

IW Monitor User Guide, Release 2.1.0

First Published: 2024-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

PREFACE

Preface v

Cisco Industrial Wireless monitor v

Related Documentation v

Communications, Services, and Additional Information v

CHAPTER 1

IW Monitor overview 1

IW Monitor interfaces 1

CHAPTER 2

Supported Network Devices and Firmware for IW Monitor 3

Supported network devices and firmware for IW Monitor 3

CHAPTER 3

Install IW Monitor Docker on Host 5

Host and network requirements 5

Docker images on IW Monitor hosts 6

Download and install Docker on the IW Monitor host 7

Download the IW Monitor image 8

Load the IW Monitor image file to the IW Monitor server 8

Run the Docker container for the first time 9

Log in to the IW Monitor for the first time 10

CHAPTER 4

Add devices to the IW Monitor 19

Add devices to the IW Monitor 19

CHAPTER 5

Manage Sections 21

Create a new section 21
Edit a section 22
Delete a section 22

CHAPTER 6 Manage Devices 23
Edit device configuration parameters 23
Detach devices 24

CHAPTER 7 Monitor Network Performance 25
Dashboard network statistics 25
Use the Table View to monitor devices 27
Uplink and downlink information 30
Parameters and descriptions for uplink and downlink information 31
View device statistics in real time 32
View devices from Topology 35
Enable MPO processing to check in topology 40
View network event logs 41
Export a network event log 43

CHAPTER 8 Configure IW Monitor Database Settings 45
Configure database storage, back up, and clean IW Monitor statistics data 45

CHAPTER 9 Configure IW Monitor Statistical Settings 47
Change the interval at which statistical data is logged 47
Configure event log settings 48
Set performance thresholds 50
Set performance thresholds for each section 51

CHAPTER 10 Manage User Accounts 53
Update a user account 53
View, add, and delete users 53

CHAPTER 11 Update IW Monitor 55

Update the IW Monitor 55

CHAPTER 12 Uninstall IW Monitor 57

Uninstall IW Monitor 57



Preface

The Cisco Industrial Wireless (IW) Monitor guide provides instructions on using the IW Monitor platform for monitoring and managing industrial wireless networks.

This guide includes:

- Cisco Industrial Wireless monitor, on page v
- Related Documentation, on page v
- Communications, Services, and Additional Information, on page v

Cisco Industrial Wireless monitor

The Cisco Industrial Wireless (IW) Monitor is an on-premises tool that manages and displays real-time data and situational alerts from all Ultra-Reliable Wireless Backhaul (URWB) devices and Cisco Wireless devices with URWB enabled.

It supports the monitoring and maintenance of multiple types of URWB and WiFi-integrated wireless devices, and provides management capabilities for both IW and Fluidmesh (end-of-life notification announced) devices.

Related Documentation

For more details about Regulatory Compliance and Safety Information, see Regulatory Compliance and Safety Information.

Communications, Services, and Additional Information

This topic provides links and information for Cisco communications, services, support, and feedback resources.

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.

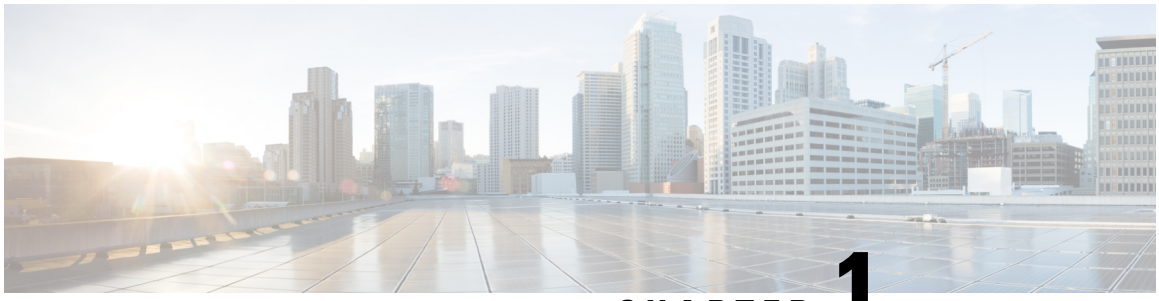
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system. This system maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

IW Monitor overview

- IW Monitor interfaces, on page 1

IW Monitor interfaces

- IW Service is a cloud-based interface for online and offline configuration of IW devices.
- IW Monitor is a diagnostic and analysis interface based on a virtual image. You install it in Docker format to monitor Fluidmesh and Industrial Wireless devices.

Functionalities of IW Monitor application

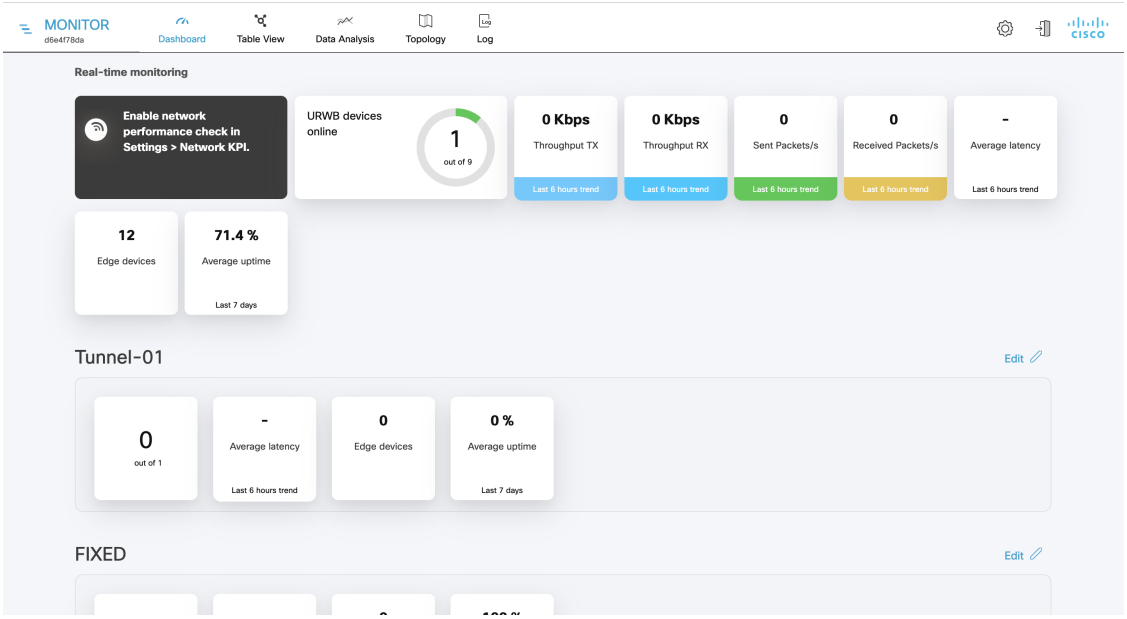
The IW Monitor application provides these functionalities:

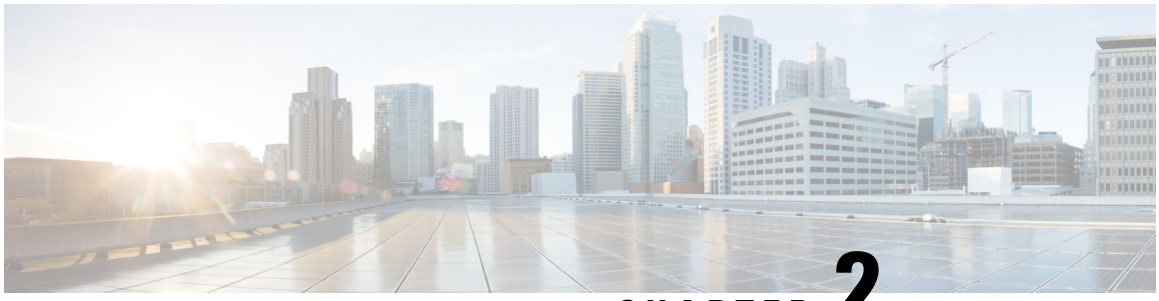
- Monitor the real time condition of networks.
- Generate statistics from network history.
- Verify if the device configuration settings are optimal for current network conditions.
- Detect network-related events for diagnostics and generate alerts if network-related faults arise.
- Analyze network data to increase system uptime and maintain optimal network performance.

To configure the IW devices, you can use any of these methods:

1. To add and configure devices using cloud-based IW Service, see IoT OD IW documentation.
2. To manually configure devices by using the device's built-in Configurator interface or through CLI, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide or Cisco IEC6400 Edge Compute Appliance Installation and Configuration Guide.

Figure 1: IW Monitor Application Overview





CHAPTER 2

Supported Network Devices and Firmware for IW Monitor

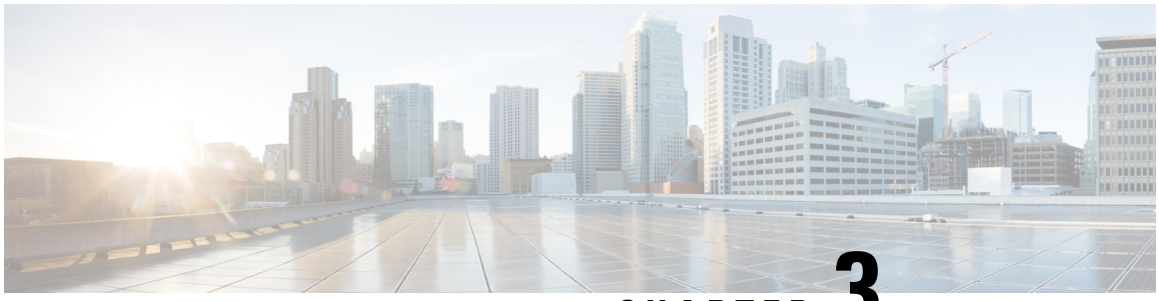
• Supported network devices and firmware for IW Monitor, on page 3

Supported network devices and firmware for IW Monitor

This reference lists the supported device models and their recommended firmware versions for IW Monitor.

Table 1: Supported Network Devices and Recommended Firmware Versions for URWB devices

Device Model	Recommended Software Version
Catalyst IW9167	17.12.1 (17.12.1.5) or later
Catalyst IW9165	17.12.1 (17.12.1.5) or later
FM 3500 and FM 4500	9.4 or later
FM 3200 and FM 4200	8.5 or later
FM 1200 VOLO	7.9 or later
FM PONTE	1.2.7 or later
FM1000 and FM10000	1.3.0 or later
FM10000 GEN2	2.3.0 or later
IEC-6400	1.1.0.7 or later



CHAPTER 3

Install IW Monitor Docker on Host

- Host and network requirements, on page 5
- Docker images on IW Monitor hosts, on page 6
- Download and install Docker on the IW Monitor host, on page 7
- Download the IW Monitor image, on page 8
- Load the IW Monitor image file to the IW Monitor server, on page 8
- Run the Docker container for the first time, on page 9
- Log in to the IW Monitor for the first time, on page 10

Host and network requirements

If an internet connection is not available, the Docker application and IW Monitor image file can be installed manually. See Installing and Running Docker Container.

Note A high-speed, high-bandwidth internet connection is recommended for installing Docker and the IW Monitor image file.

Verify that your system meets all required host specifications to run the Docker container.

Table 2: Host Requirements by Operating System

Requirement	Windows 7 or later	Mac OS X 10.9.x or later	Linux (32-bit or 64-bit)
Operating System	Windows 7 or later	Mac OS X 10.9.x or later	Linux (32-bit or 64-bit): • Ubuntu 14.04 or later • Debian 9 or later • OpenSuSE 14.2 or later • Fedora Linux 19 or later
Docker Application	Yes	Yes	Yes

Base System	Virtual machine or bare metal	Virtual machine or bare metal	Virtual machine or bare metal
Processor	Intel Core i7 or Xeon (any frequency and mandatory minimum of four cores)	Intel Core i7 or Xeon (any frequency and mandatory minimum of four cores)	Intel Core i7 or Xeon (any frequency and mandatory minimum of four cores)
RAM	16 GB minimum	16 GB minimum	16 GB minimum
Hard Disk	100 GB minimum* 1 TB or greater recommended	100 GB minimum* 1 TB or greater recommended	100 GB minimum* 1 TB or greater recommended
High speed connection to local networks and devices	Preferred	Preferred	Preferred
Screen Resolution	1024 x 768 pixel minimum	1024 x 768 pixel minimum	1024 x 768 pixel minimum

Note Use a hard disk with at least 100 GB capacity. For hard disks with less than 100 GB capacity, adjust the maximum statistics storage capacity according to the guidance in Configure database storage, back up, and clean IW Monitor statistics data, on page 45.

Use the latest version of a supported web browser to access IW Monitor.

Table 3: Supported Web Browsers

Browser	Supported Version
Mozilla Firefox	Latest
Microsoft Internet Explorer	Latest
Microsoft Edge	Latest
Google Chrome	Latest
Apple Safari	Latest

Note If needed, upgrade your browser to the latest version.

