using a non-cellular interface. Allowed values are from 30 seconds to two hours. The default is 60 seconds.

---

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

---

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

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

---

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

---

5. (Optional) Set the amount of time that the IX14 device should wait between sending keep-alive messages to the Digi Remote Manager when using a cellular interface. Allowed values are from 30

seconds to two hours. The default is 290 seconds.

---

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

---

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

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

---

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

---

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

---

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

---

7. Save the configuration and apply the change:

---

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

---

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

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

## Collect device health data and set the sample interval

You can enable or disable the collection of device health data to upload to Digi Remote Manager, and configure the interval between health sample uploads. By default, device health data upload is enabled, and the health sample interval is set to 60 minutes.

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

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Monitoring > Device Health**.
4. Device health data upload is enabled by default. Click **Enable Device Health samples upload** to disable, or to enable if it has been disabled.
5. For **Health sample interval**, select the interval between health sample uploads.
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

 **Command line**

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

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

- To enable:

---

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

---

- To disable:

---

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

---

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

---

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

---

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

5. Save the configuration and apply the change:

---

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

---

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

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

## Log into Digi Remote Manager

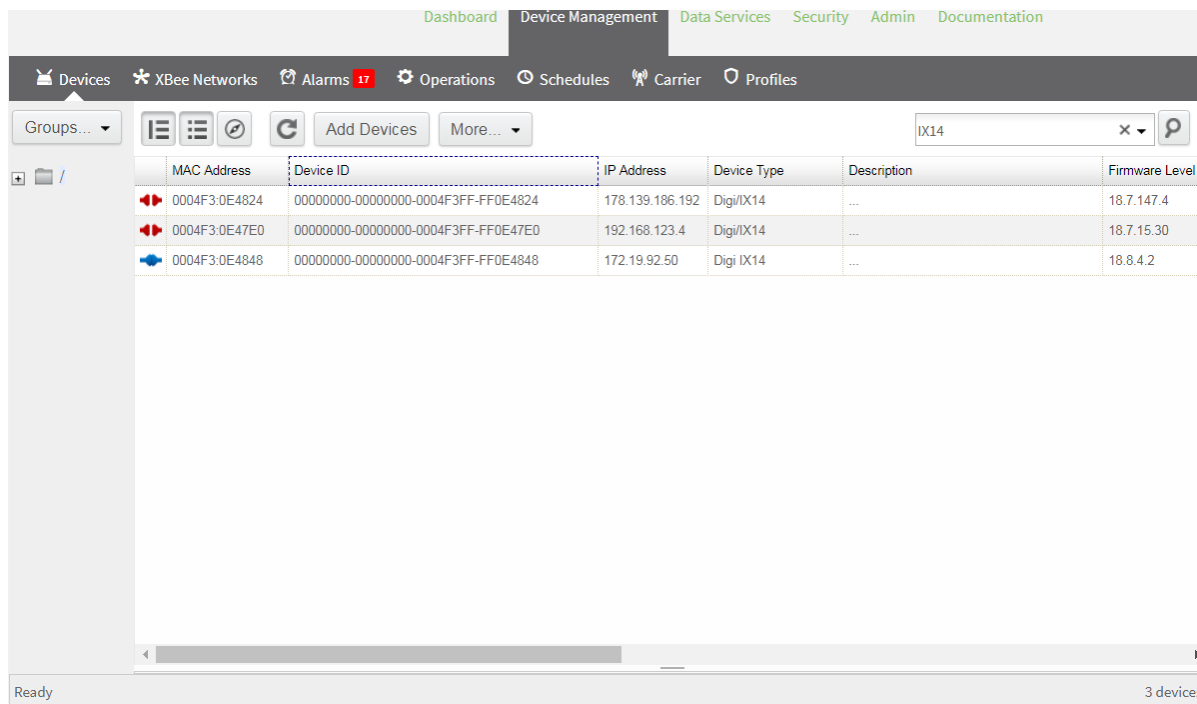
To start Digi Remote Manager

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

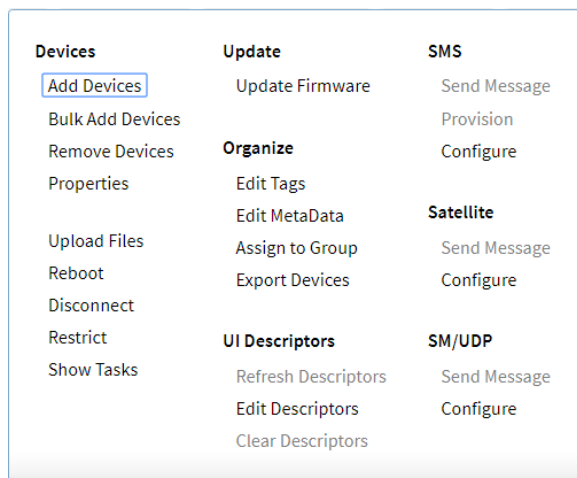
## Use Digi Remote Manager to view and manage your device

To view and manage your device:

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



4. Select your IX14 and click **Properties** to view general information for the device.
5. Click the **More** menu to perform a task.



## Add a device to Digi Remote Manager

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. Click **Add Devices**.
4. Select **MAC Address** and enter the Ethernet MAC address for your device.
5. For **Install Code**, enter the default password on the printed label packaged with your device. The same default password is also shown on the label affixed to the bottom of the device.
6. Click **Add**.
7. Click **OK**.

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

## View Digi Remote Manager configuration and connection status

To view the current Digi Remote Manager configuration:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Central management**.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. View the central management configuration:

---

```
(config)> show cloud
drm
    cellular_keep_alive 290s
    drm_url my.devicecloud.com
    keep_alive 60s
    keep_alive_misses 3
    retry_interval 30s
enable true
(config)>
```

---

1. Type **cancel** to exit configuration mode:

---

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

---

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

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

To view the status of your device's connection to Remote Manager, use the [show cloud](#) command at the command line:

### Command line

---

```
> show cloud

Device Cloud Status
-----

Status      : Connected
Server      : my.devicecloud.com
Device ID   : 00000000-00000000-0040FFFF-FF0F4594
>
```

---

The **Device ID** is the unique identifier for the device, as used by the Remote Manager.

## Use the Digi Remote Manager mobile app

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

### To download the mobile app:

- For iPhone, go to the [App Store](#)
- For Android phones, go to [Google Play](#)

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

1. From the menu, click **Log in or Sign Up**.
2. Click **Sign up** to create a new account.
3. You'll receive an email with login instructions.
4. From the **Digi Remote Manager** mobile app, click **Log in** and log into your new account.

### To register a new device:

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

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

## Configure multiple devices using profiles

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

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

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

### Learn more

- For information on using Digi Remote Manager to configure and manage 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

---

Enable IntelliFlow .....	226
Configure NetFlow Probe .....	231

## Enable IntelliFlow

IntelliFlow keeps track of network data usage and traffic information and displays the information in a series of charts available in the local WebUI. To use IntelliFlow, the IX14 must be powered on and you must have access to the local WebUI. Once you enable IntelliFlow, the **Dashboard** option appears in the main navigation menu. By default, IntelliFlow is disabled. After enabling IntelliFlow, the **Dashboard** option is included in the local WebUI main 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 IntelliFlow:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **Monitoring > IntelliFlow**.
4. Click **Enable IntelliFlow**.
5. For **Zone**, select the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone.
6. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. Enable IntelliFlow:

---

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

---

4. Set the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone:
  - a. Determine available zones:

---

```
(config)> monitoring intelliflow zone ?
```

---

Zone: The firewall zone which is assigned to the network interface(s) that IntelliFlow will see as internal clients. IntelliFlow relies on an internal to

---

---

external relationship, where the internal clients are present on the zone specified.

Format:

```
any
dynamic_routes
external
internal
ipsec
loopback
my_zone
setup
```

Default value: internal

Current value: internal

```
(config)>
```

---

- b. Set the zone to be used by IntelliFlow:

```
(config)> monitoring intelliflow zone my_zone
```

---

5. Save the configuration and apply the change:

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

---

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

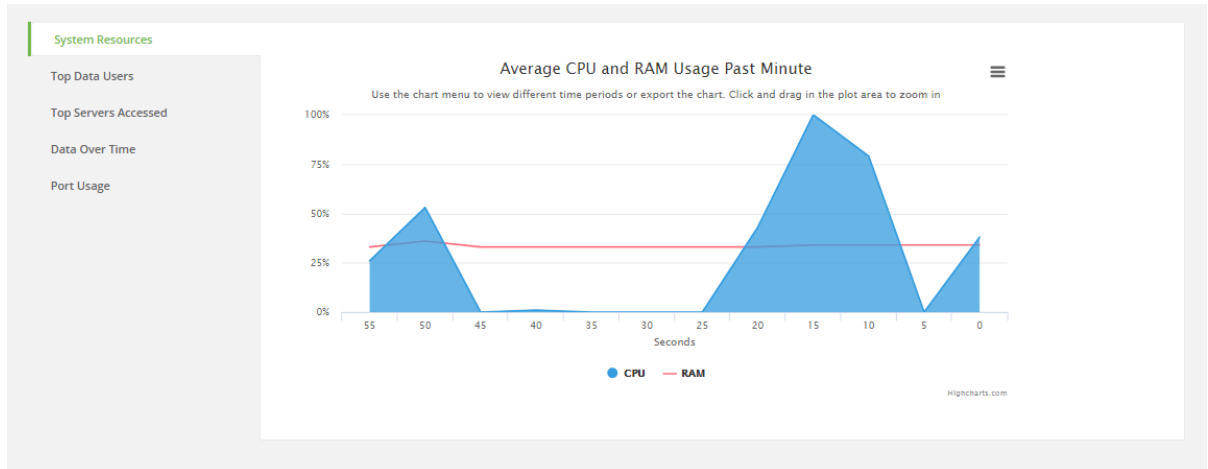
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## System resources chart

To generate a System resources chart:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. If you have not already done so, enable IntelliFlow. See [Enable IntelliFlow](#).
3. From the menu, click **Dashboard**.
4. Click **System Resources**.

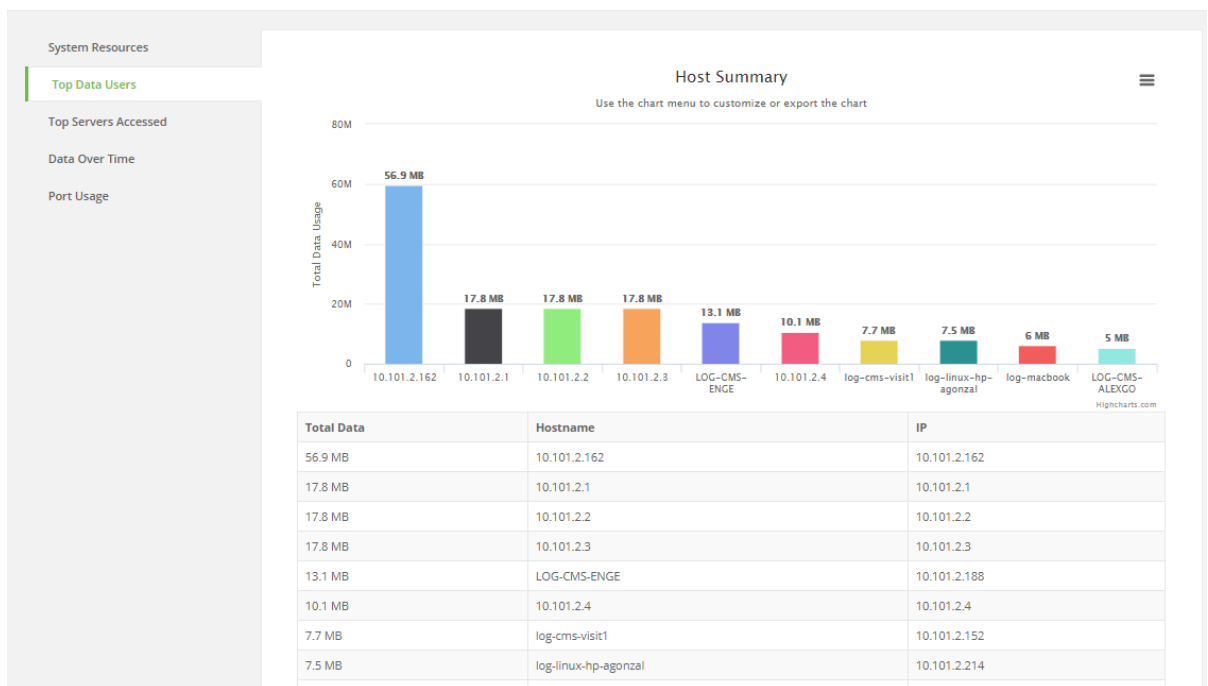


### Top data users chart

To generate a Top data users chart:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. If you have not already done so, enable IntelliFlow. See [Enable IntelliFlow](#).
3. From the menu, click **Dashboard**.
4. Click **Top Data Users**.