Docker images on IW Monitor hosts

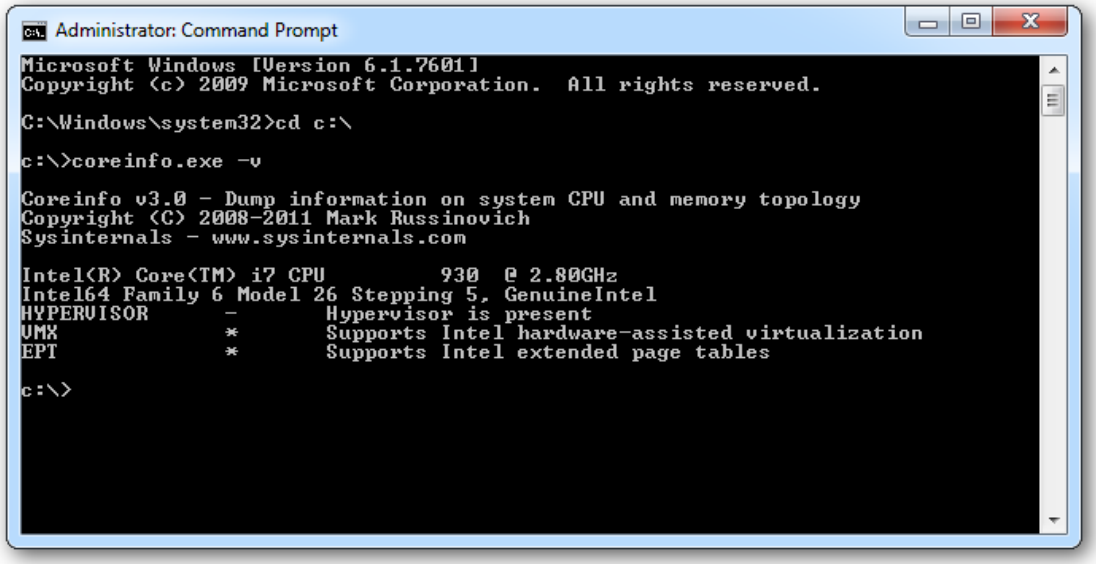
Docker is a platform that enables running containerized applications by packaging code and its dependencies into Docker images, which become containers at runtime on the Docker engine.

Prerequisites and SLAT Verification

Before installing Docker, ensure that the host CPU supports virtualization and second-level address translation (SLAT). Intel's version of SLAT is called EPT (Extended page tables).

To verify that the host's processor meets the requirement:

1. Go to Microsoft Sysinternals, and download the `Coreinfo` package.
2. Unzip the downloaded program folder to the root of the host's `C:\ drive`.
3. Open the command prompt using administrator privileges.
4. Enter the command: `coreinfo.exe -v`
   - If an Intel CPU supports SLAT, an asterisk (*) is shown in the EPT row (see this example):



   - If your CPU does not support SLAT, a dash (-) is shown in the EPT row.

Alternatively, check SLAT support using Intel Product Specification:

1. Go to Intel Product Specification.
2. Select the respective CPU, and check its specifications.

Download and install Docker on the IW Monitor host

Before you begin

Before you install and run the docker container on a Microsoft operating system, verify that Microsoft virtual machine capability (Hyper V) is running. Also, VMware is supported.

Do not install the Docker container on your local computer. Install Docker only on the host assigned to run IW Monitor. See the hardware specification requirements for the host in Host and network requirements, on page 5.

Note Oracle VM VirtualBox is not supported.

Procedure

To install Docker, you must open these protocols and ports in the firewall to ensure MONITOR works correctly.

- UDP from MONITOR to devices. Port 6600 is used for devices association.
- UDP from MONITOR to devices. Port 6610 is used for latency and jitter computation.
- Secure WebSocket from devices to MONITOR. The customer configures the port with the docker run command, usually 8443.

Step 1 Go to the Docker application download page.
Step 2 Download the correct Docker application package.
Step 3 Install the Docker application on the IW Monitor host.

Download the IW Monitor image

Procedure

Step 1 Go to software downloads.
Step 2 Download the IW Monitor image file (`iw-monitor-dockerv3. x.x.tar`).

Load the IW Monitor image file to the IW Monitor server

Procedure

Step 1 Open a command-line window.
Step 2 Enter the command: `docker load -i iw-monitor-dockerv3. x.x.tar`
Step 3 Enter the command to check if the IW Monitor image file is loaded: `docker images`

A list of Docker image files currently installed on the IW Monitor host appears.

Step 4 To get the image ID value for the IW Monitor image file:
a) Open a command-line window.

b) Enter the command: `docker images`

A list of the Docker image files currently installed on the IW Monitor host are shown.

c) Search the REPOSITORY column of the Docker image file list for the **iw-monitor image** file.

Note the IMAGE ID value of the IW Monitor Docker image.

Run the Docker container for the first time

Procedure

Step 1 Open a command-line window.

Step 2 Enter the command: `docker run -d --name iw_monitor -p 8443:8443 --restart always X` where X is the IMAGE ID value of the IW Monitor Docker image.

Note
By default, the IW Monitor in the Docker container uses these port numbers:

- Port 8443 (https with SSL)
- Encryption via HTTPS is required

Note
If you fail to use the default host port numbers due to security policy settings or the needed host port is assigned to another service, modify the `docker run` command to include an unused host port.

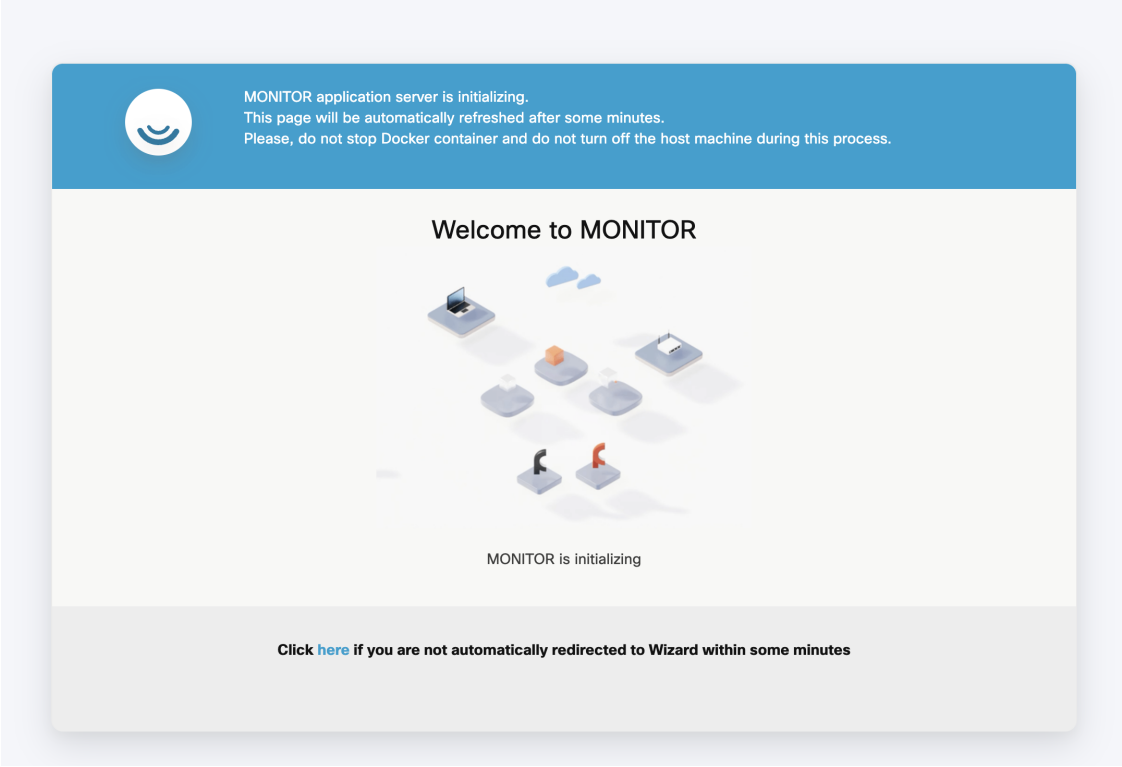
Note
For example, a run command that specifies port 3000: `docker run -d --name iw_monitor -p 3000:8443 iw_monitor`

Step 3 If you have modified the Docker run command to specify a different host port, then you must specify the port number used by IW Monitor. For more information, see Add devices to the IW Monitor, on page 19.

Step 4 Open the web browser.

Step 5 Navigate to the URL https://X:Y where X is the IP address of the IW Monitor host, and Y is the host port number.

The IW Monitor Docker container launches successfully, and the welcome page appears as shown:

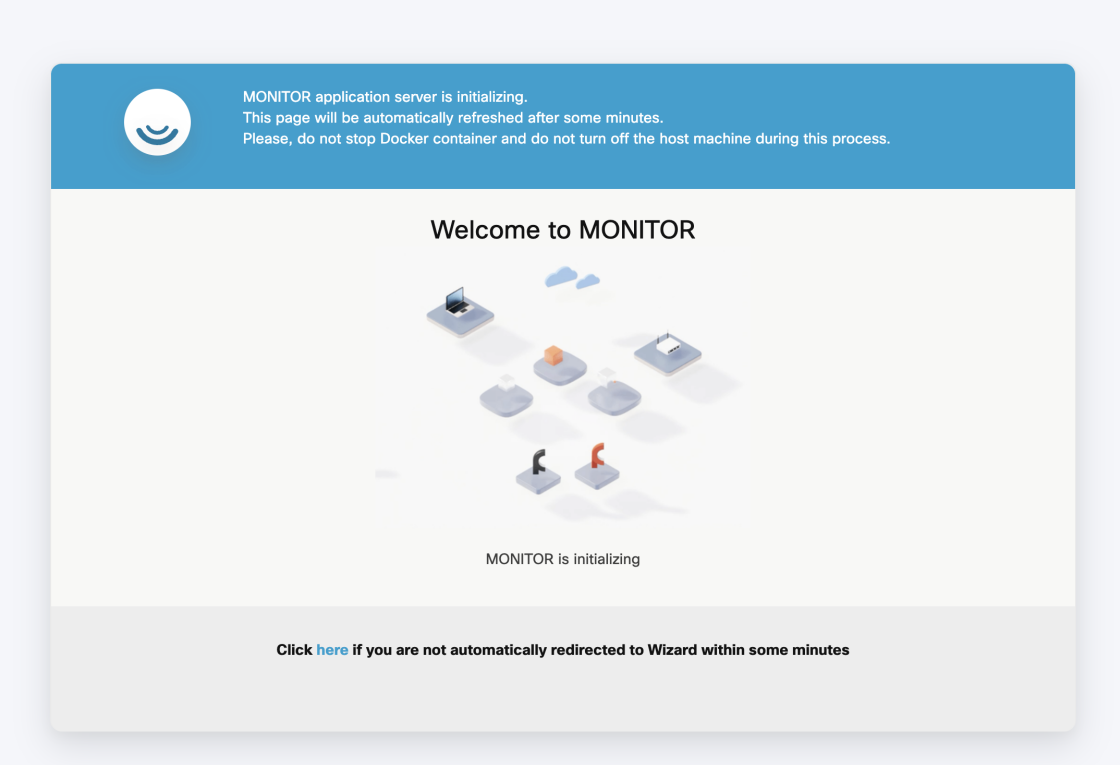


Log in to the IW Monitor for the first time

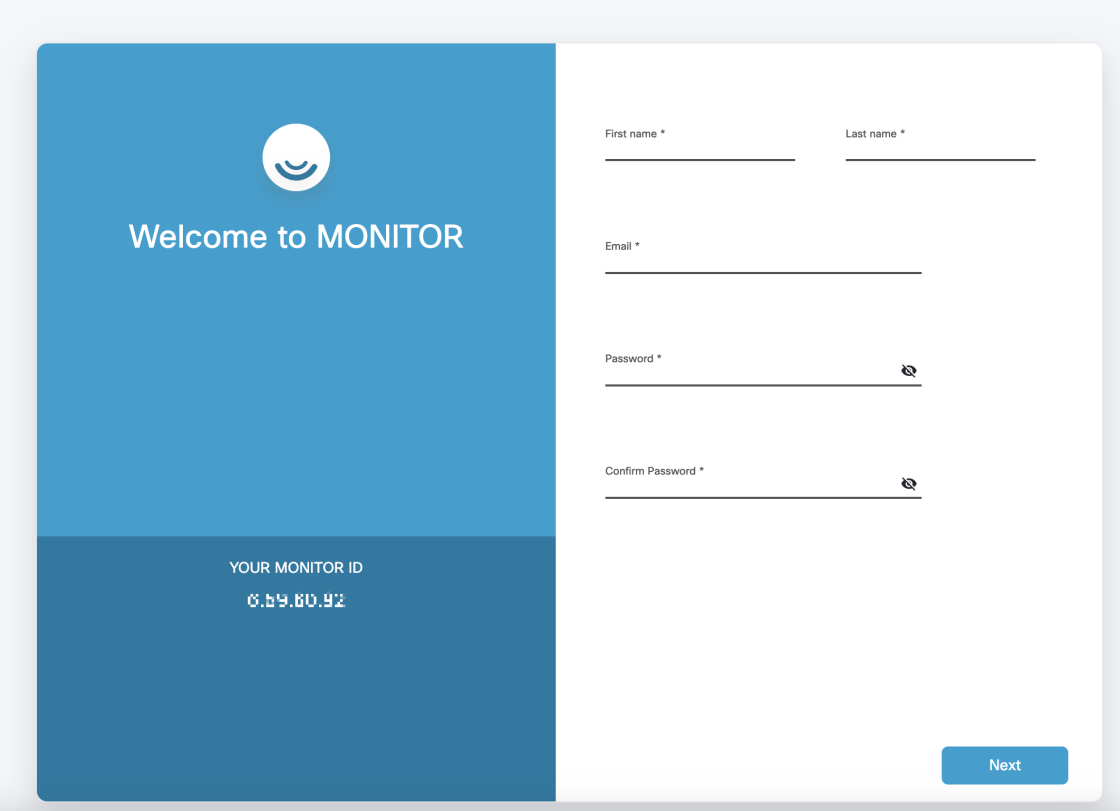
Procedure

Step 1 In the web browser, enter the URL with IP address and port number of the computer on which the IW Monitor image file: **https://[IP address]:[host port number]**

If you are running IW Monitor for the first time, this initialization page appears:

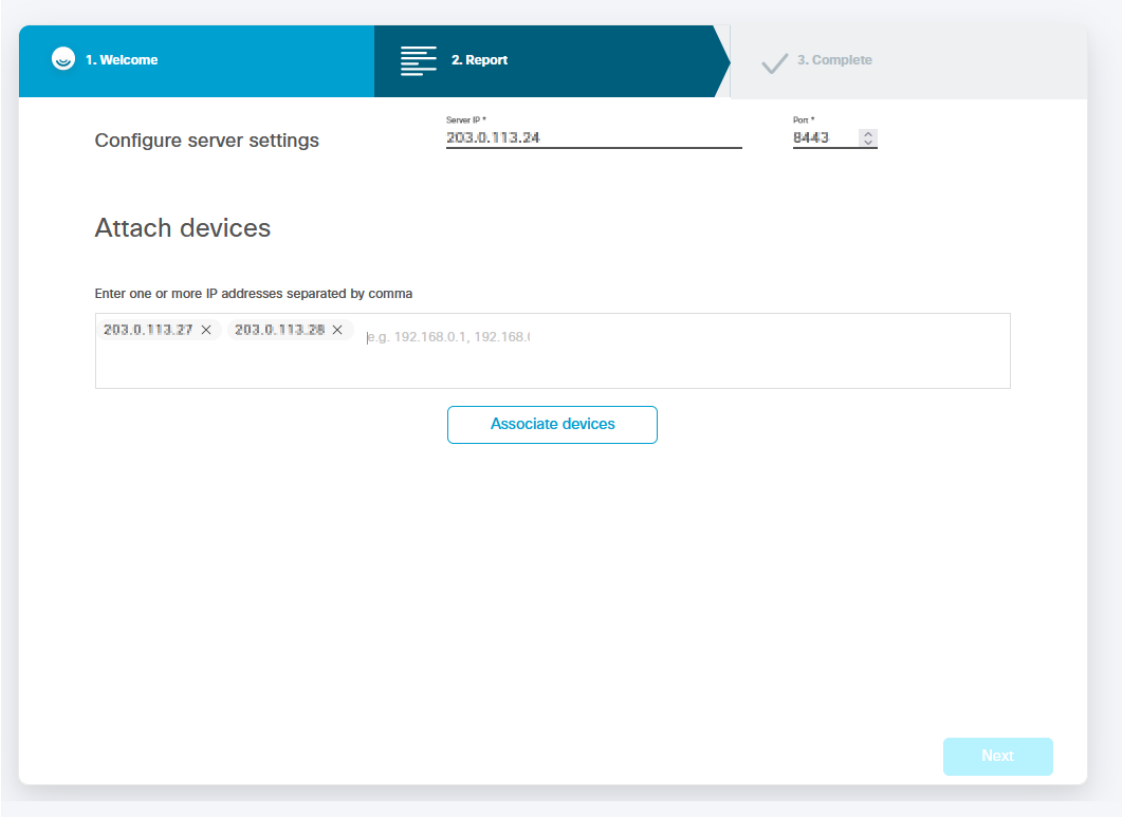


Step 2 Enter your first name, last name, email address, and login password in the respective fields. Then click **Next**.



The **Add new device** screen appears.

Step 3 Optional) If required, enter the IP address of the IW Monitor server in the **Server IP** field and the port number in the **Port** field.

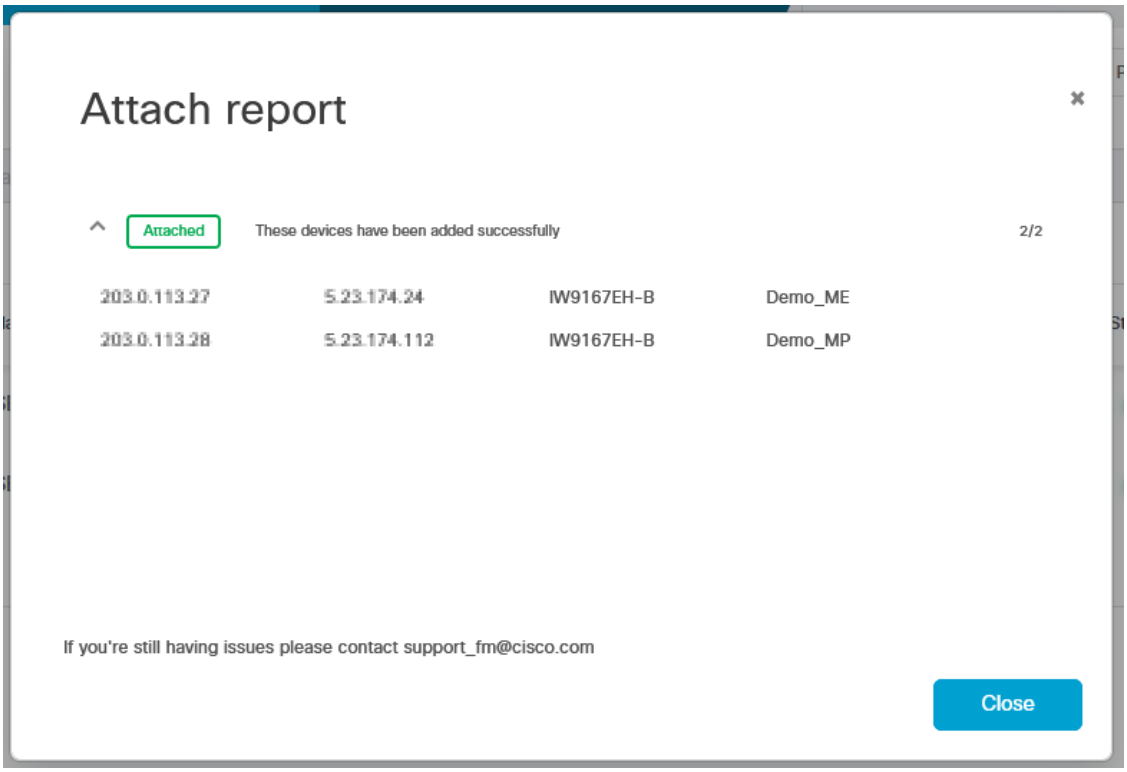


Step 4 Enter the IP addresses of all devices you want to monitor in the **IP addresses** field.

Note
Press **Enter** after entering each IP address, including the last IP address.

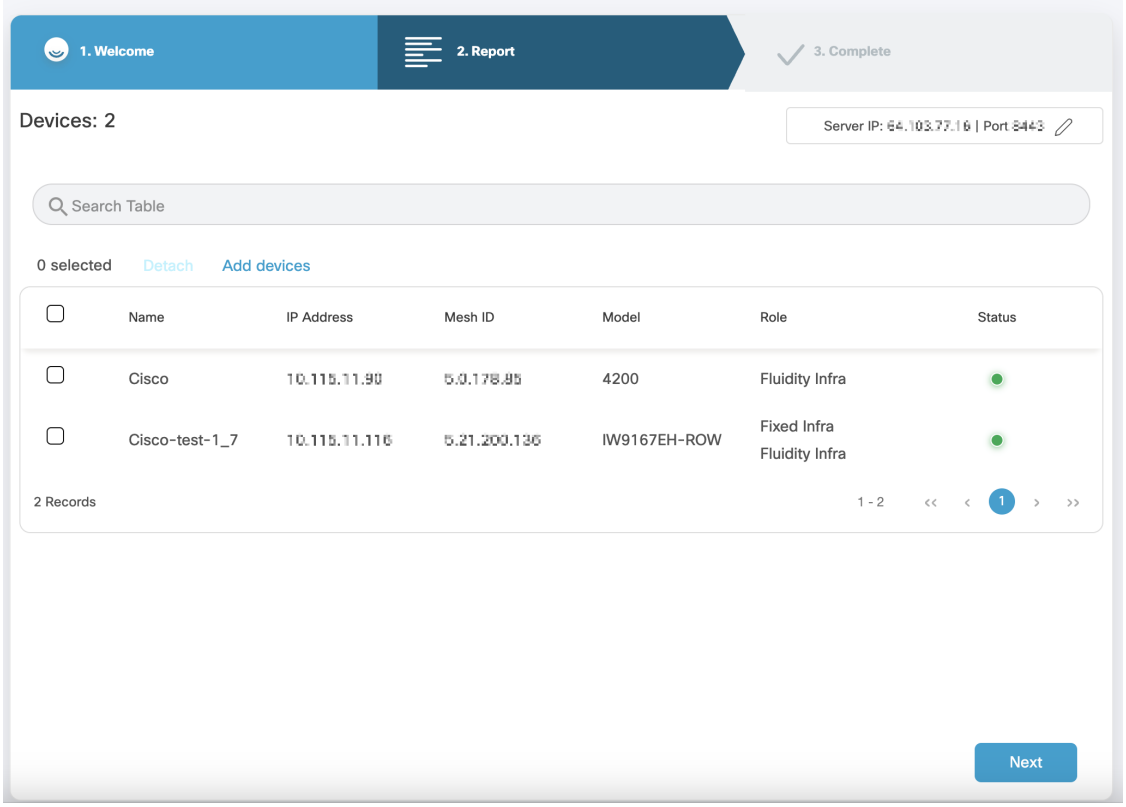
Step 5 Click **Associate devices**.

A confirmation screen appears showing that the devices are associated with the IW Monitor interface.



Step 6 Click **Close**.

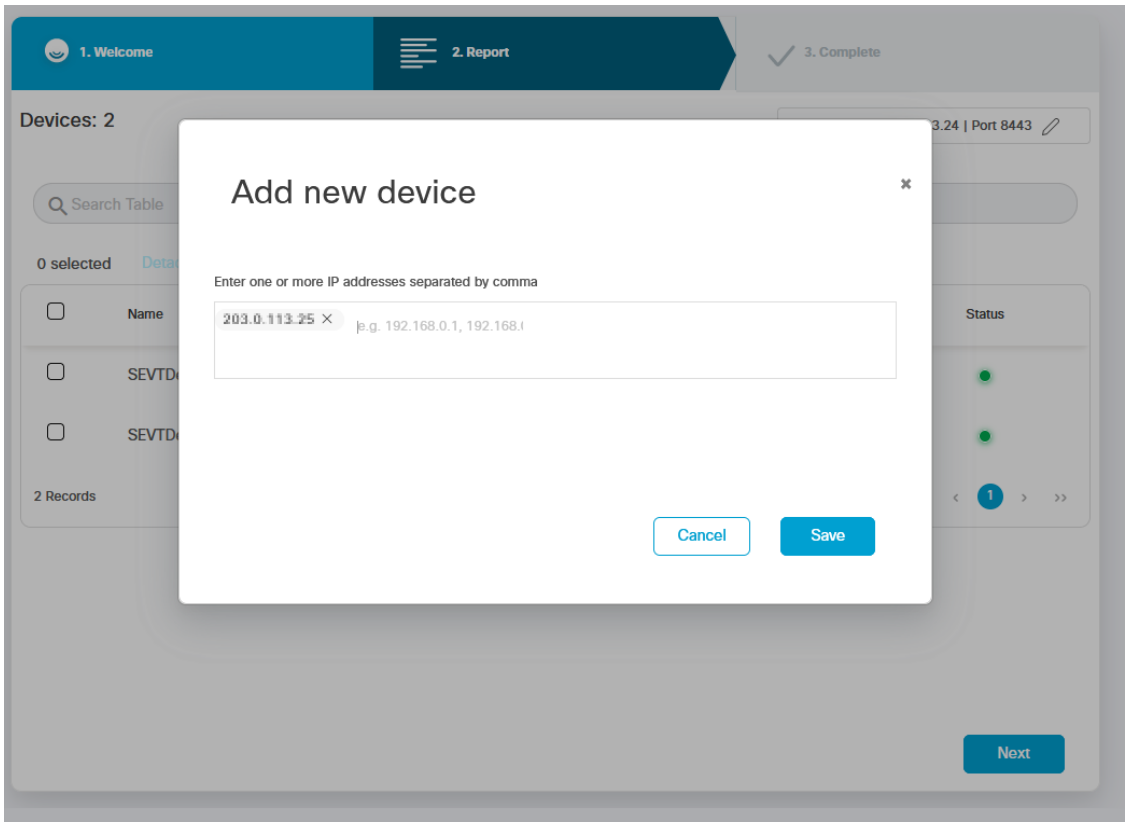
The list of devices associated with the IW Monitor interface is displayed as shown:



Step 7 Ensure that all devices are listed on the screen. If a device is missing, use these steps to add the device:

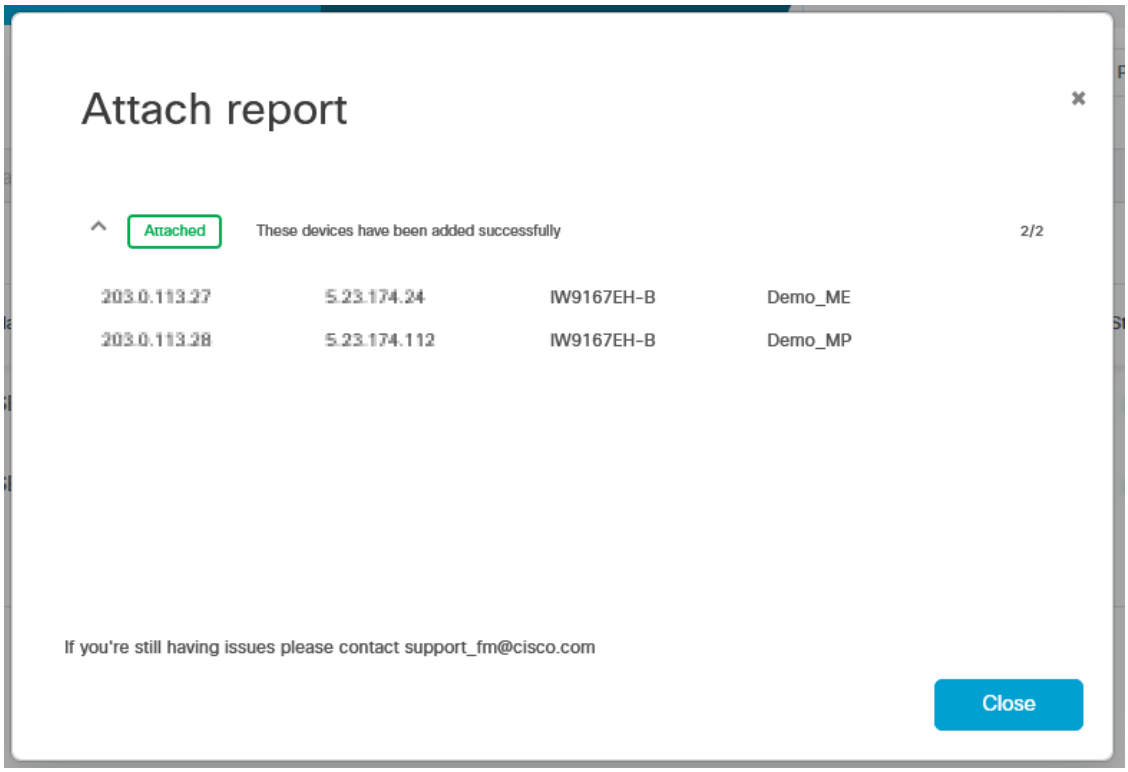
a) Click **Add Device**.

The **Add new device** screen appears.



b) Enter the IP address of the devices in the **IP addresses** field.
c) Click **Save**.

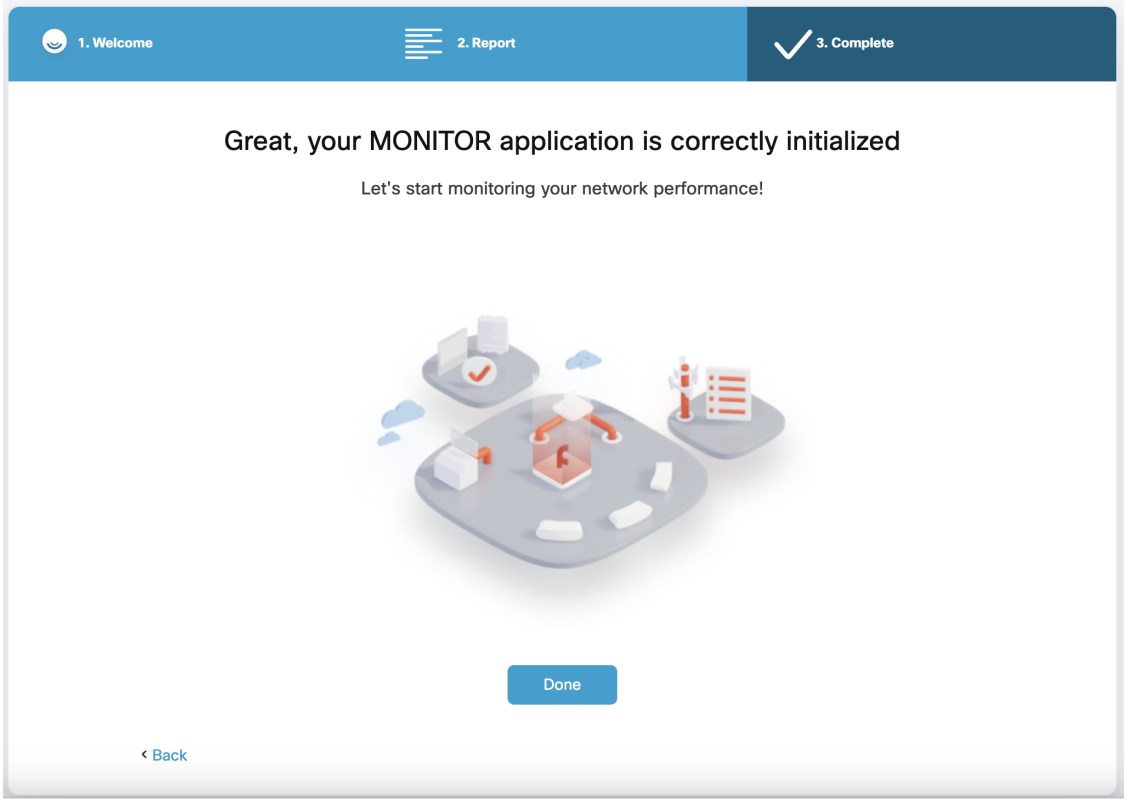
A confirmation screen appears showing that the devices are associated with the IW Monitor interface.



d) Click **Close**.

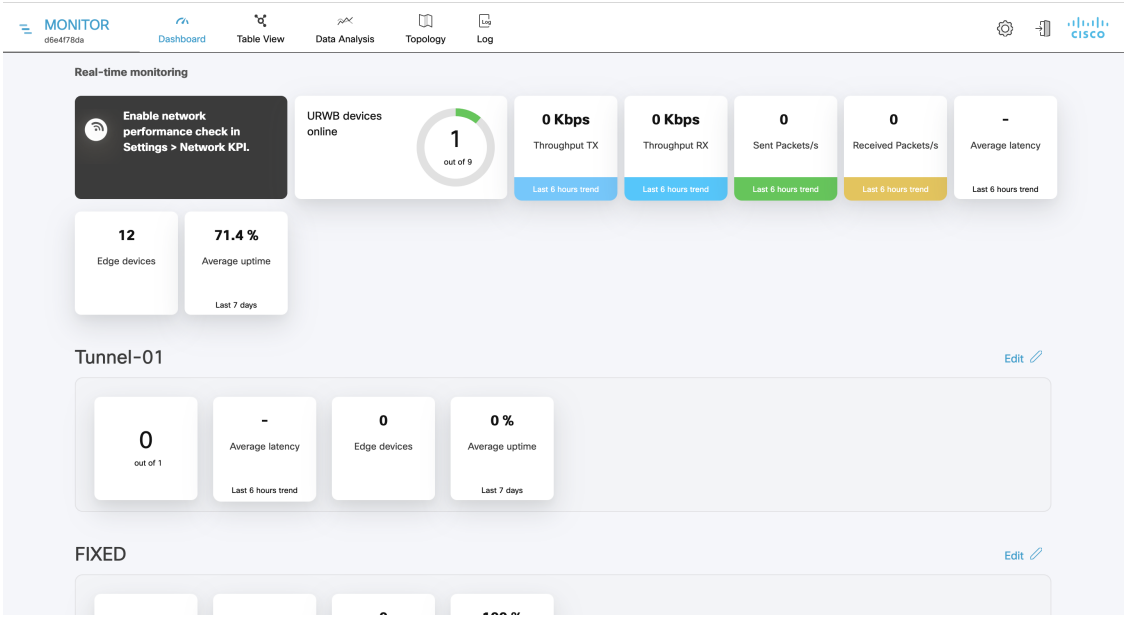
Step 8 Click **Next**.

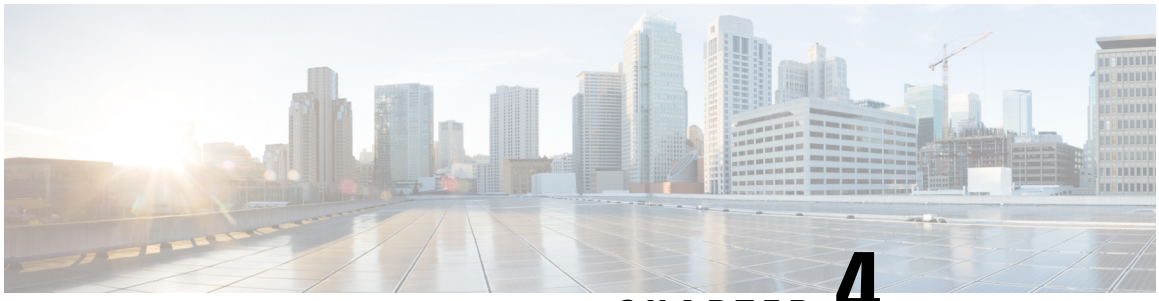
The IW Monitor analyzes the network. After the analysis is complete, the **Complete** screen appears.



Step 9 Click **Done** to complete the network setup.

The IW Monitor dashboard appears:





CHAPTER 4

Add devices to the IW Monitor

• Add devices to the IW Monitor, on page 19

Add devices to the IW Monitor

Procedure

Step 1 Click the **(settings icon)** > **Devices** from the left pane.

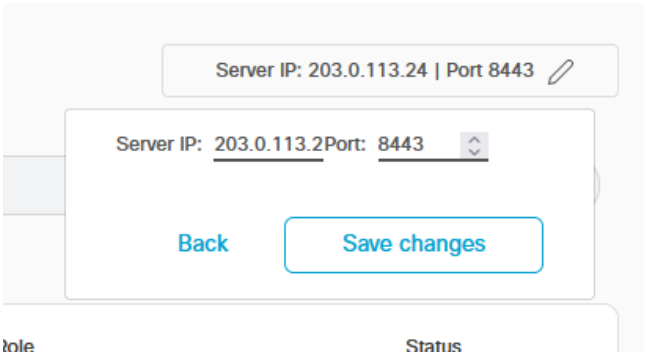
A table appears with the list of configured devices.

Step 2 Click the (edit icon) and configure the IP address of the main network server.

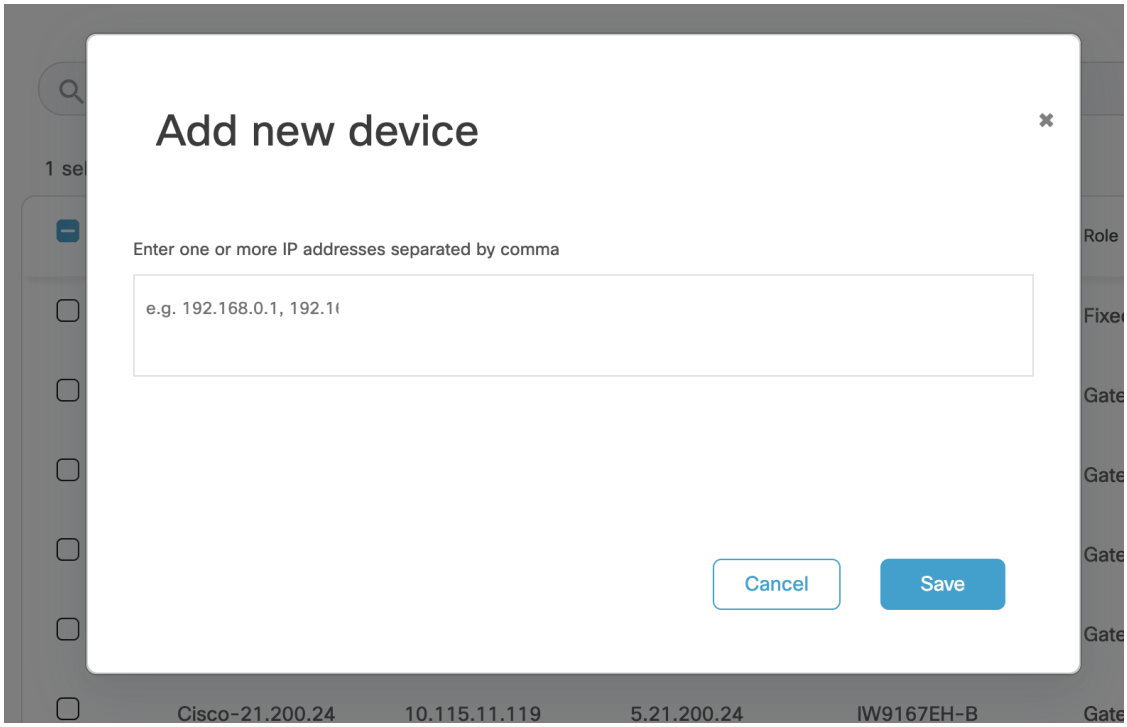
a) (Optional) Add the server IP address in the **Server IP** field.
b) If the IW Monitor host is configured to use HTTPS (secure socket layer) data transfer, enable the SSL.
c) Enter the Docker container port number and click **Save changes**.