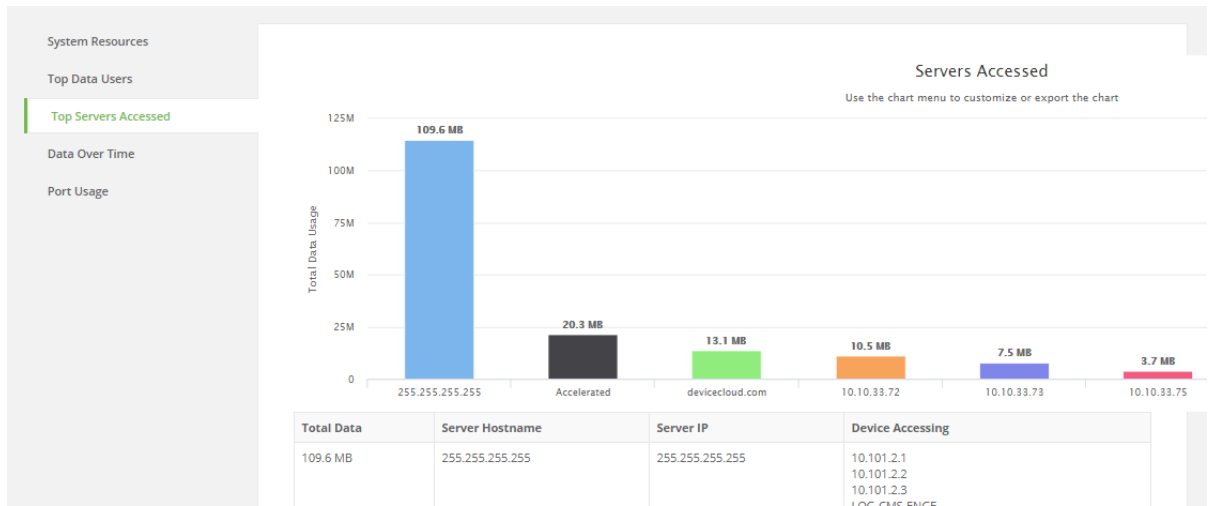


## Top servers accessed chart

To generate a Top servers accessed chart:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. If you have not already done so, enable IntelliFlow. See [Enable IntelliFlow](#).
3. From the menu, click **Dashboard**.
4. Click **Top Servers Accessed**.

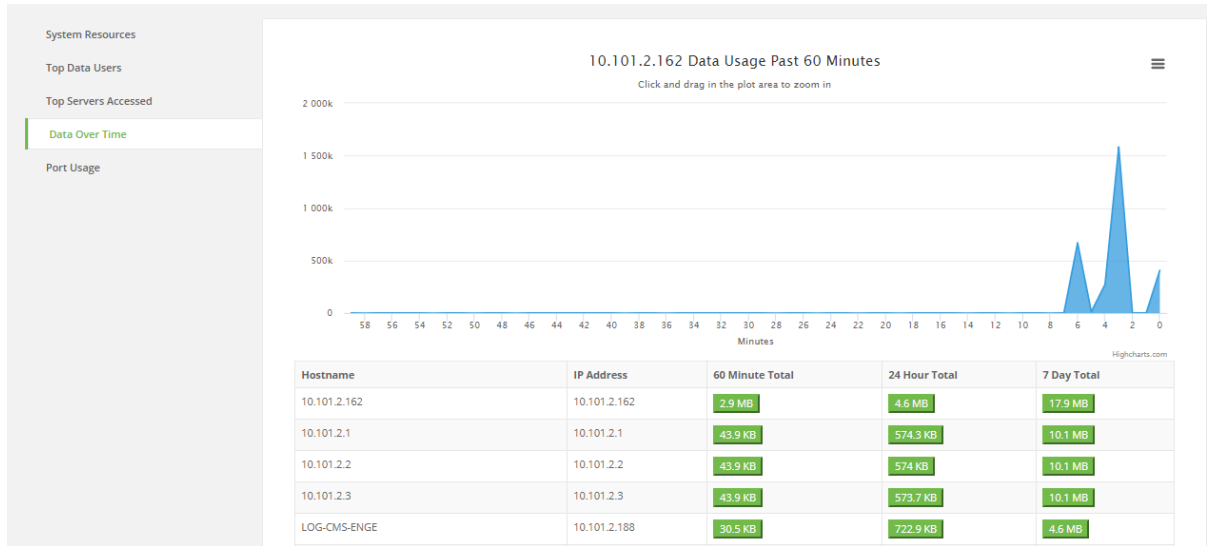


## Data over time chart

To generate a Data over time chart:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. If you have not already done so, enable IntelliFlow. See [Enable IntelliFlow](#).
3. From the menu, click **Dashboard**.
4. Click **Data Over Time**.

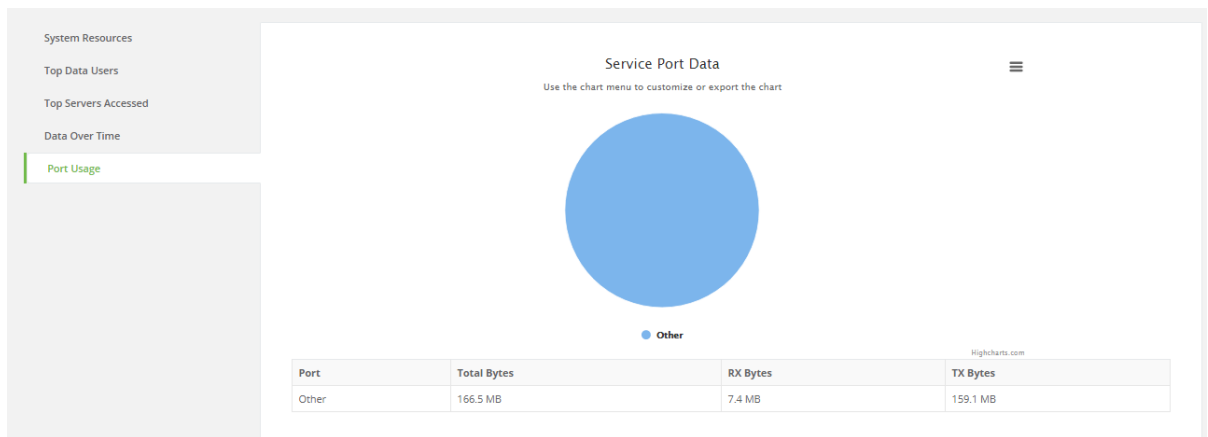


### Port usage chart

To generate a Port usage chart:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. If you have not already done so, enable IntelliFlow. See [Enable IntelliFlow](#).
3. From the menu, click **Dashboard**.
4. 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 probe is used to probe network traffic on the IX14 device and export statistics to NetFlow collectors.

### *Required configuration items*

- Enable NetFlow.
- The IP address of a NetFlow collector.

### *Additional configuration items*

- The NetFlow version.
- Enable flow sampling and select the flow sampling technique.
- The number of flows from which the flow sampler can sample.
- The number of seconds that a flow is inactive before it is exported to the NetFlow collectors.
- The number of seconds that a flow is active before it is exported to the NetFlow collectors.
- The maximum number of simultaneous flows.
- A label for the NetFlow collector.
- The port of the NetFlow collector.
- Additional NetFlow collectors.

To probe network traffic and export statistics to NetFlow collectors:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.

The **System Configuration** pane is displayed.

3. Click **Monitoring > NetFlow probe**.
4. **Enable** NetFlow probe.
5. **Protocol version:** Select the **Protocol version**. Available options are:
  - **NetFlow v5**—Supports IPv4 only.
  - **NetFlow v9**—Supports IPv4 and IPv6.
  - **NetFlow v10 (IPFIX)**—Supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

The default is **NetFlow v10 (IPFIX)**.

6. Enable **Flow sampler** by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows. Available options are:
  - **None**—No flow sampling method is used. Each flow is accounted.
  - **Deterministic**—Selects every  $n$ th flow, where  $n$  is the value of **Flow sampler population**.
  - **Random**—Randomly selects one out of every  $n$  flows, where  $n$  is the value of **Flow sampler population**.
  - **Hash**—Randomly selects one out of every  $n$  flows using the hash of the flow key, where  $n$  is the value of **Flow sampler population**.
7. For **Flow sampler population**, if you selected a flow sampler, enter the number of flows for the sampler. Allowed value is any number between **2** and **16383**. The default is **100**.
8. For **Inactive timeout**, type the the number of seconds that a flow can be inactive before sent to a collector. Allowed value is any number between **1** and **15**. The default is **15**.
9. For **Active timeout**, type the number of seconds that a flow can be active before sent to a collector. Allowed value is any number between **1** and **1800**. The default is **1800**.
10. For **Maximum flows**, type the maximum number of flows to probe simultaneously. Allowed value is any number between **0** and **2000000**. The default is **2000000**.
11. Add collectors:
  - a. Click to expand **Collectors**.
  - b. Click **Add**.
  - c. (Optional) Type a **Label** for the collector.
  - d. For **Address**, type the IP address of the collector.
  - e. (Optional) For **Port**, enter the port number used by the collector. The default is 2055.
 Repeat to add additional collectors.
12. Click **Save** to save the configuration and apply the change.  
 The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### **Command line**

1. Log into the IX14 command line as a user with Admin access.  
 Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.



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

---

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

---

3. Enable NetFlow:

---

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

---

4. Set the protocol version:

---

```
(config)> monitoring netflow protocol version
(config)>
```

---

where *version* is one of:

- **v5**—NetFlow v5 supports IPv4 only.
- **v9**—NetFlow v9 supports IPv4 and IPv6.
- **v10**—NetFlow v10 (IPFIX) supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

The default is **v10**.

4. Enable flow sampling by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows.

---

```
(config)> monitoring netflow sampler type
(config)>
```

---

where *type* is one of:

- **none**—No flow sampling method is used. Each flow is accounted.
- **deterministic**—Selects every *n*th flow, where *n* is the value of the flow sample population.
- **random**—Randomly selects one out of every *n* flows, where *n* is the value of the flow sample population.
- **hash**—Randomly selects one out of every *n* flows using the hash of the flow key, where *n* is the value of the flow sample population.

5. If you are using a flow sampler, set the number of flows for the sampler:

---

```
(config)> monitoring netflow sampler_population value
(config)>
```

---

where *value* is any number between **2** and **16383**. The default is **100**.

6. Set the number of seconds that a flow can be inactive before sent to a collector:

---

```
(config)> monitoring netflow inactive_timeout value
(config)>
```

---

where *value* is any is any number between **1** and **15**. The default is **15**.

7. Set the number of seconds that a flow can be active before sent to a collector:

---

```
(config)> monitoring netflow active_timeout value
(config)>
```

---

where *value* is any is any number between **1** and **1800**. The default is **1800**.

8. Set the maximum number of flows to probe simultaneously:

---

```
(config)> monitoring netflow max_flows value
(config)>
```

---

where *value* is any is any number between **0** and **2000000**. The default is **2000000**.

9. Add collectors:

- a. Add a collector:

---

```
(config)> add monitoring netflow collector end
(config monitoring netflow collector 0)>
```

---

- b. Set the IP address of the collector:

---

```
(config monitoring netflow collector 0)> address ip_address
(config monitoring netflow collector 0)>
```

---

- c. (Optional) Set the port used by the collector:

---

```
(config monitoring netflow collector 0)> port port
(config monitoring netflow collector 0)>
```

---

- d. (Optional) Set a label for the collector:

---

```
(config monitoring netflow collector 0)> label "This is a collector."
(config monitoring netflow collector 0)>
```

---

Repeat to add additional collectors.