For example:

- **-p 8443:8443** maps to Port 8443
- **-p 443:8443** maps to Port 443
- **-p 3000:8443** maps to Port 3000



Step 3 Click **Add Devices** to add the IP addresses of the devices.



Step 4 Add the IP addresses of the devices, separated by a comma and a space.

You can use an Excel file to enter all IP addresses in a column, then copy and paste them into the application.

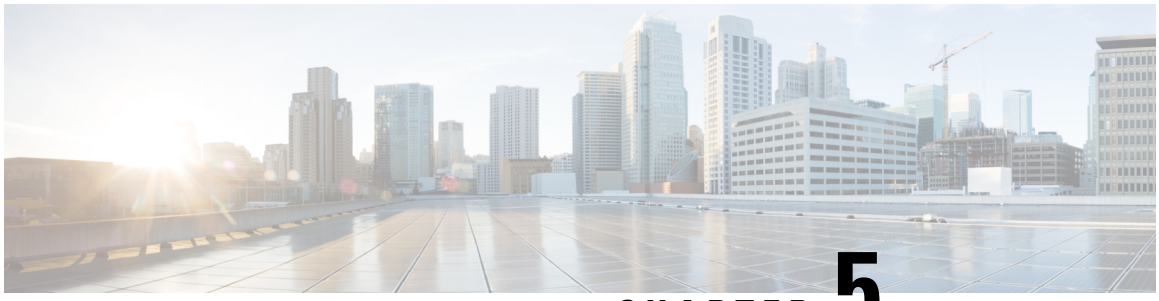
For example: 192.168.0.1, 192.168.0.2, 192.168.0.3

Note
If any IP address is not reachable, an error shows that the devices failed to attach. Verify the IP address or check if any firewall is blocking access.

If you try to add an associated device, an error message appears stating that the device could not be added.

Step 5 Click **Save**.

The newly added devices appear in the table.



CHAPTER 5

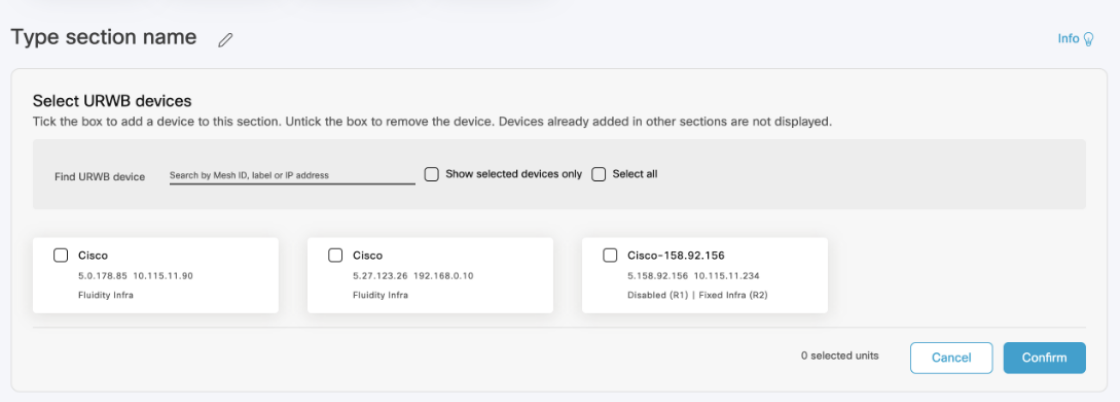
Manage Sections

- Create a new section, on page 21
- Edit a section, on page 22
- Delete a section, on page 22

Create a new section

Procedure

Step 1 Click **+ ADD SECTION**.



Step 2 Click to enter a section name.

Step 3 Use the search box to find the URWB devices by mesh ID, label (assigned device name), or the device IP address.

Step 4 Select the **Show selected devices only** checkbox to view uncategorized devices.

Uncategorized devices are not yet assigned to any section. They are displayed separately.

Note
Devices that are already added in other sections will not appear here.



Select **Select all** checkbox to select every device in the list, or select devices individually.

Step 5 Click **Confirm** to add the selected devices to the new section.

Edit a section

Procedure

Step 1 Click the to select the section you want to edit.

Step 2 Update the required fields, such as the section name or the list of devices.

Step 3 Save your changes by clicking **Confirm**.

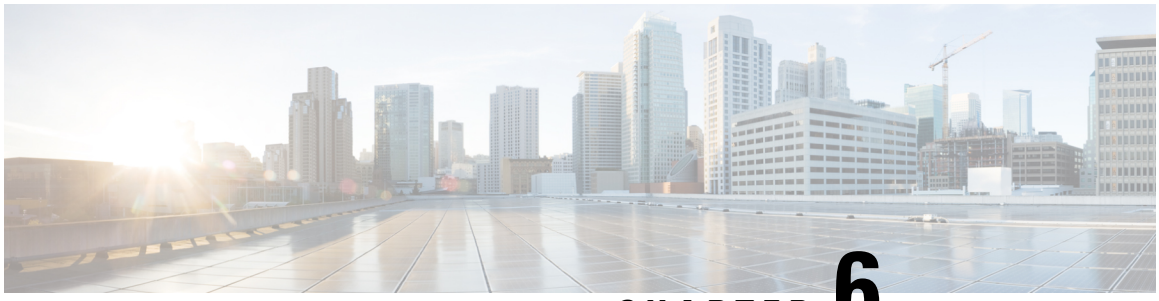
Delete a section

Procedure

Step 1 Click the to select the section you want to delete.

Step 2 Click Delete Section of the section.

Step 3 Click **Delete** to remove the selected section from your workspace.



CHAPTER 6

Manage Devices

- Edit device configuration parameters, on page 23
- Detach devices, on page 24

Edit device configuration parameters

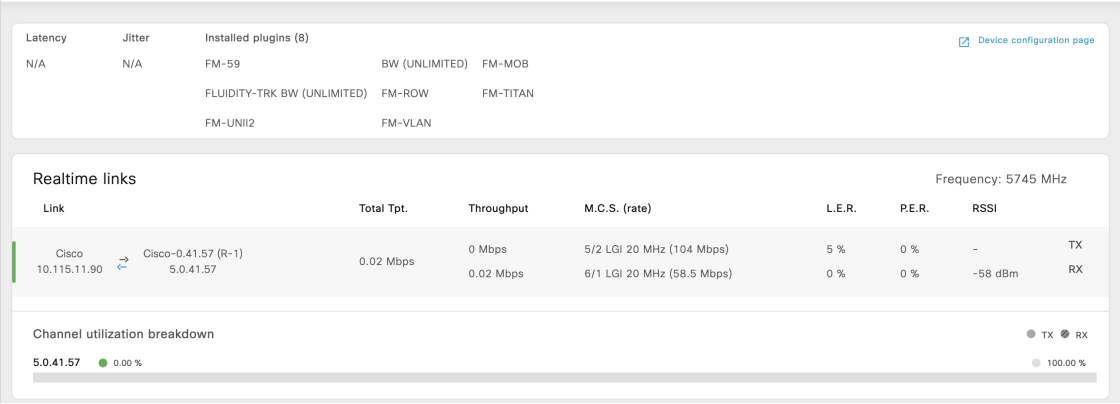
Before you begin

Ensure you have valid login credentials for the device configurator.

Procedure

Step 1 Click **Table View** to open the device table to view all devices.

Step 2 Select the device by clicking ••• next to the device whose configuration you want to edit.



Step 3 Click **Device configuration page**.

You are taken to a separate device configurator login page. Log in to the configurator interface by entering your credentials.

Step 4 Edit the configuration parameters as required.

For more instructions on editing device configuration parameters using the Configurator interface, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide.

Detach devices

Procedure

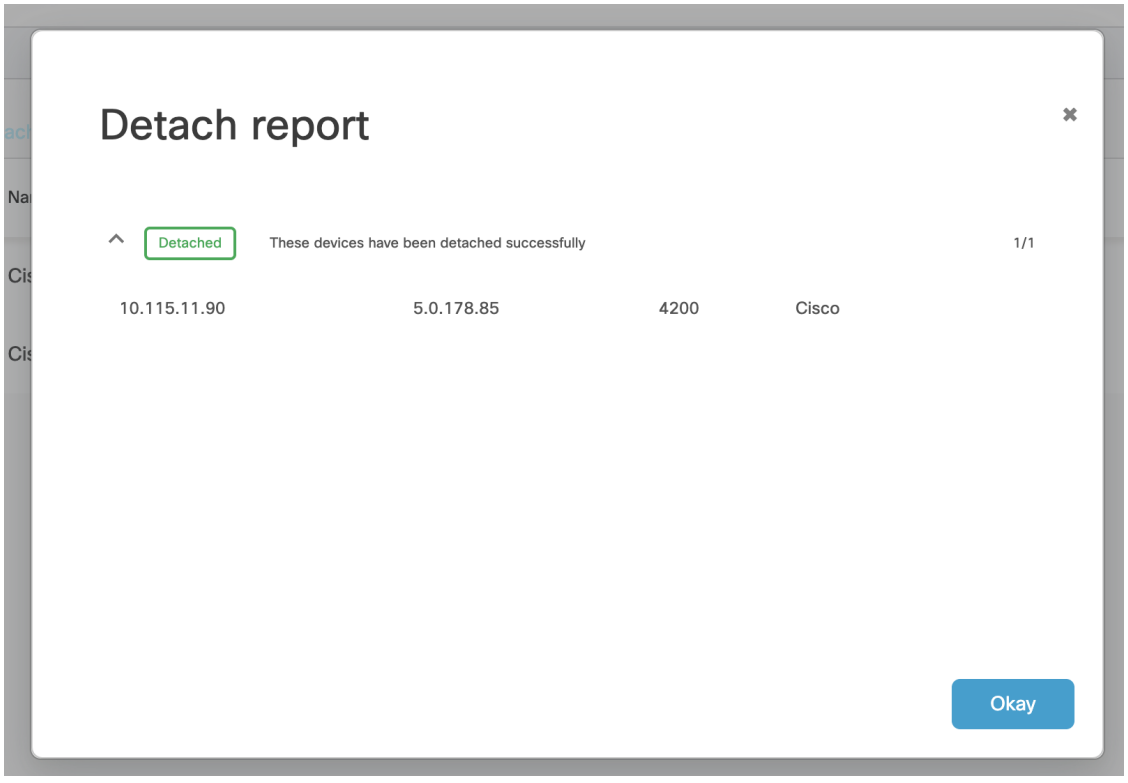
Step 1 To detach a device, navigate to **settings iconDevices**.

A table displays the devices attached to IW Monitor.

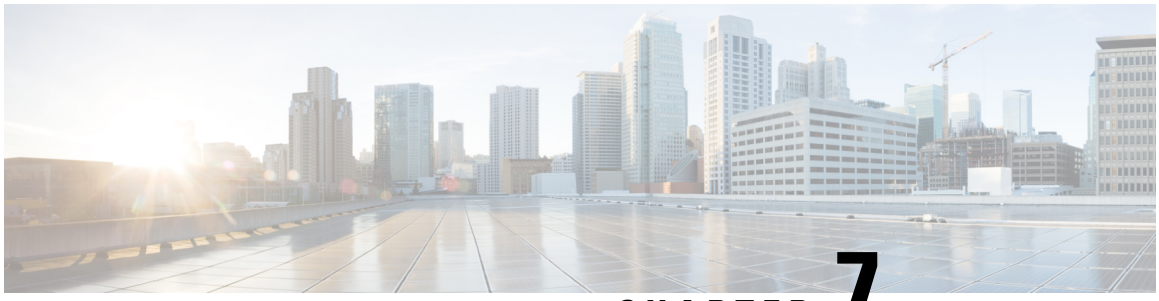
Step 2 Search for devices using the mesh ID number, assigned device name, device model, or the device's IP address. Select the devices you want to detach.

Step 3 Click **Detach**.

The system detaches the selected devices and displays a confirmation pop-up.



Step 4 To remove a device from the IW Monitor using the Configurator interface's detach function, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide.



CHAPTER 7

Monitor Network Performance

- Dashboard network statistics, on page 25
- Use the Table View to monitor devices, on page 27
- Uplink and downlink information, on page 30
- View device statistics in real time, on page 32
- View devices from Topology, on page 35
- View network event logs, on page 41

Dashboard network statistics

The network statistics view is a real-time monitoring interface that displays the performance and operating parameters of devices across different network sections.

- Shows the number of devices currently connected to IW Monitor, compared to the total associated devices.
- Displays device latency (Average latency) values across the network or section for the last six hours.
- It provides aggregate throughput for TX and RX, the number of sent and received packets per second, the current number of edge devices, and average uptime values for each network section.