10. Save the configuration and apply the change:

---

```
(config monitoring netflow collector 0)> save
Configuration saved.
>
```

---

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

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

## Diagnostics

---

Generate a support report .....	236
View event and system logs .....	237
Configure syslog servers .....	239
Configure options for the event and system logs .....	240
Analyze network traffic .....	245
Use the ping command to troubleshoot network connections .....	250
Use the traceroute command to diagnose IP routing problems .....	250

## Generate a support report

To generate and download a support report:

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **System**.
3. Under **Support Report**, click **Download Report**.

Attach the support report to any support requests.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

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

3. Use the **system support-report** command to generate the report:

```
> system support-report /etc/config/
Saving support report to /etc/config/support-report-0040D0133536-19-05-21-
13.22.15.bin
Support report saved.
>
```

4. Use the **scp** command to transfer the report to a remote host:

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/etc/config/support-report-0040D0133536-19-05-21-13.22.15.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-19-05-21-13.22.15.bin
>
```

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

## View event and system logs

See [Configure options for the event and system logs](#) for information about configuring the information displayed in event and system logs.

### To view events:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the main menu, click **Events** to display the **Event Viewer**.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use [show event](#) at the Admin CLI prompt:

---

```
> show event
```

Timestamp	Type	Category	Message
Aug 8 21:42:37	status	stat	intf=eth1~type=ethernet~rx=11332435~tx=5038762
Aug 8 21:42:35	status	system	local_time=Thu, 08 Aug 2019 21:42:35 +0000~uptime=3 hours, 0 minutes, 48 seconds
...			

---

3. (Optional) Use the **show event number *num*** command to limit the number of lines that are displayed. For example, to limit the event list to the most recent ten lines:

---

```
> show event number 10
```

Timestamp	Type	Category	Message
Aug 8 21:42:37	status	stat	intf=eth1~type=ethernet~rx=11332435~tx=5038762
Aug 8 21:42:35	status	system	local_time=Thu, 08 Aug 2019 21:42:35 +0000~uptime=3 hours, 0 minutes, 48 seconds
...			

---

4. (Optional) Use the **show event table *value*** command to limit the number of lines that are displayed. Allowed values are **error**, **info**, and **status**. For example, to limit the event list to only info messages:

---

```
> show event table info
```

Timestamp	Type	Category	Message
Aug 08 22:01:26	info	user	name=admin~service=cli~state=opened~remote=192.168.1.2

---

---

```
Aug 08 22:01:25 info user
name=admin~service=cli~state=closed~remote=192.168.1.2
...
>
```

---

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

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

#### To view system logs:

#### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System Logs**.
4. Use the pull-down filter to select the type of events you want to include in the log.

#### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use **show log** at the Admin CLI prompt:

---

```
> show log
```

Timestamp	Message
Aug 8 21:54:34	IX14 netifd: Interface 'interface_wan' is setting up now
Aug 8 21:54:35	IX14 firewalld[621]: reloading status
...	

```
>
```

---

3. (Optional) Use the **show log number num** command to limit the number of lines that are displayed. For example, to limit the log to the most recent ten lines:

---

```
> show log number 10
```

Timestamp	Message
Aug 8 21:54:34	IX14 netifd: Interface 'interface_wan' is setting up now
Aug 8 21:54:35	IX14 firewalld[621]: reloading status
...	

```
>
```

---

4. (Optional) Use the **show log filter value** command to limit the number of lines that are displayed. Allowed values are **critical**, **warning**, **info**, and **debug**. For example, to limit the event list to only info messages:

---

```
> show log filter info
```

Timestamp	Type	Category	Message
Aug 08 22:01:26	info	user	name=admin~service=cli~state=opened~remote=192.168.1.2
Aug 08 22:01:25	info	user	name=admin~service=cli~state=closed~remote=192.168.1.2
...			

---

```
>
```

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

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

## Configure syslog servers

You can configure remote syslog servers for storing event and system logs.

### WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System > Log**
4. Add and configure a remote syslog server:
  - a. Click to expand **Server list**.
  - b. Click **Add**.
  - c. **Enable** the server.
  - d. Type the host name or IP address of the **Server**.
  - e. Select the event categories that will be sent to the server.
5. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

## 3. (Optional) To configure remote syslog servers:

## a. Add a remote server:

```
(config)> add system log remote end
(config system log remote 1)>
```

## b. Enable the server:

```
(config system log remote 1)> enable true
(config system log remote 1)>
```

## c. Set the host name or IP address of the server:

```
(config system log remote 1)> server hostname
(config system log remote 1)>
```

## d. The event categories that will be sent to the server are automatically enabled when the server is enabled. To disable:

## ■ To disable informational event messages:

```
(config system log remote 1)> info false
(config system log remote 1)>
```

## ■ To disable status event messages:

```
(config system log remote 1)> status false
(config system log remote 1)>
```

## ■ To disable informational event messages:

```
(config system log remote 1)> error false
(config system log remote 1)>
```

## 4. Save the configuration and apply the change:

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

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

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

## Configure options for the event and system logs

The default configuration for event and system logging is:

- The heartbeat interval, which determines the amount of time to wait before sending a heartbeat event if no other events have been sent, is set to 30 minutes.
- All event categories are enabled.

To change or disable the heartbeat interval, or to disable event categories, and to perform other log configuration:



## WebUI

1. Log into the IX14 WebUI as a user with Admin access.
2. On the menu, click **Configuration**.  
The **System Configuration** pane is displayed.
3. Click **System > Log**
4. (Optional) To change the **Heartbeat interval** from the default of 30 minutes, type a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Heartbeat interval** to ten minutes, enter **10m** or **600s**.  
To disable the **Heartbeat interval**, enter **0s**.
5. (Optional) To disable event categories, or to enable them if they have been disabled:
  - a. Click to expand **Event Categories**.
  - b. Click an event category to expand.
  - c. Depending on the event category, you can enable or disable informational events, status events, and error events. Some categories also allow you to set the **Status interval**, which is the time interval between periodic status events.
6. (Optional) To configure remote syslog servers to which log messages will be sent:
  - a. Click to expand **Server list**.
  - b. Click **Add**.
  - c. **Enable** the server.
  - d. Type the host name or IP address of the **Server**.
  - e. Select the event categories that will be sent to the server.
7. Enable **Preserve system logs** to save the current session's system log after a reboot.  
By default, the IX14 device erases system logs each time the device is powered off or rebooted.

---

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

---

8. Click **Save** to save the configuration and apply the change.  
The **Save** button is located at the bottom of the WebUI page. You may need to scroll to the bottom of the page to locate it.

## Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

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

---

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

---

3. (Optional) To change the heartbeat interval from the default of 30 minutes, set a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent.

---

```
(config)> system log heartbeat_interval value
(config)>
```

---

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

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

---

```
(config)> system log heartbeat_interval 600s
(config)>
```

---

To disable the heartbeat interval, set the value to **0s**

4. Enable preserve system logs functionality to save the current session's system log after a reboot. By default, the IX14 device erases system logs each time the device is powered off or rebooted.

---

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

---



---

```
(config)> system log persistent true
(config)>
```

---

5. (Optional) To disable event categories, or to enable them if they have been disabled:
  - a. Use the question mark (?) to determine available event categories:

---

```
(config)> system log event ?
```

```
Event categories: Settings to enable individual event categories.
```

```
Additional Configuration
```

```
-----
--
arping                ARP ping
config                Configuration
dhcpserver            DHCP server
firmware              Firmware
location              Location
modem                 Modem
netmon                Active recovery
network               Network interfaces
openvpn               OpenVPN
portal                Captive portal
remote                Remote control
```

---

---

restart	Restart
serial	Serial
sms	SMS commands
speed	Speed
stat	Network statistics
user	User
wireless	WiFi
wol	Wake-On-LAN

---

```
(config)> system log event
```

---

- b. Depending on the event category, you can enable or disable informational events, status events, and error events. Some categories also allow you to set the status interval, which is the time interval between periodic status events. For example, to configure DHCP server logging:
- i. Use the question mark (?) to determine what events are available for DHCP server logging configuration:

---

```
(config)> system log event dhcpserver ?
...
DHCP server: Settings for DHCP server events. Informational events are
generated
when a lease is obtained or released. Status events report the current
list of
leases.
```

Parameters	Current Value	
-----	-----	-----
info	true	Enable informational events
status	true	Enable status events
status_interval	30m	Status interval

```
(config)> system log event dhcpserver
```

---

- ii. To disable informational messages for the DHCP server:

---

```
(config)> system log event dhcpserver info false
(config)>
```

---

- iii. To change the status interval:

---

```
(config)> system log event dhcpserver status_interval value
(config)>
```

---

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

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

---

```
(config)> system log event dhcpserver status_interval 600s
(config)>
```

---

6. (Optional) To configure remote syslog servers to which log messages will be sent:

a. Add a remote server:

```
(config)> add system log remote end  
(config system log remote 1)>
```

b. Enable the server:

```
(config system log remote 1)> enable true  
(config system log remote 1)>
```

c. Set the host name or IP address of the server:

```
(config system log remote 1)> server hostname  
(config system log remote 1)>
```

d. The event categories that will be sent to the server are automatically enabled when the server is enabled. To disable:

■ To disable informational event messages:

```
(config system log remote 1)> info false  
(config system log remote 1)>
```

■ To disable status event messages:

```
(config system log remote 1)> status false  
(config system log remote 1)>
```

■ To disable informational event messages:

```
(config system log remote 1)> error false  
(config system log remote 1)>
```

7. Save the configuration and apply the change:

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

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

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

## Analyze network traffic

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:

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **cli-legacy**:

```
> cli-legacy
#
```

3. Set the interfaces for capturing packets using the **analyzer interfaces** command. For example, to capture data on the ethernet and cellular interfaces:

```
# analyzer interfaces eth0 wwan0
```

To display the available interfaces, enter the **analyzer 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 **analyzer 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 **analyzer 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 **analyzer filter** parameter. For example:

---

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

---

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

## Example filters for capturing data traffic

The following are examples of filters on data traffic capturing for several types of network data.

### Example IPv4 capture filters

Capture traffic to and from IP host **192.168.1.1**:

---

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

---

Capture traffic from IP host **192.168.1.1**:

---

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

---

Capture traffic to IP host **192.168.1.1**:

---

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

---

Capture traffic for a particular IP protocol:

---

```
# analyzer filter ip proto <protocol>
```

---

Replace **<protocol>** with a number in the range of **1** to **255** or one of the following keywords: **\icmp**, **icmp6**, **igmp**, **pim**, **ah**, **esp**, **vrp**, **\udp**, or **\tcp**.

---

**Note** When you specify **\icmp**, **\tcp**, or **\udp** as a protocol, you must precede the name with the backslash character.

---

Capture traffic to and from a TCP port **80**:

---

```
# analyzer filter ip proto \tcp and port 80
```

---

Capture traffic to UDP port **53**:

---

```
# analyzer filter ip proto \udp and dst port 53
```

---

Capture traffic from UDP port **53**:

---

```
# analyzer filter ip proto \udp and src port 53
```

---

Capture to and from IP host **10.0.0.1** but filter out ports **22** and **80**:

---

```
# analyzer filter ip host 10.0.0.1 and not (port 22 or port 80)
```

---

### **Example Ethernet capture filters**

Capture Ethernet packets to and from host **00:40:FF:0F:45:94**:

---

```
# analyzer filter ether host 00:40:FF:0F:45:94
```

---

Capture Ethernet packets from host **00:40:FF:0F:45:94**:

---

```
# analyzer filter ether src 00:40:FF:0F:45:94:
```

---

Capture Ethernet packets to host **00:40:FF:0F:45:94**:

---

```
# analyzer filter ether dst 00:40:FF:0F:45:94
```

---

### **Show captured traffic data**

To view captured data traffic, use the **analyzer 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+gcc9146.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 > 239.255.255.255.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 **analyzer 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.

1. Type **exit** to exit cli-legacy mode:

---

```
# exit
>
```

---

2. Type **scp** to use the Secure Copy program to copy the file to your PC:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
remote
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX14 device.

For example:

To download the traffic saved in the file **/etc/config/analyzer/eth0.pcpng** to a PC with the IP **192.168.210.2**, for a user named **maria**, to the **/home/maria** directory:

---