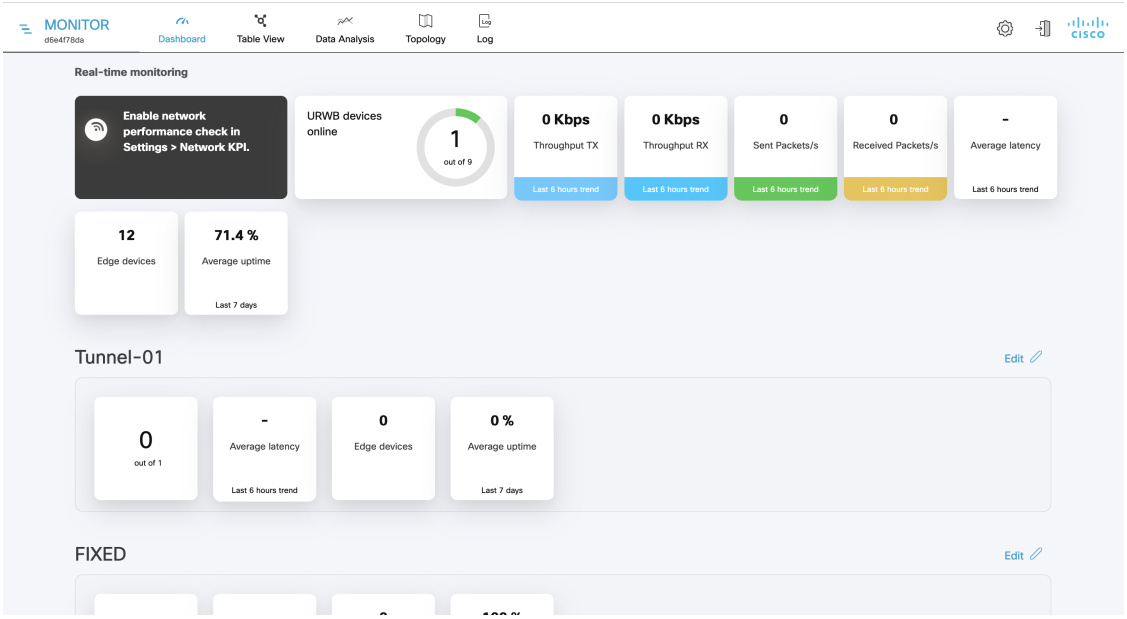
Network Statistics Reference Information

The network statistics view provides detailed information about the performance and health of each network section and its devices.

- Number of devices currently connected to IW Monitor, in relation to the total number of devices associated with IW Monitor.
- Device latency (**Average latency**) values across the network or section during the last six hours.
- Aggregate network throughput transmitted (**Throughput TX**) by all devices in the network during the last six hours.
- Aggregate network throughput received (**Throughput RX**) by all devices in the network during the last six hours.
- Aggregate number of data packets sent (**Sent Packets/s**) by all devices in the network during the last six hours.

- Aggregate number of data packets received (**Received Packets/s**) by all devices in the network during the last six hours.
- Current number of edge devices (**Edge devices**).
- Average network or section uptime value (**Average uptime**). The average uptime value is the combined percentage of time for each network device or section connected to the IW Monitor in the last seven days.

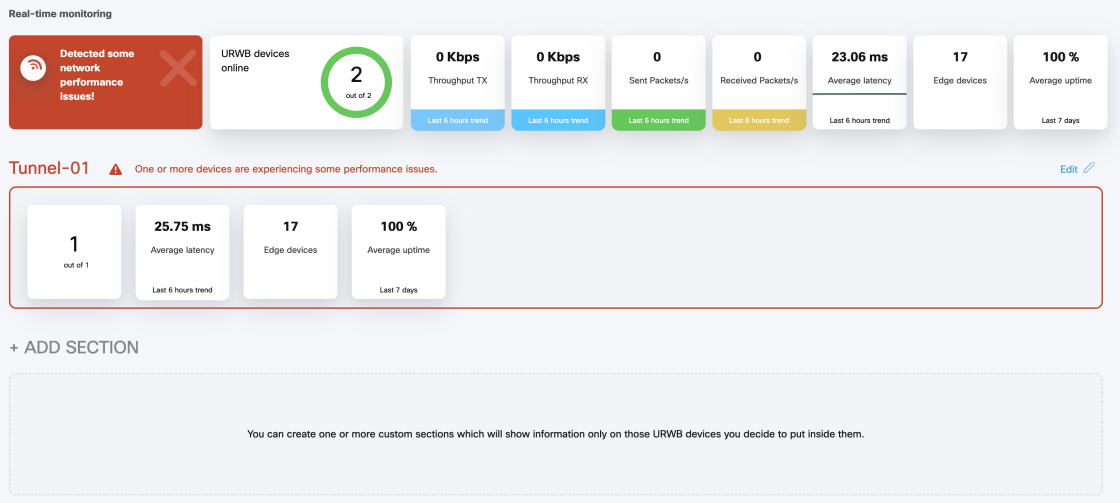
Figure 2: Network Statistics Overview



When a performance-related fault occurs, a thin red box appears around the affected section to indicate the need for immediate investigation.

The **+ ADD SECTION** button at the bottom allows you to customize the section with the device information you want to monitor. To add a new section to an existing network, see Create a new section, on page 21.

Figure 3: Section Customization Example



Use the Table View to monitor devices

The Table View is a feature in IW Monitor that displays all devices in a tabular format, showing their status, attributes, and section assignments.

- Devices without an assigned section appear under **Uncategorized**.
- Devices assigned to specific network sections appear in their respective sections.
- Each device entry displays parameters including Status, Mode, Label, IP Address, Mesh ID, Firmware Version, Role, Frequency, TX Power, Max TX Power, and Channel width.

Device Table View Reference Information

The Table View provides a comprehensive overview of all devices with their current status and key operational parameters. Users can search for devices, filter by status, and review detailed attribute descriptions.

- Users can search for devices by Mesh ID, assigned device name, or IP address.
- Users can filter devices by status: **Critical**, **Warning**, or **Disconnected**.
- Device attributes and their descriptions are provided in the table.

Table 4: Device Attribute Descriptions

Parameter	Description

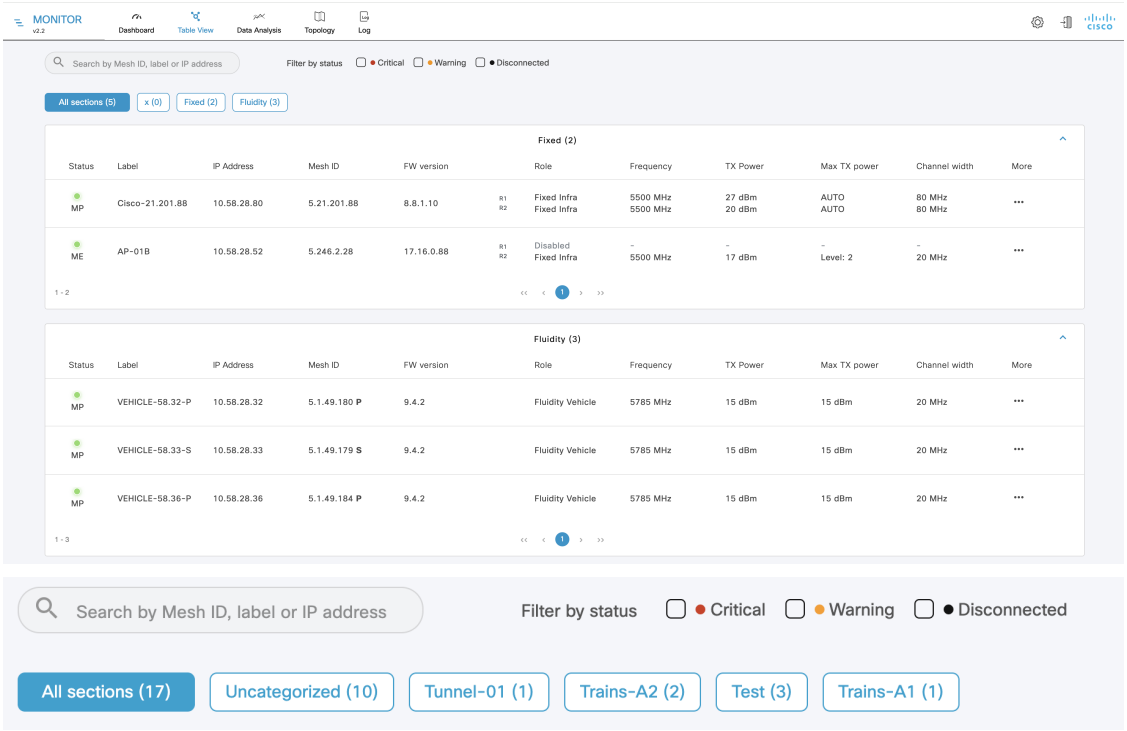
Status	Icon colors represent device status:
	• **Green**: Device is online and connected to an IW Monitor with all performance levels in an acceptable range.
	• **Gray**: Device is disconnected from IW Monitor.
	• **Orange**: Device is online and connected to the IW Monitor but has one or more problems causing lower-than-optimal performance.
	• **Red**: Device is online and connected to IW Monitor but has one or more problems causing unacceptably low performance.
	  • High packet error rate
	  • High link error rate
	  • Low received signal strength
	  • High traffic latency
	
	Icon designations:
	• **ME**: Device is configured as a mesh end.
	• **MP**: Device is configured as a mesh point.
	• **BR**: Device is configured as a wireless bridge device.
	• **PONTE**: Applicable only for FM PONTE devices.
	• **GGW**: Gateway is configured as a Global Gateway.

Label	User-assigned device name. **Note** You cannot change the device name using IW Monitor. Use IoT OD IW service, the device offline web interface (Configurator), or the device's command-line interface (CLI) to change the device's name.
IP Address	Shows the IP address of the device.

Parameter	Description
Mesh ID	Unique, factory-set mesh identification number (for example, 5.a.b.c). • If set as the primary vehicle-mounted network device, letter **P** is shown next to the Mesh ID. • If set as a secondary device, letter **S** is shown next to the Mesh ID.
FW Version	Firmware release number.
Role	Role designations for URWB-configured device status include: • **Fixed Infra**: Device is part of a fixed-based infrastructure. • **Fluidity Vehicle**: Device is part of a Fluidity network, installed in a moving vehicle. • **Fluidity Infra**: Device is part of a Fluidity network, installed as part of a fixed infrastructure. **Note** For dual-radio devices, the **Role** parameter is specified for each radio interface. If the radio interface is disabled, the interface status shows **Disabled**.
Frequency	Current operating frequency of the device. **Note** For dual-radio devices, the **Frequency** parameter is shown for each radio interface.
TX Power	Current value in dBm of the radio device's transmission power. **Note** For dual-radio devices, the **TX Power** parameter is shown for each radio interface.
Channel width	Operating channel width of the radio device. **Note** For dual-radio devices, the **Channel width** parameter is shown for each radio interface.

Note Use the filter options to quickly identify devices with critical, warning, or disconnected status for efficient monitoring and troubleshooting.

Figure 4: Table View and Filter Visuals



Using Table View to Monitor Devices

For example, to view all devices with a critical status, select the **Critical** filter. The Table View will display only those devices whose thresholds are beyond the upper threshold limit. Similarly, use the search bar to locate a device by its Mesh ID or IP address.

Uplink and downlink information

- Uplink and downlink information provides real-time metrics and status for a selected device in Table View.
- Key parameters include latency, jitter, installed plugins, license, link endpoints, role, throughput, modulation and coding schema, error rates, signal strength, channel utilization, and attached devices.
- Each parameter offers specific insights into device performance and connectivity.

Parameters and descriptions for uplink and downlink information

To view the uplink and downlink information for a device in the Table View, click the (…) icon next to the device to display the detailed information.

Table 5: Uplink and Downlink Parameters

Parameter	Description
Latency	Shows the current network latency (the delay period between data transmission by the IW Monitor host and reception of a reply by a radio device). The latency value is calculated as half of the round-trip time of the relevant packets.
Jitter	Shows the current amount of network jitter (the deviation from the true periodicity of periodic data signals in relation to a reference clock signal).
Installed plugins	Shows list of the software plug-ins currently installed on the device. This item is only applicable for legacy Fluidmesh products.
License	Shows the device's license level. This information applies only for Catalyst IW9165, IW9167, and IEC-6400 gateway. The **License** level can be **Essential** , **Advantage** , or **Premier** .
Link	Shows the two endpoints of the wireless link.
Role	Role designations are: • **Fixed Infrastructure** : The radio unit is part of a wired LAN based infrastructure. • **Fluidity Infrastructure** : The radio unit is part of a Fluidity network, and installed in a moving vehicle. • **Fluidity Vehicle** : The radio unit is part of a Fluidity network, and installed as part of a fixed infrastructure.
Total Throughput (Total Tpt.)	Shows the combined throughput rate per second for the uplink and downlink.
Throughput	Upper value shows the throughput rate per second for the downlink. The lower value shows the throughput rate per second for the uplink.
M.C.S. (rate)	Shows the modulation and coding schema used by the relevant uplink or downlink.

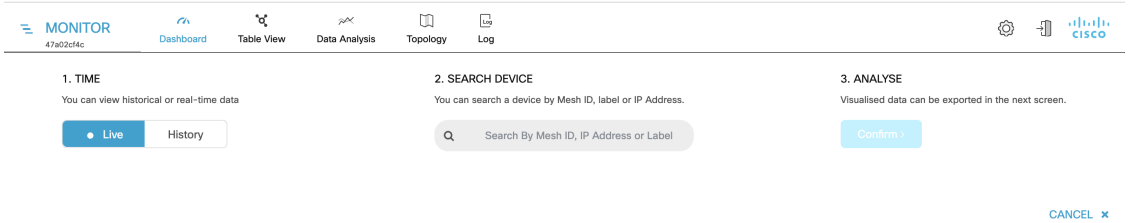
Parameter	Description
L.E.R.	Shows the link error rate for the relevant uplink or downlink.
P.E.R.	Shows the packet error rate for the relevant uplink or downlink.
RSSI	Shows the received signal strength indication for the relevant uplink or downlink.
Channel utilization breakdown	• The total width of the bar represents the total bandwidth of the channel carrying the uplink and downlink. • The solid portion represents the portion of bandwidth currently being used to transmit data. • The striped portion represents the portion of bandwidth currently being used to receive data. • The gray portion represents the portion of bandwidth that is currently not utilized. • Numerical percentage readouts are provided for transmission, reception, and non-utilization.
Attached devices	This is a list of devices that are part of the section.

View device statistics in real time

IW Monitor provides network statistics that allow you to view the network-related performance of any device in the current network. You can view device statistics as events occur in real time. You can also view a performance graph showing the device's historical performance over time.

Procedure

Step 1 Click **Data Analysis**.



Step 2 In the **TIME** field, you can switch between real-time and historical data for analysis.

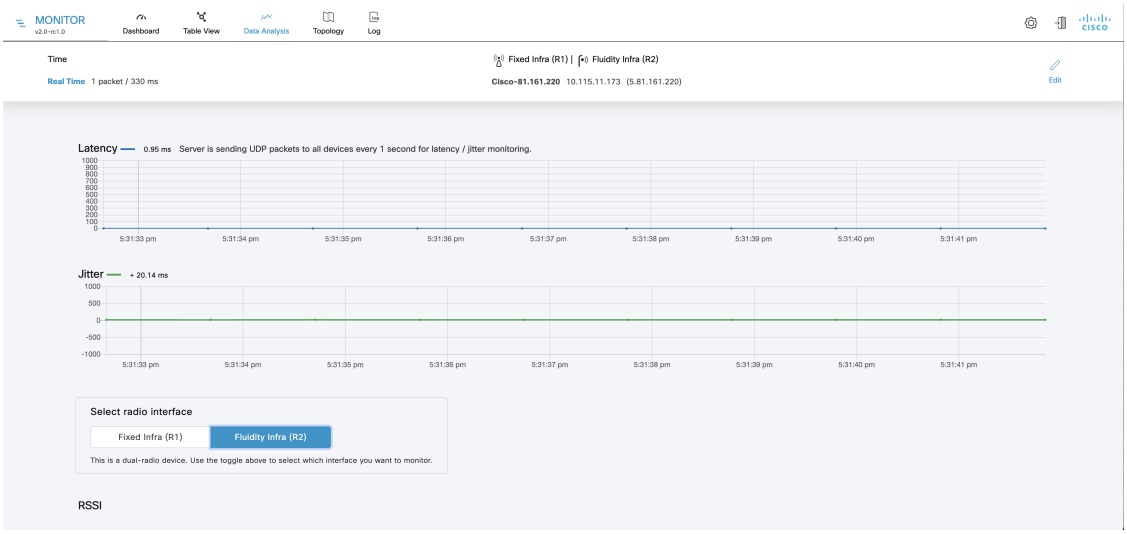
a) To view statistics for a device during a specific period, select the **History** tab.

b) In the **Custom time range** field, select the start and end dates and times for the range.

Note
The selected duration can't be more than 1 hour.

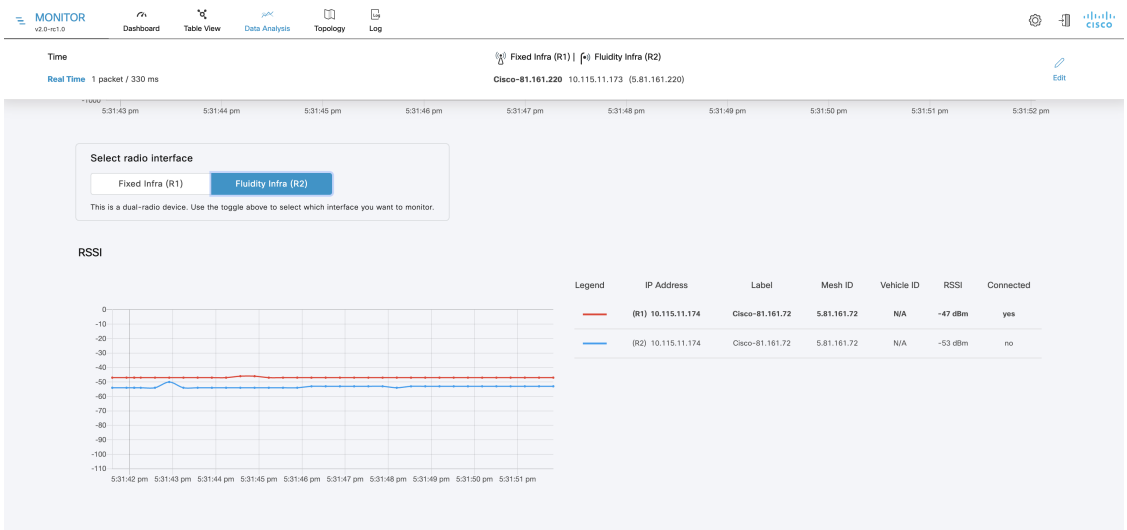
Step 3 In the **SEARCH DEVICE** field, search for a device by mesh ID, assigned device name, or IP address.

Step 4 In the **ANALYSE** field, click **Confirm** to proceed.



A real-time statistical view of the device appears. If you select the **History** tab, a time slider for the chosen period is also displayed.

a. The first graph shows the received signal strengths for the device and other radio units that it could connect to.



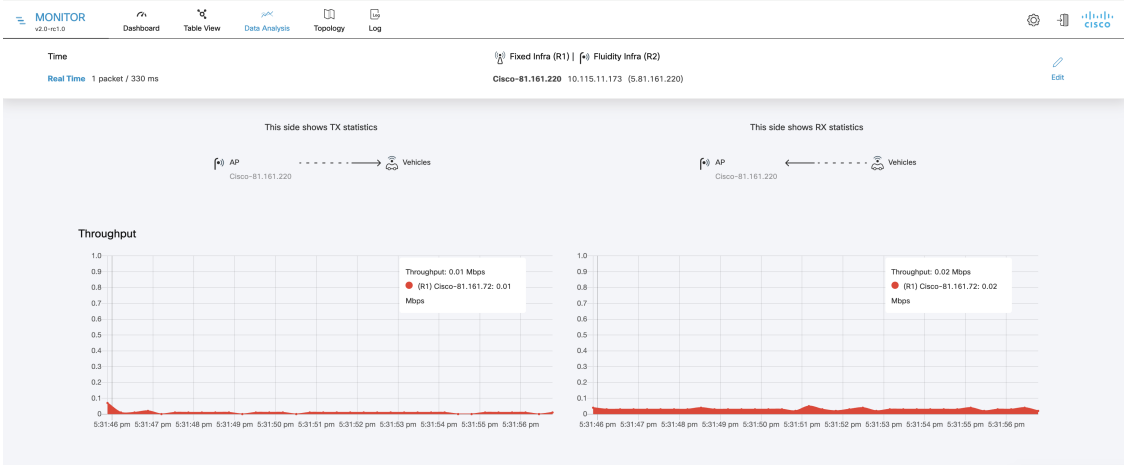
- The upper left corner of the graph shows whether the device currently accepts handoff requests.
- If the chosen device is currently connected to a Fluidity-enabled (vehicle-mounted) radio unit, a thick, dashed black line is superimposed over the Fluidity device's RSSI line. This line is the RSSI envelope and represents the strongest available signal.

Note

In the right-hand section of the graph, devices to which the current device is connected are listed in descending order of received signal strength (RSSI).

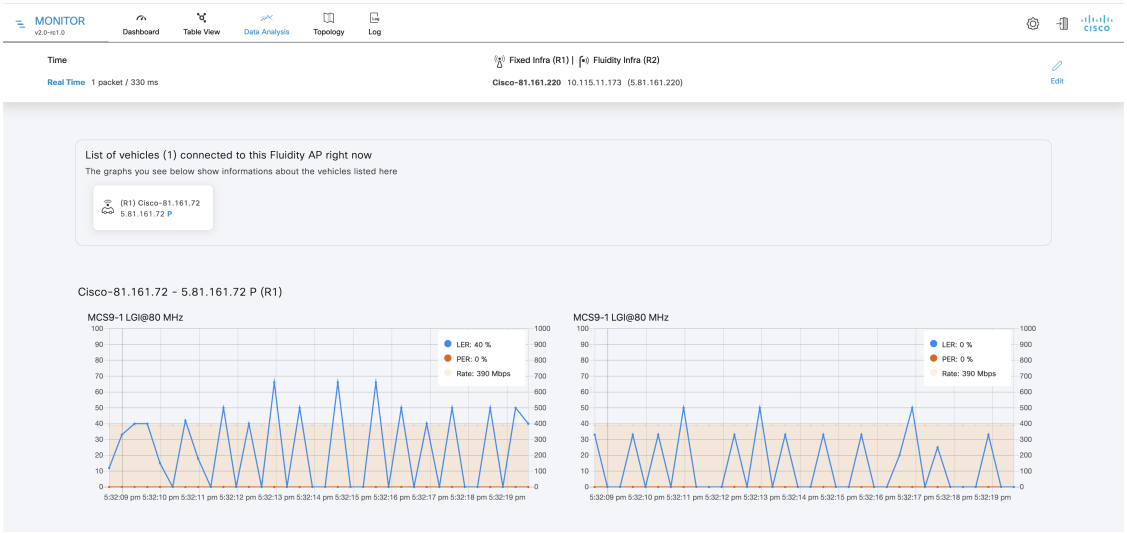
b. The throughput graphs display throughput statistics over time in Mbps, shown for the selected device and its current connection.

Note
The left graph shows uplink statistics (data flow from the current unit), while the right graph shows downlink statistics (data flow to the current unit).



c. The LER/PER graphs show the current link error rates, packet error rates (expressed as percentages over time), and comparative signal modulation rates. LER and PER are shown for both the selected device and its current connection.

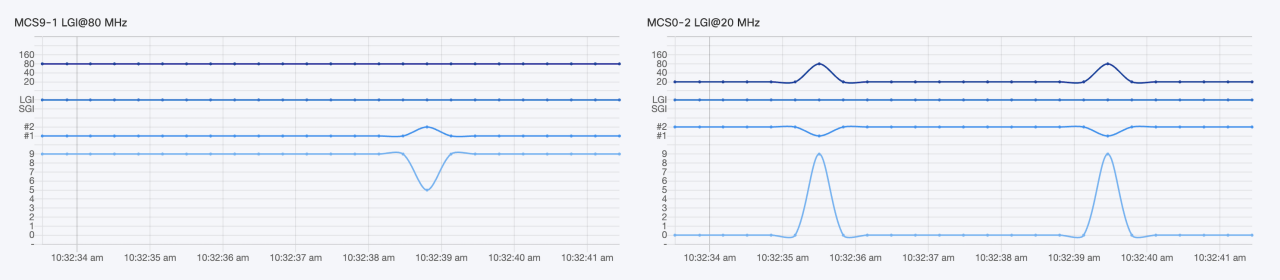
Note
The left graph shows uplink statistics (data flow from the current device), while the right graph shows downlink statistics (data flow to the current device).



d. The graphs in the fourth row show the modulation and coding schemas (MCS) for the selected device and its current connection.

Note
The left graph shows uplink MCS statistics for the current device, while the right graph shows downlink MCS statistics for the unit to which the current device is connected.

e. The upper left corner of the graph shows whether the device currently accepts handoff requests.



Note
This graph is shown only for vehicles.

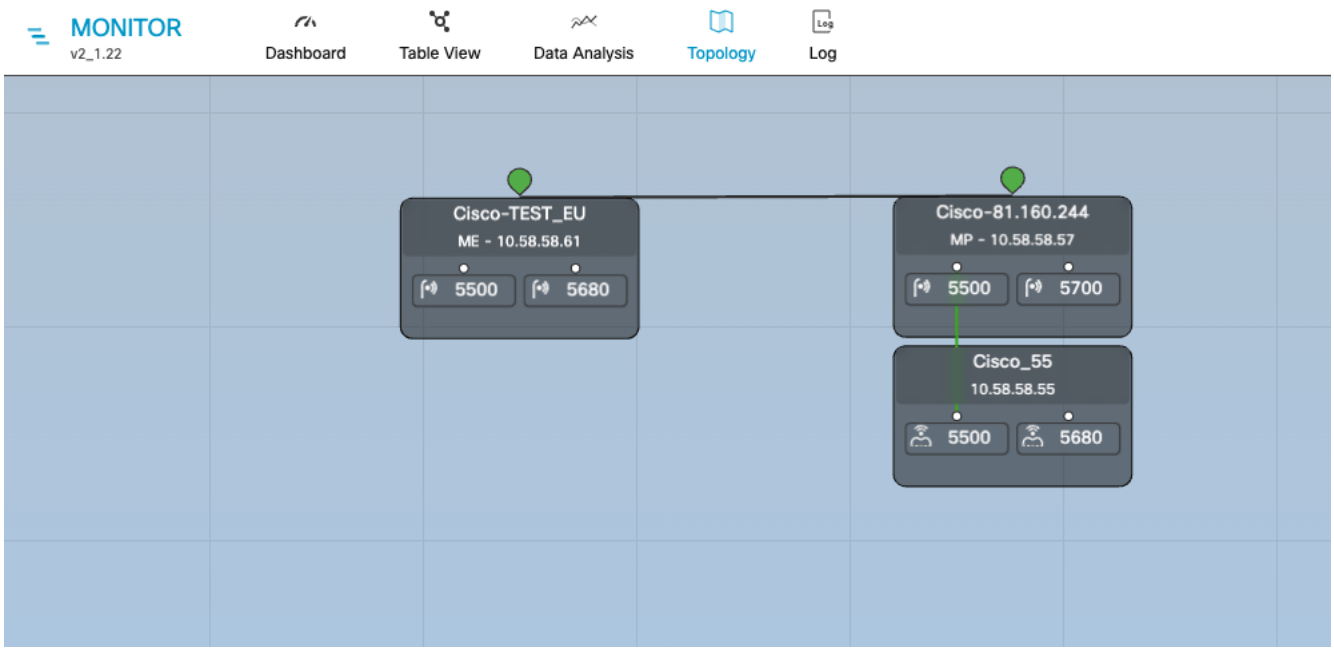
Step 5 Click **Edit** to view statistics for a different device.