```
> scp host 192.168.210.2 user maria remote /home/maria local
/etc/config/analyzer/eth0.pcpng to remote
```

```
maria@192.168.210.2's password:
```

```
eth0.pcpng                               100%  11KB 851.3KB/s   00:00
```

---

## Clear captured data

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

---

```
# analyzer clear
```

---

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

---

## Use the ping command to troubleshoot network connections

Use the [ping](#) command to troubleshoot connectivity problems.

### Ping to check internet connection

To check your internet connection:

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type the ping command followed by the host name or IP address of the server to be pinged:

---

```
> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=10.7 ms
...
>
```

---

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

### Stop ping commands

To stop pings when the number of pings to send (the **count** parameter) has been set to a high value, enter **Ctrl+C**.

## Use the traceroute command to diagnose IP routing problems

Use the **traceroute** command to diagnose IP routing problems. This command traces the route to a remote IP host and displays results. The **traceroute** command differs from [ping](#) in that traceroute shows where the route fails, while ping simply returns a single error on failure.

See the [traceroute](#) command description for command syntax and examples. The **traceroute** command has several parameters. Only **host** is required.

- **host**: The IP address of the destination host.
- **bypass**: Send directly to a host on an attached network.
- **debug**: Enable socket level debugging.
- **dontfragment**: Do not fragment probe packets.
- **first\_ttl**: Specifies with what TTL to start. (Default: 1)
- **gateway**: Route the packet through a specified gateway.
- **icmp**: Use ICMP ECHO for probes.
- **interface**: Specifies the interface.

- **ipchecksums**: Calculate ip checksums.
- **max\_ttl**: Specifies the maximum number of hops. (Default: 30)
- **nomap**: Do not map IP addresses to host names
- **nqueries**: Sets the number of probe packets per hop. (Default: 3)
- **packetlen**: Total size of the probing packet. (Default: -1)
- **pausesecs**: Minimal time interval between probes (Default: 0)
- **port**: Specifies the destination port. (Default: -1)
- **src\_addr**: Chooses an alternative source address.
- **tos**: Set Type of Service. (Default: -1)
- **verbose**: Verbose output.
- **waittime**: Max wait for a response to a probe. (Default: 5)

### Example

This example shows using **traceroute** to verify that the IX14 device can route to host **8.8.8.8** ([www.google.com](http://www.google.com)) through the default gateway. The command output shows that **15** routing hops were required to reach the host:

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, use the **traceroute** command to view IP routing information:

---

```
> traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 52 byte packets
 1 192.168.8.1 (192.168.8.1) 0 ms 0 ms 0 ms
 2 10.10.10.10 (10.10.10.10) 0 ms 2 ms 2 ms
 3 * 10.10.8.23 (10.10.8.23) 1 ms 1 ms
 4 96.34.84.22 (96.34.84.22) 1 ms 1 ms 1 ms
 5 96.34.81.190 (96.34.81.190) 2 ms 2 ms 2 ms
 6 * * *
 7 96.34.2.12 (96.34.2.12) 11 ms 11 ms 11 ms
 8 * * *
 9 8.8.8.8 (8.8.8.8) 11 ms 11 ms 11 ms
>
```

---

By entering a **whois** command on a Unix device, the output shows that the route is as follows:

1. **192/8**: The local network of the IX14 device.
2. **192.168.8.1**: The local network gateway to the Internet.
3. **96/8**: Charter Communications, the network provider.
4. **216/8**: Google Inc.

### Stop the traceroute process

To stop the traceroute process, enter **Ctrl-C**.

## File system

---

File system .....	253
Display directory contents .....	253
Create a directory .....	253
Display file contents .....	254
Copy a file or directory .....	255
Move or rename a file or directory .....	255
Delete a file or directory .....	256
Upload and download files .....	257

## File system

The IX14 local file system has approximately 100 MB of space available for storing files, such as Python programs, alternative configuration files and firmware versions, and release files, such as cellular module images. The writable directories within the filesystem are:

- /tmp
- /opt
- /etc/config

Files stored in the /tmp directory do not persist across reboots. Therefore, /tmp is a good location to upload temporary files, such as files used for firmware updates. Files stored in /opt and /etc/config do persist across reboots, but are deleted if a factory reset of the system is performed. See [Reset the device to factory defaults](#) for more information.

## Display directory contents

This procedure is not available through the WebUI. To display directory contents by using the Admin CLI, use the `ls` command, specifying the name of the directory.

For example:

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **mkdir /path/dir\_name**. For example, to create a directory named **temp** in **/etc/config**:

---

```
> ls /etc/config
...
-rw-r--r--  1 root    root          1436 Aug 12 21:36 ssl.crt
-rw-----  1 root    root          3895 Aug 12 21:36 ssl.pem
-rw-r--r--  1 root    root           10 Aug  5 06:41 start
drwxr-xr-x  2 root    root           160 Aug 25 17:49 temp
>
```

---

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

## Create a directory

### Command line

This procedure is not available through the WebUI. To make a new directory, use the `mkdir` command, specifying the name of the directory.

For example:

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **mkdir /path/dir\_name**. For example, to create a directory named **temp** in **/etc/config**:

---

```
> mkdir /etc/config/temp
>
```

---

3. Verify that the directory was created:

---

```
> ls /etc/config
...
-rw-r--r--  1 root    root      1436 Aug 12 21:36 ssl.crt
-rw-----  1 root    root      3895 Aug 12 21:36 ssl.pem
-rw-r--r--  1 root    root         10 Aug  5 06:41 start
drwxr-xr-x  2 root    root        160 Aug 25 17:49 temp
>
```

---

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

## Display file contents

This procedure is not available through the WebUI. To display the contents of a file by using the Admin CLI, use the [more](#) command, specifying the name of the directory.

For example:

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **more /path/filename**. For example, to view the content of the file **accns.json** in **/etc/config**:

---

```
> more /etc/config/accns.json
{
  "auth":
    "user": {
      "root": {
        "password":
"$2a$05$W1s1s1oxsadf/n4J0XT.Rgr6ewr1yerHtXQdbafsatGswKg0YUm"
      }
    }
  },
  "schema": {
    "version": "461"
  }
}
```

---

---

```

    }
  }
>

```

---

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

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

## Copy a file or directory

This procedure is not available through the WebUI. To copy a file or directory by using the Admin CLI, use the **cp** command, specifying the existing path and filename followed by the path and filename of the new file, or specifying the existing path and directory name followed by the path and directory name of the new directory.

### Command line

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **cp /path/filename|dir\_name /path[filename]|dir\_name**. For example:
  - To copy the file **/etc/config/accns.json** to a file named **backup\_cfg.json** in a directory named **/etc/config/test**, enter the following:

---

```

> cp /etc/config/accns.json /etc/config/test/backup_cfg.json
>

```

---

- To copy a directory named **/etc/config/test** to **/opt**:

---

```

> cp /etc/config/test/ /opt/
>

```

---

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

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

## Move or rename a file or directory

This procedure is not available through the WebUI. To move or rename a file or directory by using the Admin CLI, use the **mv** command.

### Command line

To rename a file named **test.py** in **/etc/config/scripts** to **final.py**:

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type:

---

```
> mv /etc/config/scripts/test.py /etc/config/scripts/final.py
>
```

---

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

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

To move **test.py** from **/etc/config/scripts** to **/opt**:

1. Log into the IX14 command line as a user with Admin access.

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

2. At the Admin CLI prompt, type:

---

```
> mv /etc/config/scripts/test.py /opt/
>
```

---

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

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

## Delete a file or directory

This procedure is not available through the WebUI. To delete a file or directory by using the Admin CLI, use the [rm](#) command.

### Command line

To delete a file named **test.py** in **/etc/config/scripts**:

1. Log into the IX14 command line as a user with Admin access.

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

2. At the Admin CLI prompt, type:

---

```
> rm /etc/config/scripts/test.py
rm: remove '/etc/config/scripts/test.py'? yes
>
```

---

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

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

To delete a directory named **temp** from **/opt**:

1. Log into the IX14 command line as a user with Admin access.

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



2. At the Admin CLI prompt, type:

---

```
> rm /opt/temp/
rm: descend into directory '/opt/temp'? yes
rm: remove directory '/opt/temp'? yes
>
```

---

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

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

## Upload and download files

This procedure is not available through the WebUI. You can download and upload files by using the [scp](#) Secure Copy command, or by using a utility such as SSH File Transfer Protocol (SFTP) or an SFTP application like FileZilla.

### Upload or download files using the Secure Copy command

#### **Copy a file from a remote host to the IX14 device**

To copy a file from a remote host to the IX14 device, issue the [scp](#) command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
local
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the /etc/config directory on the IX14 device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/IX14-19.8.1.30.bin local
/etc/config/ to local
admin@192.168.4.1's password: adminpwd
IX14->19.8.1.30.bin          100%   36MB   11.1MB/s   00:03
>
```

---

#### **Transfer a file from the IX14 device to a remote host**

To copy a file from the IX14 device to a remote host, issue the [scp](#) command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
remote
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX14 device.

For example:

To copy a support report from the IX14 device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

---

```
> system support-report /etc/config/  
Saving support report to /etc/config/support-report-0040D0133536-19-05-21-  
13.22.15.bin  
Support report saved.  
>
```

---

2. Use the **scp** command to transfer the report to a remote host:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local  
/etc/config/support-report-0040D0133536-19-05-21-13.22.15.bin to remote  
admin@192.168.4.1's password: adminpwd  
support-report-0040D0133536-19-05-21-13.22.15.bin  
>
```

---

## Upload or download files using SFTP

### ***Transfer a file from a remote host to the IX14 device***

This example uploads firmware from a remote host to the IX14 device with an IP address of **192.168.2.1**, using the username **ahmed**:

---

```
$ sftp ahmed@192.168.2.1  
Password:  
Connected to 192.168.2.1  
sftp> put IX14-19.8.1.30  
Uploading IX14-19.8.1.30 to IX14-19.8.1.30  
IX14-19.8.1.30  
 100% 24M 830.4KB/s 00:00  
sftp> exit  
$
```

---

**Transfer a file from the IX14 device to a remote host**

This example downloads a file named **test.py** from the IX14 device at the IP address of **192.168.2.1** with a username of **ahmed** to the local directory on the remote host:

---

```
$ sftp ahmed@192.168.2.1
Password:
Connected to 192.168.2.1
sftp> get test.py
Fetching test.py to test.py
test.py
 100% 254   0.3KB/s   00:00
sftp> exit
$
```

---

## Digi IX14 regulatory and safety statements

---

### Notes, cautions, and warnings

---



**WARNING!** To comply with FCC/IC RF exposure limits, maintain at least a **20 cm** distance between any IX14 antennas 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 IX14 reverts to factory default settings.

---

### Restricted access location notice for 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.

---

## RF exposure statement

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

## Federal Communication (FCC) Part 15 Class B

### Radio Frequency Interference (RFI) (FCC 15.105)

The Digi IX14 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)

IX14 complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

### Modifications (FCC 15.21)

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

## European Community - CE Mark Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for the IX14 concerning emissions, EMC, and safety. For more information, see [www.digi.com/resources/certifications](http://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 IX14 is certified for use in several European countries. For information, visit [www.digi.com/resources/certifications](http://www.digi.com/resources/certifications).

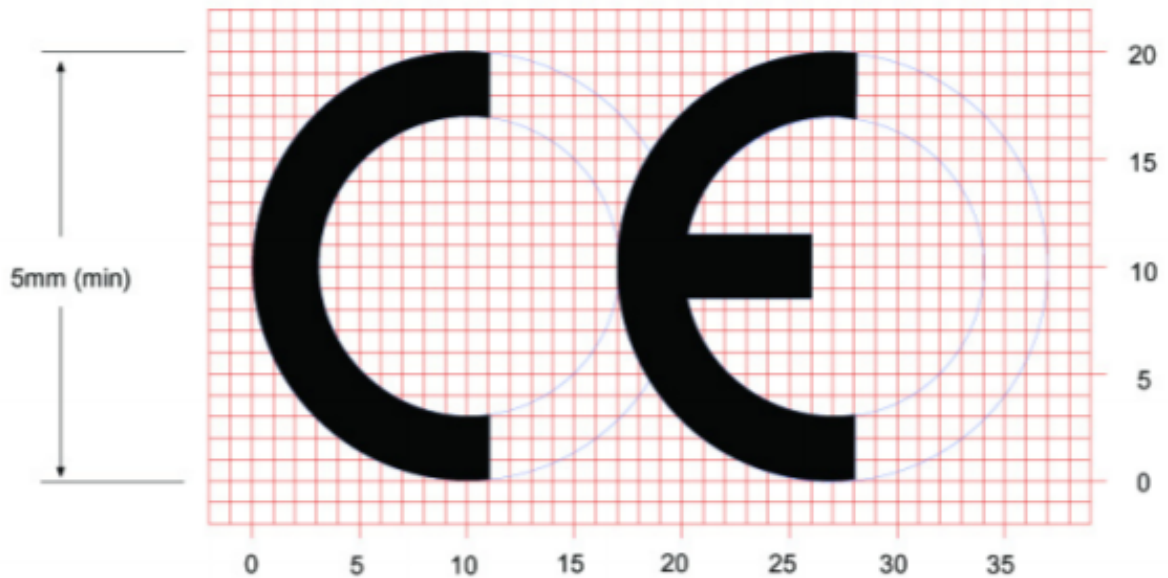
If the IX14 is incorporated into a product, the manufacturer must ensure compliance of the final product with articles 3.1a and 3.1b of the RE Directive (Radio Equipment Directive). A Declaration of Conformity must be issued for each of these standards and kept on file as described in the RE

Directive (Radio Equipment Directive). Furthermore, the manufacturer must maintain a copy of the (product name) 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.

#### **OEM labeling requirements**

The 'CE' marking must be affixed to a visible location on the OEM product.

#### **CE labeling requirements**



The CE mark shall consist of the initials “CE” taking the following form:

- If the CE marking is reduced or enlarged, the proportions given in the above graduated drawing must be respected.
- The CE marking must have a height of at least 5mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

## Maximum transmit power for radio frequencies

The following tables show the maximum transmit power for frequency bands.

### Cellular frequency bands

Frequency bands	Maximum transmit power
Cellular LTE 700 MHz Cellular LTE 800 MHz Cellular LTE 850 MHz Cellular LTE 900 MHz Cellular LTE 1700 MHz Cellular LTE 1800 MHz Cellular LTE 1900 MHz Cellular LTE 2100 MHz	200 mW
Cellular LTE 2600 MHz Cellular LTE 2300 MHz Cellular LTE 2500 MHz	158.49 mW

### Wi-Fi frequency bands

Frequency bands	Maximum transmit power
13 overlapping channels at 22 MHz or 40 MHz wide spaced at 5 MHz Centered at 2.412 MHz to 2.472 MHz	651.784 mW
165 overlapping channels at 22 MHz or 40 MHz or 80 MHz wide spaced at 5 MHz Centered at 5180 MHz to 5825 MHz	351.295 mW

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

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class B prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

## RoHS compliance statement

All Digi International Inc. products that are compliant with the RoHS Directive (EU Directive 2002/95/EC and subsequent amendments) are marked as **RoHS COMPLIANT**. RoHS COMPLIANT means that the substances restricted by the EU Directive 2002/95/EC and subsequent amendments of the European Parliament are not contained in a finished product above threshold limits mandated by EU Directive 2002/95/EC and subsequent amendments, unless the restrictive substance is subject of an exemption contained in the RoHS Directive. Digi International Inc., cannot guarantee that inventory held by distributors or other third parties is RoHS compliant.

## Safety notices

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

## Safety statements



**WARNING!** RISK OF EXPLOSION IF BATTERY IS REPLACED BY INCORRECT BATTERY TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

---



**ATTENTION!** IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS

---



**WARNING!** For ambient temperatures above 60° C, this equipment must be installed in a Restricted Access Location only.

---





**AVERTISSEMENT!** Cet équipement est destiné à être installé dans un lieu d'accès restreint uniquement.



**CAUTION!** Hot parts!

To avoid burns when handling device parts, wait at least one half hour after switching off the device before handling parts.



**PRUDENCE!** Pièces chaudes!

Doigts brûlés lors de la manipulation des pièces. Attendez une demi-heure après la mise hors tension avant de manipuler les pièces

## 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 placed 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.

## 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	<ul style="list-style-type: none"><li>■ EN 300 328 v1.8.1</li><li>■ EN 301-489-17 V3.1.12017</li><li>■ EN 301-489-52 V1.1.0:2016</li><li>■ FCC Part 15 Subpart B Class B</li></ul>
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 IX14 datasheet, available on the IX14 product page.

## Command line interface

---

Access the command line interface .....	269
Log in to the command line interface .....	269
Exit the command line interface .....	270
Execute a command from the web interface .....	270
Display help for commands and parameters .....	271
Auto-complete commands and parameters .....	273
Available commands .....	274
Use the scp command .....	275
Display status and statistics using the show command .....	276
Device configuration using the command line interface .....	278
Execute configuration commands at the root Admin CLI prompt .....	278
Configuration mode .....	280

## Access the command line interface

You can access the IX14 command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

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

To access the command line, your device must be configured to allow access, and you must log in with a user who has been configured for the appropriate access. For further information about configuring access to these services, see:

- Serial: [Configure the serial port](#)
- WebUI: [Configure the web administration service](#)
- SSH: [Configure SSH access](#)
- Telnet: [Configure telnet access](#)

## Log in to the command line interface

### Command line

1. Connect to the IX14 device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See [Access the command line interface](#) for more information.
  - For serial connections, the default configuration is:
    - **115200** baud rate
    - **8** data bits
    - **no** parity
    - **1** stop bit
    - **no** flow control
  - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** on the WAN/ETH1 .
2. At the login prompt, enter the username and password of a user with Admin access:

---

```
login: root
Password: *****
```

---

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

3. Depending on your device model and the configuration of your user, you may be presented with another menu, for example:

---

Access selection menu:

```
a: Admin CLI
1: Serial: port1          (9600,8,1,none,none)
2: Serial: port2          (9600,8,1,none,none)
q: Quit
```

---

---

```
Select access or quit [admin] :
```

---

Type **a** or **admin** to access the IX14 command line.

You will now be connected to the Admin CLI:

---

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

---

```
>
```

---

## Exit the command line interface

### Command line

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

---

```
> exit
```

---

2. Depending on your device model and the configuration of your user, you may be presented with another menu, for example:

---

```
Access selection menu:
```

```

a: Admin CLI
1: Serial: port1      (9600,8,1,none,none)
2: Serial: port2      (9600,8,1,none,none)
q: Quit
```

---

```
Select access or quit [admin] :
```

---

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

## Execute a command from the web interface

1. Log into the IX14 WebUI as a user with Admin access.
2. At the main menu, click **Terminal**. The device console appears.

---

```
IX14 login:
```

---

3. Log into the IX14 command line as a user with Admin access.

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

The Admin CLI prompt appears.

---

```
>
```

---

## Display help for commands and parameters

### The help command

When executed from the root command prompt, **help** displays information about autocomplete operations, how to move the cursor on the IX14 command line, and other keyboard shortcuts:

---

```
> help

Commands
-----
?          Show commands help
<Tab>     Tab completion, displays all valid commands to complete command,
          if only one command is possible, it is used
<Space>   Like tab except shortest prefix is used if command is valid
<Enter>   Enter an input. If quoting then a new line is created instead. If
          the input is invalid then characters will be deleted until a
          prefix for a valid command is found.

Ctrl + A  Move cursor to start of line
Ctrl + E  Move cursor to end of line
Ctrl + W  Delete word under cursor until start of line or [\'," ,\,/,.]
Ctrl + R  If the current input is invalid then characters will be deleted
          until a prefix for a valid command is found.

Ctrl + left  Jump cursor left until start of line or [\'," ,\,/,.]
Ctrl + right Jump cursor right until start of line or [\'," ,\,/,.]

>
```

---

### The question mark (?) command

When executed from the root command prompt, **?** displays available commands:

---

```
> ?

Commands
-----
config      View and modify the configuration
exit        Exit the CLI
cli-legacy  Enter the legacy Admin CLI.
cp          Copy a file or directory.
help        Show CLI editing and navigation commands.
ls          List a directory.
mkdir       Create a directory.
modem       Modem commands.
more        View a file.
mv          Move a file or directory.
ping        Ping a host.
reboot      Reboot the system.
rm          Remove a file or directory.
scp         Copy a file or directory over SSH.
show        Show instance statistics.
system      System commands.
traceroute  Print the route packets trace to network host.
update      Update firmware.

>
```

---

>

## Display help for individual commands

When included with a command name, both **?** and **help** provide further information about the command. For example:

1. To display further information about the **show** command, type either **show ?** or **show help**:

> show ?

Commands

```
-----
arp          Show ARP tables.cloudShow drm statistics.
cloud       Show drm statistics
config      Show config deltas.
dhcp-lease  Show DHCP leases.
event       Show event list
ipsec       Show IPsec statistics.
log         Show syslog.
manufacture Show manufacturer information.
modem       Show modem statistics.
network     Show network interface statistics.
openvpn     Show OpenVPN statistics.
route       Show IP routing information.
serial      Show serial statistics.
system      Show system statistics.
version     Show firmware version.
```

> show

2. To display a syntax diagram and parameter information about a specific command:

> show arp ?

Syntax: arp [ipv4] [ipv6] [verbose]

Parameters

```
-----
ipv4        Display IPv4 routes.
ipv6        Display IPv6 routes.
verbose     Display more information.
```

> show arp



## Use the Tab key or the space bar to display abbreviated help

When executed from the root command prompt, pressing the **Tab** key or the space bar displays an abbreviated list of available commands:

---

```
><space>
config      exit      cli-legacy cp      help      ls      mkdir
modem      more      mv        ping      reboot    rm      scp
show       system    traceroute update
>
```

---

Similar behavior is available with any command name:

---

```
> config network interface <space>
..          ...          defaultip          defaultlinklocal lan
loopback    modem
> config network interface
```

---

## Auto-complete commands and parameters

When entering a command and parameter, press the **Tab** key to cause the command line interface to auto-complete as much of the command and parameter as possible. Typing the space bar has similar behavior. If multiple commands are available that will match the entered text, auto-complete is not performed and the available commands are displayed instead.

Auto-complete applies to these command elements only :

- Command names. For example, typing **net<Tab>** auto-completes the command as **network**.
- Parameter names. For example:
  - **ping hostname int<Tab>** auto-completes the parameter as **interface**.
  - **system b<Tab>** auto-completes the parameter as **backup**.
- Parameter values, where the value is one of an enumeration or an on/off type; for example:

---

```
(config)> serial port1 enable t<Tab>
```

---

auto-completes to

---

```
(config)> serial port1 enable true
```

---

Auto-complete does not function for:

- Parameter values that are string types.
- Integer values.
- File names.
- Select parameters passed to commands that perform an action.

## Available commands

The following commands are available from the root command prompt:

Command	Description
<b>config</b>	Used to view and modify the configuration.  See <a href="#">Device configuration using the command line interface</a> for more information about using the <b>config</b> command.
<b>exit</b>	Exits the CLI.
<b>cli-legacy</b>	Changes to legacy CLI mode.
<b>cp</b>	Copies a file or directory.
<b>help</b>	Displays: <ul style="list-style-type: none"> <li>■ CLI editing and navigation commands, when executed from the root command prompt.</li> <li>■ Available commands, syntax diagram, and parameter information, when executed in conjunction with another command.</li> </ul> See <a href="#">Display help for commands and parameters</a> for information about the <b>help</b> command.
<b>ls</b>	Lists the contents of a directory.
<b>mkdir</b>	Creates a directory.
<b>modem</b>	Executes modem commands.
<b>more</b>	Displays the contents of a file.
<b>mv</b>	Moves a file or directory.
<b>ping</b>	Pings a remote host using Internet Control Message Protocol (ICMP) Echo Request messages.
<b>reboot</b>	Reboots the IX14 device.
<b>rm</b>	Removes a file.
<b>scp</b>	Uses the secure copy protocol (SCP) to transfer files between the IX14 device and a remote host.  See <a href="#">Use the scp command</a> for information about using the <b>scp</b> command.
<b>show</b>	Displays information about the device and the device's configuration.  See <a href="#">Display status and statistics using the show command</a> for more information about the show command.
<b>system</b>	Issues commands related to system functionality.

Command	Description
<b>tracert</b>	Sends and tracks route packets to a destination host.
<b>update</b>	Updates the device firmware.

**Note** For commands that operate on the IX14's file system, such as the **cp**, **ls**, and **mkdir** commands, see [File system](#) for information about the file system, including how to copy, move and delete files and directories.

## Use the scp command

The **scp** command uses Secure Copy Protocol (SCP) to transfer files between the IX14 device and a remote host.

### Required configuration items

- The hostname or IP address of the remote host.
- The username and password of the user on the remote host.
- Whether the file is being copied to the IX14 device from a remote host, or to the remote host from the IX14 device.
  - If the file is being copied to the IX14 device from a remote host:
    - The path and filename of the file on the remote host that will be copied to the IX14 device.
    - The location on the IX14 device where the file will be copied.
  - If the file is being copied to a remote host from the IX14 device:
    - The path and filename of the file on the IX14 device that will be copied to the remote host.
    - The location on the remote host where the file will be copied.

### Copy a file from a remote host to the IX14 device

To copy a file from a remote host to the IX14 device, issue the **scp** command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the IX14 device.
- *local-path* is the location on the IX14 device where the file will be copied.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the /etc/config directory on the IX14 device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/IX14-19.8.1.30.bin local
/etc/config/ to local
admin@192.168.4.1's password: adminpwd
IX14->19.8.1.30.bin          100%   36MB   11.1MB/s   00:03
>
```

---

### Transfer a file from the IX14 device to a remote host

To copy a file from the IX14 device to a remote host, issue the `scp` command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
remote
```

---

where:

- *hostname-or-ip* is the hostname or ip address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the IX14 device.

For example:

To copy a support report from the IX14 device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

---

```
> system support-report /etc/config/
Saving support report to /etc/config/support-report-0040D0133536-19-05-21-
13.22.15.bin
Support report saved.
>
```

---

2. Use the **scp** command to transfer the report to a remote host:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/etc/config/support-report-0040D0133536-19-05-21-13.22.15.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-19-05-21-13.22.15.bin
>
```

---

## Display status and statistics using the show command

The IX14 **show** command display status and statistics for various features.

For example:

### show config

The `show config` command displays all the configuration settings for the device that have been changed from the default settings. This is a particularly useful when troubleshooting the device.

---

```
> show config

auth tacacs+ service "login"
auth user root password
```

---

```

"$2a$05$WlJQhquI7BgSytkpobKhaeLPtWraGANBcrLEaJX/wJv63JENW/H0u"
add auth user admin
add auth user admin group end "admin"
add auth user admin group end "serial"
auth user admin password
"$2a$05$RdGYz1sLKbWrqe6cZjlsd.otg03JZR6n9939XV6EYWUSP0tMAz05W"
network interface lan ipv4 type "dhcp"
network interface lan zone "external"
network interface modem modem apn 0 apn "10569.mcs"
network interface modem modem apn_lock "true"
schema version "445"

>
    
```

## show system

The [show system](#) command displays system information and statistics for the device, including CPU usage.

```

> show system

Model                : Digi IX14
Serial Number        : IX14-000068
Hostname              : TIX14
MAC                  : 0040D0133536

Hardware Version     : 50001947-01 1P
Firmware Version     : 19.8.1.30
Bootloader Version   : 1

Current Time         : Tue, 16 July 2019 21:14:12
CPU                  : 2.7
Uptime               : 23 hours, 30 minutes, 21 seconds (84621s)
Temperature          : 38C

Description          : Digi IX14
Contact              : username

>
    
```

## show network

The [show network](#) command displays status and statistics for network interfaces.

```

> show network

Interface      Proto  Status  Address
-----
defaultip      IPv4   up       192.168.210.1/24
defaultlinklocal IPv4   up       169.254.100.100/16
lan            IPv4   up       192.168.3.1
lan            IPv6   up       0:0:0:0:0:ffff:c0a8:301
loopback       IPv4   up       127.0.0.1/8
wan            IPv4   up       192.168.4.1/24
wan            IPv6   up       fd00:2704::240:ffff:fe80:120/64

>
    
```

## Device configuration using the command line interface

The **config** command allows for device configuration from the command line. All configuration tasks that can be performed by using the WebUI can also be performed by using the **config** command.

There are two ways to invoke the **config** command from the CLI:

- Execute the **config** command and parameters at the root prompt. See [Execute configuration commands at the root Admin CLI prompt](#) for more information.
- Enter configuration mode by executing the **config** command without any parameters. See [Configuration mode](#) for more information.

### Execute configuration commands at the root Admin CLI prompt

You can execute the **config** command at the root Admin CLI prompt with any appropriate parameters. When the **config** command is used in this way, changes to the device's configuration are automatically saved when the command is executed.

For example, to disable the SSH service from the root prompt, enter the following command:

---

```
> config service ssh enable false
>
```

---

The IX14 device's ssh service is now disabled.

---

**Note** When the **config** command is executed at the root prompt, certain configuration actions that are available in configuration mode cannot be performed. This includes validating configuration changes, canceling and reverting configuration changes, and performing actions on elements in lists. See [Configuration mode](#) for information about using configuration mode.

---

### Display help for the config command from the root Admin CLI prompt

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character after the **config** command. For example:

1. 

```
> config ?
```
- 

Will display the following help information:

---

```
> config ?
```

Additional Configuration

```
-----
application          Custom scripts
auth                  Authentication
cloud                 Central management
firewall              Firewall
monitoring            Monitoring
network               Network
serial                Serial
service               Services
```

---

---

```
system          System
vpn             VPN
```

Run "config" with no arguments to enter the configuration editing mode.

```
> config
```

---

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command:

```
> config service ?
Services
```

```
Additional Configuration
```

---

```
bluetooth      Bluetooth
dns            DNS
mdns          Service Discovery (mDNS)
multicast      Multicast
ntp           NTP
remote_control Remote control
snmp          SNMP
ssh           SSH
telnet        Telnet
web_admin     Web administration
```

```
> config service
```

---

3. Next, display help for the **config service ssh** command:

```
> config service ssh ?
```

SSH: An SSH server for managing the device.

Parameters	Current Value	
enable	true	Enable
key	[private]	Private key
port	22	Port

```
Additional Configuration
```

---

```
acl           Access control list
mdns
```

```
> config service ssh
```

---

4. Lastly, display the allowed values and other information for the **enable** parameter:

```
> config service ssh enable ?
```

Enable: Enable the service.

---

---

```
Format: true, false, yes, no, 1, 0
Default value: true
Current value: true
```

```
> config service ssh enable
```

---

## Configuration mode

Configuration mode allows you to perform multiple configuration tasks and validate the changes prior to saving them. You can cancel all changes without saving them at any time. Configuration changes do not take effect until the configuration is saved.

### Enable configuration mode

To enable configuration mode, at the root prompt, enter the **config** command without any parameters:

---

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

---

When the command line is in configuration mode, the prompt will change to include **(config)**, to indicate that you are currently in configuration mode.

### Enter configuration commands in configuration mode

There are two ways to enter configuration commands while in configuration mode:

- Enter the full command string from the config prompt.  
For example, to disable the ssh service by entering the full command string at the config prompt:

---

```
(config)> service ssh enable false
(config)>
```

---

- Execute commands by moving through the configuration schema.  
For example, to disable the ssh service by moving through the configuration and then executing the **enable false** command:
1. At the **config** prompt, enter **service** to move to the **service** node:

---

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

---

2. Enter **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

3. Enter **enable false** to disable the **ssh** service:

---

```
(config service ssh)> enable false
(config service ssh)>
```

---



See [Move within the configuration schema](#) for more information about moving within the configuration.

## Save changes and exit configuration mode

To save changes that you have made to the configuration while in configuration mode, use **save**. The save command automatically validates the configuration changes; the configuration will not be saved if it is not valid. Note that you can also validate configuration changes at any time while in configuration mode by using the **validate** command.

---

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

---

After using **save** to save changes to the configuration, you will automatically exit configuration mode. To return to configuration mode, type **config** again.

## Exit configuration mode without saving changes

You can discard any unsaved configuration changes and exit configuration mode by using the **cancel** command:

---

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

---

After using **cancel** to discard unsaved changes to the configuration, you will automatically exit configuration mode.

## Configuration actions

In configuration mode, configuration actions are available to perform tasks related to saving or canceling the configuration changes, and to manage items and elements in lists. The commands can be listed by entering a question mark (?) at the **config** prompt.

The following actions are available:

Configuration actions	Description
<b>cancel</b>	Discards unsaved configuration changes and exits configuration mode.
<b>save</b>	Saves configuration changes and exits configuration mode.
<b>validate</b>	Validates configuration changes.
<b>revert</b>	Reverts the configuration to default settings. See <a href="#">The revert command</a> for more information.
<b>show</b>	Displays configuration settings.

Configuration actions	Description
<b>add</b>	Adds a named element, or an element in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>add</b> command with lists.
<b>del</b>	Deletes a named element, or an element in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>del</b> command with lists.
<b>move</b>	Moves elements in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>move</b> command with lists.

## Display command line help in configuration mode

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character at the **config** prompt. For example:

1. Enter **?** at the **config** prompt:

```
(config)> ?
```

This will display the following help information:

```
(config)> ?
```

```
Additional Configuration
```

```
-----
application      Custom scripts
auth              Authentication
cloud             Central management
firewall          Firewall
modem             Modem
monitoring        Monitoring
network           Network
serial            Serial
service           Services
system            System
vpn               VPN
```

```
(config)>
```

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command, use one of the following methods:

- At the **config** prompt, enter **service ?**:

```
(config)> service ?
```

- At the **config** prompt:
  - a. Enter **service** to move to the **service** node:

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

- b. Enter **?** to display help for the **service** node:

```
(config service)> ?
```

Either of these methods will display the following information:

```
config> service ?

Services

Additional Configuration
-----
dns                DNS
mdns               Service Discovery (mDNS)
multicast          Multicast
ntp                NTP
remote_control     Remote control
snmp               SNMP
ssh                SSH
telnet             Telnet
web_admin          Web administration

(config)> service
```

3. Next, to display help for the **service ssh** command, use one of the following methods:

- At the **config** prompt, enter **service ssh ?**:

```
(config)> service ssh ?
```

- At the **config** prompt:
  - a. Enter **service** to move to the **service** node:

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

- b. Enter **ssh** to move to the **ssh** node:

```
(config service)> ssh
(config service ssh)>
```

- c. Enter **?** to display help for the **ssh** node:

```
(config service ssh)> ?
```

Either of these methods will display the following information:

```
(config)> service ssh ?
```

---

SSH: An SSH server for managing the device.

Parameters	Current Value	
enable	true	Enable
key	[private]	Private key
port	22	Port

Additional Configuration

---

acl	Access control list
mdns	

```
(config)> service ssh
```

4. Lastly, to display allowed values and other information for the **enable** parameter, use one of the following methods:

- At the **config** prompt, enter **service ssh enable ?**:

```
(config)> service ssh enable ?
```

- At the **config** prompt:

- a. Enter **service** to move to the **service** node:

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

- b. Enter **ssh** to move to the **ssh** node:

```
(config service)> ssh
(config service ssh)>
```

- c. Enter **enable ?** to display help for the **enable** parameter:

```
(config service ssh)> enable ?
(config service ssh)>
```

Either of these methods will display the following information:

```
(config)> service ssh enable ?
```

---

Enable: Enable the service.  
 Format: true, false, yes, no, 1, 0  
 Default value: true  
 Current value: true

```
(config)> service ssh enable
```

## Move within the configuration schema

You can perform configuration tasks at the CLI by moving within the configuration.

- Move forward one node in the configuration by entering the name of an Additional Configuration option:

1. At the **config** prompt, type **service** to move to the **service** node:

---

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

---

2. Type **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

3. Type **acl** to move to the **acl** node:

---

```
(config service ssh)> acl
(config service ssh acl)>
```

---

4. Type **zone** to move to the **zone** node:

---

```
(config service ssh acl)> zone
(config service ssh acl zone)>
```

---

You can also enter multiple nodes at once to move multiple steps in the configuration:

---

```
(config)> service ssh acl zone
(config service ssh acl zone)>
```

---

- Move backward one node in the configuration by entering two periods (..):

---

```
(config service ssh acl zone)> ..
(config service ssh acl)>
```

---

You can also move back multiples nodes in the configuration by typing multiple sets of two periods:

---

```
(config service ssh acl zone)> .. .. ..
(config service)>
```

---

- Move to the root of the config prompt from anywhere within the configuration by entering three periods (...):

---

```
(config service ssh acl zone)> ...
(config)>
```

---

## Manage elements in lists

While in configuration mode, you can use the **add**, **del**, and **move** action commands to manage elements in a list. When working with lists, these actions require an index number to identify the list item that will be acted on.

### Add elements to a list

When used with parameters that contains lists of elements, the **add** command is used to add an element to the list.

For example, to add an authentication method:

1. Display current authentication method by using the **show** command:

---

```
(config)> show auth method
0 local
(config)>
```

---

2. Add an authentication method by using the **add index\_item** command. For example:

- To add the TACACS+ authentication method to the beginning of the list, use the index number **0**:

---

```
(config)> add auth method 0 tacacs+
(config)> show auth method
0 tacacs+
1 local
(config)>
```

---

- To add the TACACS+ authentication method to the end of the list, use the **end** keyword:

---

```
(config)> add auth method end tacacs+
(config)> show auth method
0 local
1 tacacs+
(config)>
```

---

#### The end keyword

As demonstrated above, the **end** keyword is used to add an element to the end of a list. Additionally, the **end** keyword is used to add an element to a list that does not have any elements.

For example, to add an authentication group to a user that has just been created:

1. Use the **show** command to verify that the user is not currently a member of any groups:

---

```
(config)> show auth user new-user group
(config)>
```

---

2. Use the **end** keyword to add the admin group to the user's configuration:

---

```
(config)> add auth user new-user group end admin
(config)>
```

---

3. Use the **show** command again to verify that the admin group has been added to the user's configuration:

---

```
(config)> show auth user new-user group
0 admin
(config)>
```

---

### Delete elements from a list

When used with parameters that contains lists of elements, the **del** command is used to delete an element in the list.

For example, to delete an authentication method:

1. Use the **show** command to display current authentication method configuration:

---

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

---

2. Delete one of the authentication methods by using the **del index\_number** command. For example:
  - a. To delete the local authentication method, use the index number **0**:

---

```
(config)> del auth method 0
(config)>
```

---

- b. Use the **show** command to verify that the local authentication method was removed:

---

```
(config)> show auth method
0 tacacs+
1 radius
(config)>
```

---

### Move elements within a list

Use the **move** command to reorder elements in a list.

For example, to reorder the authentication methods:

1. Use the **show** command to display current authentication method configuration:

---

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

---

2. To configure the device to use TACACS+ authentication first to authenticate a user, use the **move index\_number\_1 index\_number\_2** command:

---

```
(config)> move auth method 1 0
(config)>
```

---

3. Use the **show** command again to verify the change:

---

```
(config)> show auth method
0 tacacs+
1 local
2 radius
(config)>
```

---

## The revert command

The **revert** command is used to revert changes to the IX14 device's configuration and restore default configuration settings. The behavior of the revert command varies depending on where in the configuration hierarchy the command is executed, and whether the optional **path** parameter is used. After executing the revert command, you must save the configuration changes by using the **save** command. You can also discard the configuration changes by using the **cancel** command.



**CAUTION!** The **revert** command reverts all changes to the default configuration, not only unsaved changes.

---

### Revert all configuration changes to default settings

To discard all configuration changes and revert to default settings, use the **revert** command at the config prompt without the optional **path** parameter:

1. At the config prompt, enter **revert**:

---

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

---

2. Set the password for the root user prior to saving the changes:

---

```
(config)> auth user root password pwd
(config)>
```

---

3. Save the configuration and apply the change:

---

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

---

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

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

### Revert a subset of configuration changes to the default settings

There are two methods to revert a subset of configuration changes to the default settings.

- Enter the **revert** command with the **path** parameter. For example, to revert all changes to the authentication methods configuration:

1. Enter the **revert** command with the **path** set to **auth method**:

---

```
(config)> revert auth method
(config)>
```

---

2. Save the configuration and apply the change:

---

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

---



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

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

- Move to the location in the configuration and enter the **revert** command without the **path** parameter. For example:
1. Change to the auth method node:

```
(config)> auth method
(config auth method)>
```

2. Enter the **revert** command:

```
(config auth method)> revert
(config auth method)>
```

3. Save the configuration and apply the change:

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

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

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

- You can also use a combination of both of these methods:
1. Change to the **auth** node:

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

2. Enter the **revert** command with the **path** set to **method**:

```
(config auth)> revert method
(config auth)>
```

3. Save the configuration and apply the change:

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

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

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

## Enter strings in configuration commands

For string parameters, if the string value contains a space, the value must be enclosed in quotation marks. For example, to assign a descriptive name for the device using the **system** command, enter:

```
(config)> system description "Digi IX14"
```

## Example: Create a new user by using the command line

In this example, you will use the IX14 command line to create a new user, provide a password for the user, and assign the user to authentication groups.

1. Log into the IX14 command line as a user with Admin access.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

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

---

3. At the config prompt, create a new user with the username **user1**:
  - Method one: Create a user at the root of the config prompt:

---

```
(config)> add auth user user1
(config auth user user1)>
```

---

- Method two: Create a user by moving through the configuration:
  - a. At the config prompt, enter **auth** to move to the **auth** node:

---

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

---

- b. Enter **user** to move to the **user** node:

---

```
(config auth)> user
(config auth user)>
```

---

- c. Create a new user with the username **user1**:

---

```
(config auth user)> add user1
(config auth user user1)>
```

---

4. Configure a password for the user:

---

```
(config auth user user1)> password pwd1
(config auth user user1)>
```

---

5. List available authentication groups:

---

```
(config auth user user1)> show .. .. group
```

```
admin
  acl
    admin
      enable true
    nagios
      enable false
    openvpn
      enable false
      no tunnels
```

---

---

```
portal
  enable false
  no portals
serial
  enable false
  no ports
shell
  enable false

serial
  acl
    admin
      enable true
    nagios
      enable false
    openvpn
      enable false
      no tunnels
    portal
      enable false
      no portals
    serial
      enable true
      ports
        0 port1
    shell
      enable false
(config auth user user1)>
```

---

6. Add the user to the admin group:

---

```
(config auth user user1)> add group end admin
(config auth user user1)>
```

---

7. Save the configuration and apply the change:

---

```
(config auth user user1)> save
Configuration saved.
>
```

---

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

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

## Command line reference

cp .....	293
ls .....	294
mkdir .....	295
modem at .....	296
modem at-interactive .....	297
modem pin change .....	298
modem pin disable .....	299
modem pin enable .....	300
modem pin status .....	301
modem pin unlock .....	302
modem puk status .....	303
modem puk unlock .....	304
modem reset .....	305
modem sim-slot .....	306
more .....	307
mv .....	308
ping .....	309
reboot .....	310
rm .....	311
scp .....	312
show arp .....	313
show cloud .....	314
show config .....	315
show dhcp-lease .....	316
show event .....	317
show ipsec .....	318
show log .....	319
show manufacture .....	320
show modem .....	321
show network .....	322
show openvpn client .....	323
show openvpn server .....	324
show route .....	325
show serial .....	326
show system .....	327
show version .....	328
show wifi ap .....	329
show wifi client .....	330
system backup .....	331
system factory-erase .....	332
system restore .....	333
system support-report .....	334
traceroute .....	335
update firmware .....	338

## **cp**

Copy a file or directory.

## **Syntax**

---

```
cp source destination [force]
```

---

## **Parameters**

### **source**

The path and filename of the source file to be copied.

Syntax: *string*

### **destination**

The destination path to copy the source file or directory to.

Syntax: *string*

### **force**

Do not ask to overwrite the destination file if it exists.

Default: false

## **ls**

List a directory.

## **Syntax**

---

```
ls path [show-hidden]
```

---

## **Parameters**

### **path**

The directory path to be listed.

Syntax: *string*

### **show-hidden**

Show hidden files and directories. Hidden filenames begin with '!'.  
Default: false

## **mkdir**

Create a directory. Parent directories are created as needed.

### **Syntax**

---

```
mkdir path
```

---

### **Parameters**

**path**

The path of the directory to be created.

Syntax: *string*

## **modem at**

Send an AT command to the modem and display the response.

### **Syntax**

---

```
modem at cmd [imei string] [name string]
```

---

### **Parameters**

#### **cmd**

The at command string to be sent to the modem.

Syntax: *string*

#### **imei**

The IMEI of the modem.

Syntax: [*string*]

#### **name**

The configured name of the modem.

Syntax: [*network-modem*]



## **modem at-interactive**

Start an AT command session on the modem's AT serial port.

### **Syntax**

---

```
modem at-interactive [imei string] [name string]
```

---

### **Parameters**

**imei**

The IMEI of the modem.

Syntax: [*string*]

**name**

The configured name of the modem.

Syntax: [*network-modem*]

## modem pin change

Change the SIM's PIN code. Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

### Syntax

---

```
modem pin change old-pin new-pin [imei string] [name string]
```

---

### Parameters

**old-pin**

The existing PIN code.

Syntax: *string*

**new-pin**

The new PIN code.

Syntax: *string*

**imei**

The IMEI of the modem.

Syntax: [*string*]

**name**

The configured name of the modem.

Syntax: [*network-modem*]

## modem pin disable

Disable the PIN lock on the SIM card that is active in the modem. Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

### Syntax

---

```
modem pin disable pin [imei string] [name string]
```

---

### Parameters

**pin**

The SIM's PIN code.

Syntax: *string*

**imei**

The IMEI of the modem.

Syntax: [*string*]

**name**

The configured name of the modem.

Syntax: [*network-modem*]

## modem pin enable

Enable the PIN lock on the SIM card that is active in the modem. The SIM card will need to be unlocked before each use. Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

## Syntax

---

```
modem pin enable PIN [imei STRING] [name STRING]
```

---

## Parameters

### pin

Syntax: *string*

### imei

Syntax: [*string*]

### name

Syntax: [*network-modem*]

## modem pin status

Print the PIN lock status and the number of PIN enable/disable/unlock attempts remaining. The SIM will be PUK locked when there are no remaining retries

## Syntax

---

```
modem pin status [name STRING] [imei STRING]
```

---

## Parameters

### name

Syntax: [*network-modem*]

### imei

Syntax: [*string*]

## modem pin unlock

Temporarily unlock the SIM card with a PIN code. Set the PIN field in the modem interface's configuration to unlock the SIM card automatically before use.



**WARNING!** Attempting to use an incorrect PIN code may PUK lock the SIM.

---

## Syntax

---

```
modem pin unlock PIN [imei STRING] [name STRING]
```

---

## Parameters

### pin

Syntax: *string*

### imei

Syntax: [*string*]

### name

Syntax: [*network-modem*]

## modem puk status

Print the PUK status and the number of PUK unlock attempts remaining.

### Syntax

---

```
modem puk status [name STRING] [imei STRING]
```

---

### Parameters

**name**

Syntax: [*network-modem*]

**imei**

Syntax: [*string*]

## modem puk unlock

Unlock the SIM with a PUK code from the SIM provider.

### Syntax

---

```
modem puk unlock PUK NEW-PIN [imei STRING] [name STRING]
```

---

### Parameters

**puk**

Syntax: *string*

**new-pin**

Syntax: *string*

**imei**

Syntax: [*string*]

**name**

Syntax: [*network-modem*]



## modem reset

Reset the modem hardware (reboot it). This can be useful if the modem has stopped responding to the network or is behaving inconsistently.

## Syntax

---

```
modem reset [name STRING] [imei STRING]
```

---

## Parameters

### name

Syntax: [*network-modem*]

### imei

Syntax: [*string*]

## modem sim-slot

Show or change the modem's active SIM slot. This applies only to modems with multiple SIM slots.

### Syntax

---

```
modem sim-slot slot (1|2|show) [imei STRING] [name STRING]
```

---

### Parameters

**slot**

Syntax: (**1|2|show**)

**imei**

Syntax: [*string*]

**name**

Syntax: [*network-modem*]

## **more**

View a file.

## **Syntax**

---

`more PATH`

---

## **Parameters**

### **path**

Syntax: *string*

## **mv**

Move a file or directory.

## **Syntax**

---

```
mv SOURCE DESTINATION [force]
```

---

## **Parameters**

### **source**

Syntax: *string*

### **destination**

The destination path to move the source file or directory to.

Syntax: *string*

### **force**

Do not ask to overwrite the destination file if it exists.

Syntax: *boolean*

Default: *false*

## ping

Ping a host using ICMP echo.

## Syntax

---

```
ping HOST [count INTEGER] [interface STRING] [ipv6] [size INTEGER]
```

---

## Parameters

### host

The name or address of the remote host to send ICMP ping requests to.

Syntax: {*hostname*|*IPv4\_address*|*IPv6\_address*}

### count

The number of ICMP ping requests to send before terminating.

Syntax: *integer*

Minimum: 1

Default: 100

### interface

The network interface to send ping packets from when the host is reachable over a default route. If not specified, the system's primary default route will be used.

Syntax: [*network-interface*]

### ipv6

Use the host's IPv6 address if a hostname is given as the 'host' argument.

Syntax: *boolean*

Default: false

### size

The number of bytes sent in the ICMP ping request.

Syntax: *integer*

Minimum: 0

Default: 56

## **reboot**

Reboot the system.

## **Syntax**

---

reboot

---

## **rm**

Remove a file or directory.

## **Syntax**

---

```
rm PATH [force]
```

---

## **Parameters**

### **path**

Syntax: *string*

### **force**

Force the file to be removed without asking.

Syntax: *boolean*

Default: false

## scp

Copy a file or directory over SSH.

## Syntax

---

```
scp LOCAL REMOTE HOST USER [port INTEGER] to (remote|local)
```

---

## Parameters

### local

The file to copy to or from on the local device.

Syntax: *string*

### remote

The file to copy to or from on the remote host.

Syntax: *string*

### host

Syntax: {*hostname|IPv4\_address|IPv6\_address*}

### user

The username to use when connecting to the remote host.

Syntax: *string*

### port

The SSH port to use to connect to the remote host.

Syntax: *integer*

Minimum: 1

Maximum: 65535

Default: 22

### to

Copy the file from the local device to the remote host, or from the remote host to the local device.

Syntax: (**remote|local**)



## **show arp**

Show ARP tables, if no IP version is specified IPv4 & IPV6 will be displayed.

## **Syntax**

---

```
show arp [ipv4] [ipv6] [verbose]
```

---

## **Parameters**

### **ipv4**

Display IPv4 routes. If no IP version is specified IPv4 & IPV6 will be displayed

Syntax: *boolean*

Default: false

### **ipv6**

Display IPv6 routes. If no IP version is specified IPv4 & IPV6 will be displayed

Syntax: *boolean*

Default: false

### **verbose**

Display more information (less concise, more detail).

Syntax: *boolean*

Default: false

## **show cloud**

Show Digi Remote Manager status and statistics.

### **Syntax**

---

```
show cloud
```

---

## **show config**

Show changes made to default configuration.

### **Syntax**

---

```
show config
```

---

## show dhcp-lease

Show DHCP leases.

### Syntax

---

```
show dhcp-lease [all] [verbose]
```

---

### Parameters

#### **all**

Show all leases (active and inactive (not in etc/config/dhcp.\*lease)).

Syntax: *boolean*

Default: false

#### **verbose**

Display more information (less concise, more detail).

Syntax: *boolean*

Default: false

## show event

Show event list (high level).

## Syntax

---

```
show event [table (status|error|info)] [number INTEGER]
```

---

## Parameters

### **table**

Type of event log to be displayed (status, error, info).

Syntax: [**(status|error|info)**]

### **number**

Number of lines to retrieve from log.

Syntax: *integer*

Minimum: 1

Default: 20

## show ipsec

Show IPsec status & statistics.

## Syntax

---

```
show ipsec [tunnel STRING] [all]
```

---

## Parameters

### **tunnel**

Display more details and config data for a specific IPsec tunnel.

Syntax: [*vpn-ipsec-tunnel*]

### **all**

Display all tunnel including disabled tunnel.

Syntax: *boolean*

Default: false

show log [*number* INTEGER] [*filter* (**critical|warning|debug|info**)]

## show log

Show system log

### Syntax

---

```
show log [numberINTEGER] [filter(critical|warning|debug|info)]
```

---

### Parameters

#### **number**

Number of lines to retrieve from log.

Syntax: *integer*

Minimum: 1

Default: 20

#### **filter**

Filters for type of log message displayed (critical, warning, info, debug). Because filtering the entire log file can be time-consuming, this parameter filters based on the number of messages retrieved based on the **number** parameter, rather than the complete log file. To retrieve more messages of the filtered type, increase the number of messages retrieved by using the **number** parameter.

Syntax: [(critical|warning|debug|info)]

## **show manufacture**

Show manufacturer information.

### **Syntax**

---

```
show manufacture
```

---



## show modem

Show modem status & statistics.

## Syntax

---

```
show modem [name STRING] [imei STRING] [verbose]
```

---

## Parameters

### **name**

Syntax: [*network-modem*]

### **imei**

Syntax: [*string*]

### **verbose**

Display more information (less concise, more detail).

Syntax: *boolean*

Default: false

## show network

Show network interface status & statistics.

### Syntax

---

```
show network [interface STRING] [all] [verbose]
```

---

### Parameters

#### **interface**

Display more details and config data for a specific network interface.

Syntax: [*network-interface*]

#### **all**

Display all interfaces including disabled interfaces.

Syntax: *boolean*

Default: false

#### **verbose**

Display more information (less concise, more detail).

Syntax: *boolean*

Default: false

## show openvpn client

Show OpenVPN client status & statistics.

### Syntax

---

```
show openvpn client [name STRING] [all]
```

---

### Parameters

**name**

Display more details and config data for a specific OpenVPN client.

Syntax: [*vpn-openvpn-client*]

**all**

Display all clients including disabled clients.

Syntax: *boolean*

Default: false

## show openvpn server

Show OpenVPN server status & statistics.

### Syntax

---

```
show openvpn server [name STRING] [all]
```

---

### Parameters

#### **name**

Display more details and config data for a specific OpenVPN server.

Syntax: [*vpn-openvpn-server*]

#### **all**

Display all servers including disabled servers.

Syntax: *boolean*

Default: false

## show route

Show IP routing information.

## Syntax

---

```
show route [ipv4] [ipv6] [verbose]
```

---

## Parameters

### ipv4

Display IPv4 routes.

Syntax: *boolean*

Default: false

### ipv6

Display IPv6 routes.

Syntax: *boolean*

Default: false

### verbose

Display more information (less concise, more detail).

Syntax: *boolean*

Default: false

## **show serial**

Show serial status & statistics.

### **Syntax**

---

```
show serial [port STRING]
```

---

### **Parameters**

**port**

Display more details and config data for a specific serial port.

Syntax: [*serial*]

## **show system**

Show system status & statistics.

### **Syntax**

---

```
show system [verbose]
```

---

### **Parameters**

**verbose**

Display more information (disk usage, etc).

Syntax: *boolean*

Default: false

## **show version**

Show firmware version.

### **Syntax**

---

```
show version [verbose]
```

---

### **Parameters**

#### **verbose**

Display more information (build date).

Syntax: *boolean*

Default: false



## show wifi ap

Display details for Wi-Fi access points.

### Syntax

---

```
show wifi ap [name STRING] [all]
```

---

### Parameters

#### **name**

Display more details for a specific Wi-Fi access point.

Syntax: [*network-wireless-ap*]

#### **all**

Display all Wi-Fi access points including disabled Wi-Fi access points.

Syntax: *boolean*

Default: false

## show wifi client

Display details for Wi-Fi client mode connections.

### Syntax

---

```
show wifi client [name STRING] [all]
```

---

### Parameters

#### **name**

Display more details for a specific Wi-Fi client mode connection.

Syntax: [*network-wireless-client*]

#### **all**

Display all Wi-Fi clients including disabled Wi-Fi client mode connections.

Syntax: *boolean*

Default: false

## system backup

Save the device's configuration to a file. Archives are full backups including generated SSH keys and dynamic DHCP lease information. Command backups are a list of CLI commands required to build the device's configuration.

## Syntax

---

```
system backup PATH [passphrase STRING] [type (cli-config|archive)]
```

---

## Parameters

### path

Syntax: *string*

### passphrase

Dependency: type=archive

Syntax: [*string*]

### type

The type of backup file to create. Archives are full backups including generated SSH keys and dynamic DHCP lease information. CLI configuration backups are a list of CLI commands used to build the device's configuration.

Syntax: **(cli-config|archive)**

Default: archive

## **system factory-erase**

Erase the device to restore to factory defaults. All configuration and automatically generated keys will be erased.

### **Syntax**

---

```
system factory-erase
```

---

## **system restore**

Restore the device's configuration from a backup archive or CLI commands file.

### **Syntax**

---

```
system restore PATH [passphrase STRING]
```

---

### **Parameters**

**path**

Syntax: *string*

**passphrase**

Syntax: [*string*]

## **system support-report**

Save a support report to a file and include with support requests.

### **Syntax**

---

```
system support-report PATH
```

---

### **Parameters**

**path**

Syntax: *string*

## traceroute

Print the route packets trace to network host.

## Syntax

```
traceroute HOST [bypass] [debug] [dontfragment] [first_ttl INTEGER] [gateway  
STRING] [icmp] [interface STRING] [ipchecksums] [max_ttl INTEGER] [nomap]  
[nqueries INTEGER] [packetlen INTEGER] [pausesecs INTEGER] [port  
INTEGER] [src_addr STRING] [tos INTEGER] [verbose] [waittime INTEGER]
```

## Parameters

### host

The host that we wish to trace the route packets for.

Syntax: {hostname|IPv4\_address|IPv6\_address}

### bypass

Bypass the normal routing tables and send directly to a host on an attached network.

Syntax: *boolean*

Default: false

### debug

Enable socket level debugging.

Syntax: *boolean*

Default: false

### dontfragment

Do not fragment probe packets.

Syntax: *boolean*

Default: false

### first\_ttl

Specifies with what TTL to start.

Syntax: *integer*

Minimum: 1

Default: 1

### gateway

Tells traceroute to add an IP source routing option to the outgoing packet that tells the network to route the packet through the specified gateway

Syntax: [{IPv4\_address|IPv6\_address}]

**icmp**

Use ICMP ECHO for probes.

Syntax: *boolean*

Default: false

**interface**

Specifies the interface through which traceroute should send packets. By default, the interface is selected according to the routing table.

Syntax: [*network-interface*]

**ipchecksums**

Calculate ip checksums.

Syntax: *boolean*

Default: false

**max\_ttl**

Specifies the maximum number of hops (max time-to-live value) traceroute will probe.

Syntax: *integer*

Minimum: 1

Default: 30

**nomap**

Do not try to map IP addresses to host names when displaying them.

Syntax: *boolean*

Default: false

**nqueries**

Sets the number of probe packets per hop. A value of -1 indicates

Syntax: *integer*

Minimum: 1

Default: 3

**packetlen**

Total size of the probing packet. Default 60 bytes for IPv4 and 80 for Ipv6. A value of -1 specifies that the default value will be used.

Syntax: *integer*

Minimum: -1

Default: -1

**pausesecs**

Minimal time interval between probes

Syntax: *integer*

Minimum: 0

Default: 0

**port**

Specifies the destination port base traceroute will use (the destination port number will be incremented by each probe). A value of -1 specifies that no specific port will be used.



Syntax: *integer*

Minimum: -1

Default: -1

**src\_addr**

Chooses an alternative source address. Note that you must select the address of one of the interfaces. By default, the address of the outgoing interface is used.

Syntax: [{IPv4\_address|IPv6\_address}]

**tos**

For IPv4, set the Type of Service (TOS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput). Note that in order to use some TOS precedence values, you have to be super user. For IPv6, set the Traffic Control value. A value of -1 specifies that no value will be used.

Syntax: *integer*

Minimum: -1

Default: -1

**verbose**

Verbose output.

Syntax: *boolean*

Default: false

**waittime**

Determines how long to wait for a response to a probe.

Syntax: *integer*

Minimum: 1

Default: 5

## **update firmware**

Update device firmware

### **Syntax**

---

```
update firmware FILE
```

---

### **Parameters**

**file**

Syntax: *string*