View devices from Topology

Follow these steps to view and configure devices in Topology:

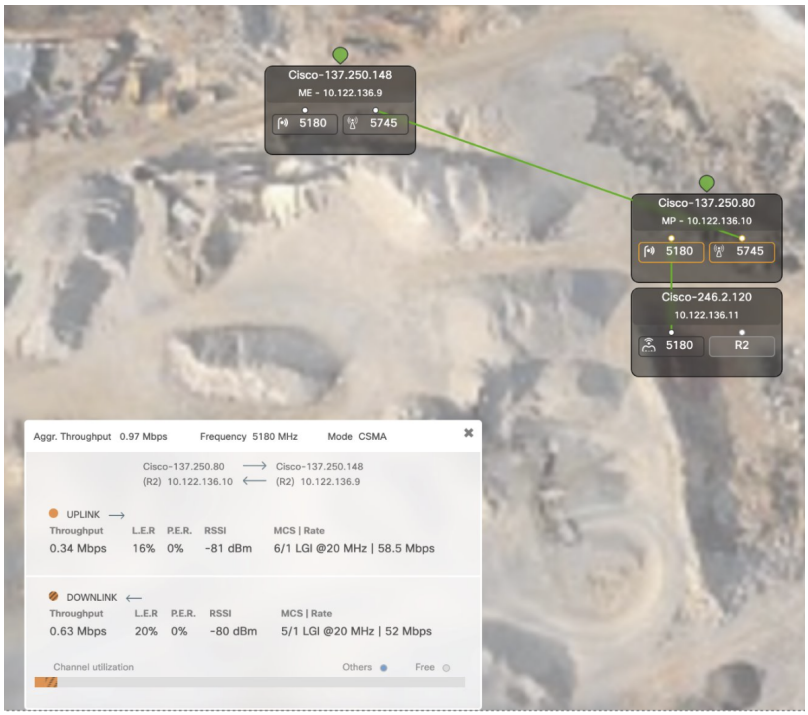
Procedure

Step 1 Click **Topology** to view network device layout.

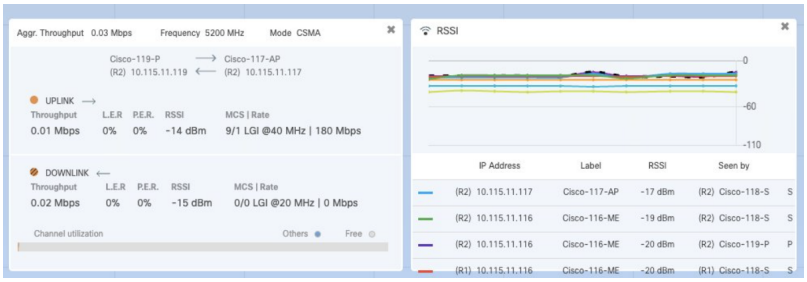


Step 2 Click a device to view its details.

Step 3 Click a wireless link or a mobile unit for link details.



Step 4 Click the Fluidity Vehicle Unit for mobile asset information.



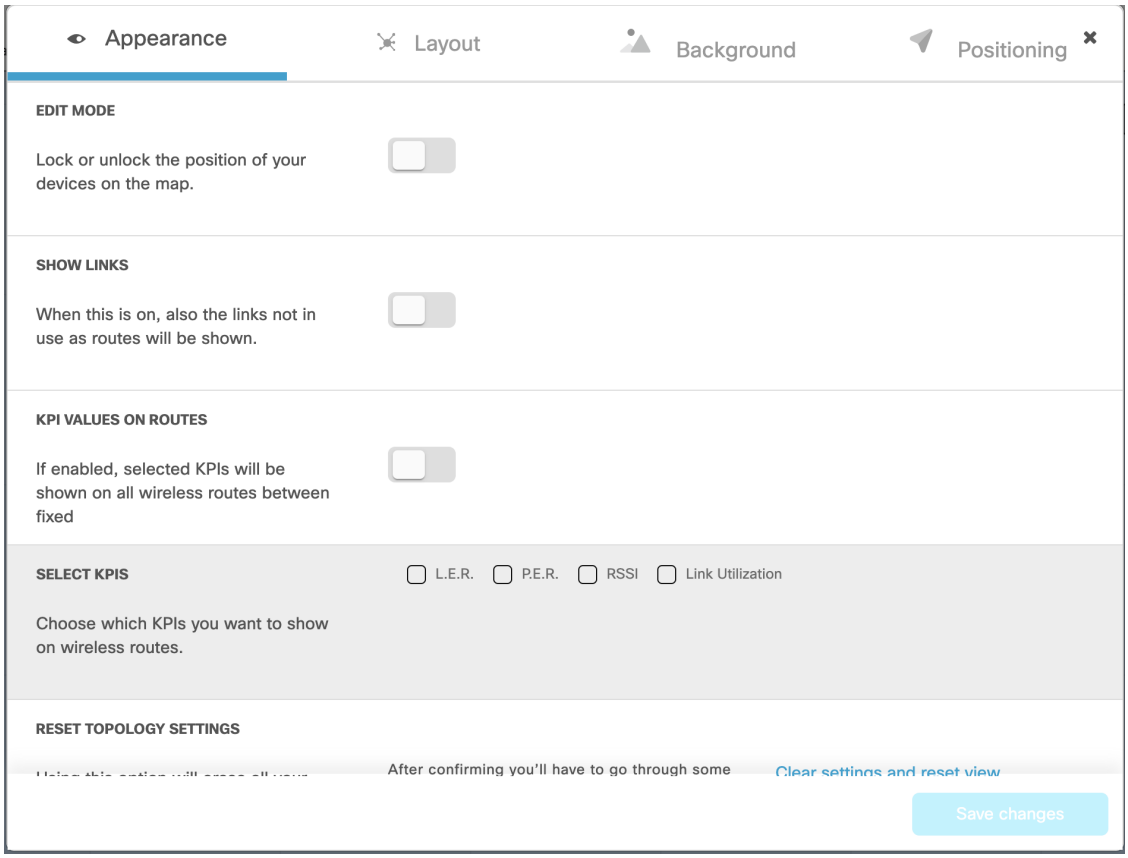
Step 5 Click **Web page**to open a separate device configurator login page.

- Log in with your credentials to access the configurator interface page.
- For more, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide.

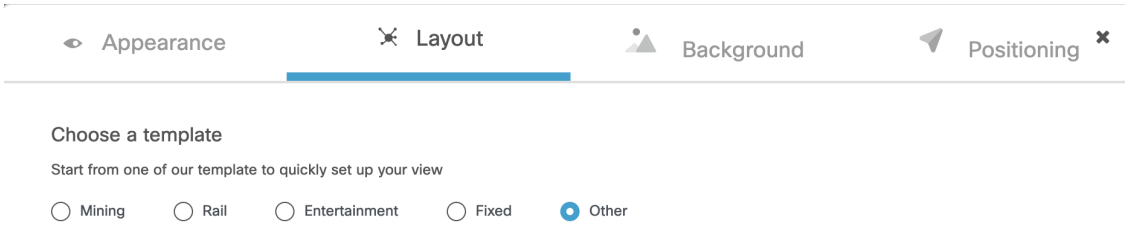
Step 6 Click **Settings**to adjust topology view settings:

a) In the **Appearance** toggle:

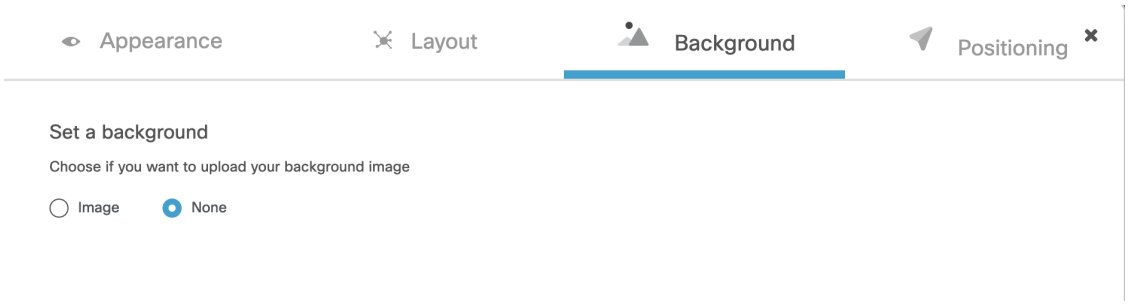
- **EDIT MODE** : to lock/unlock device positions on the topology map.
- **SHOW LINKS** : to display inactive links not in use as routes are shown.
- **KPI VALUES ON ROUTES** : to show performance metrics. (**L.E.R** , **P.E.R** , **RSSI** , and **Link Utilization**) will be shown for all wireless routes.
- **RESET TOPOLOGY SETTINGS** : to restore default settings.



b) In the **Layout** tab, select a view template.

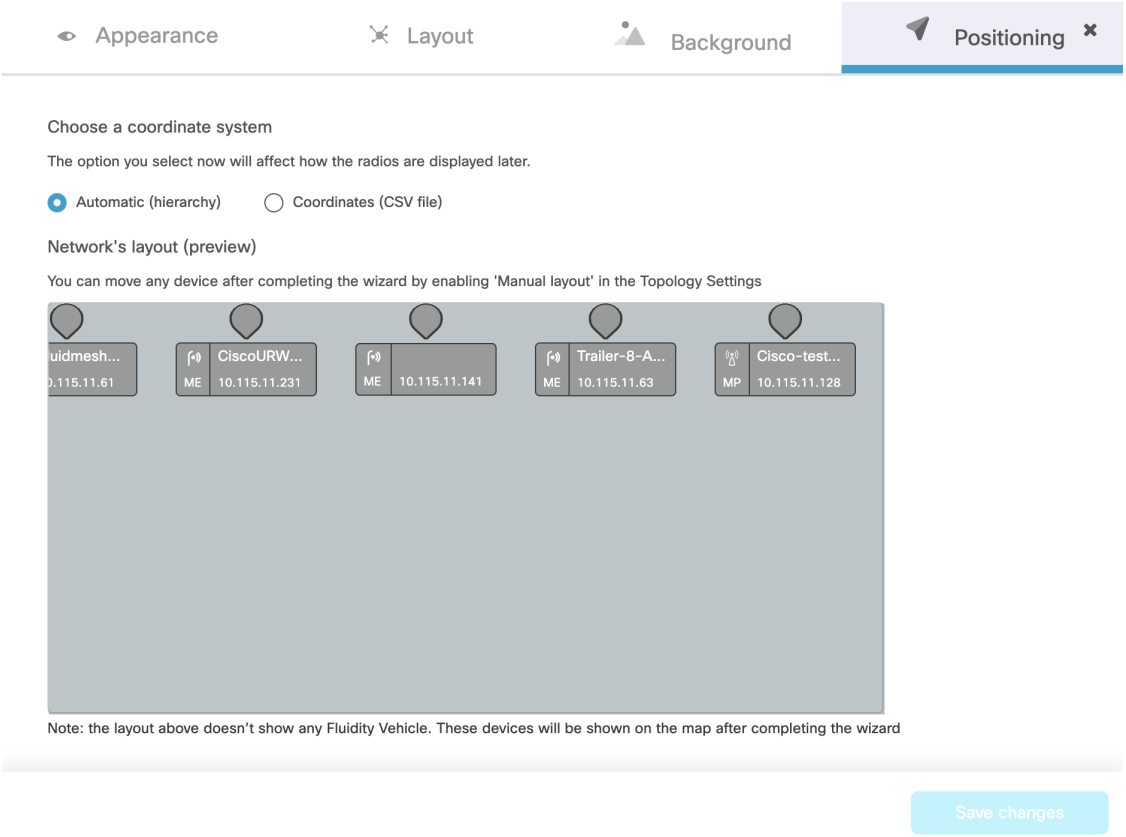


c) In the **Background** tab, customize the topology background.



d) In the **Positioning** tab, choose automatic or CSV-based positioning.

- **Automatic (hierarchy)** - Allows the devices to be positioned automatically as a tree.

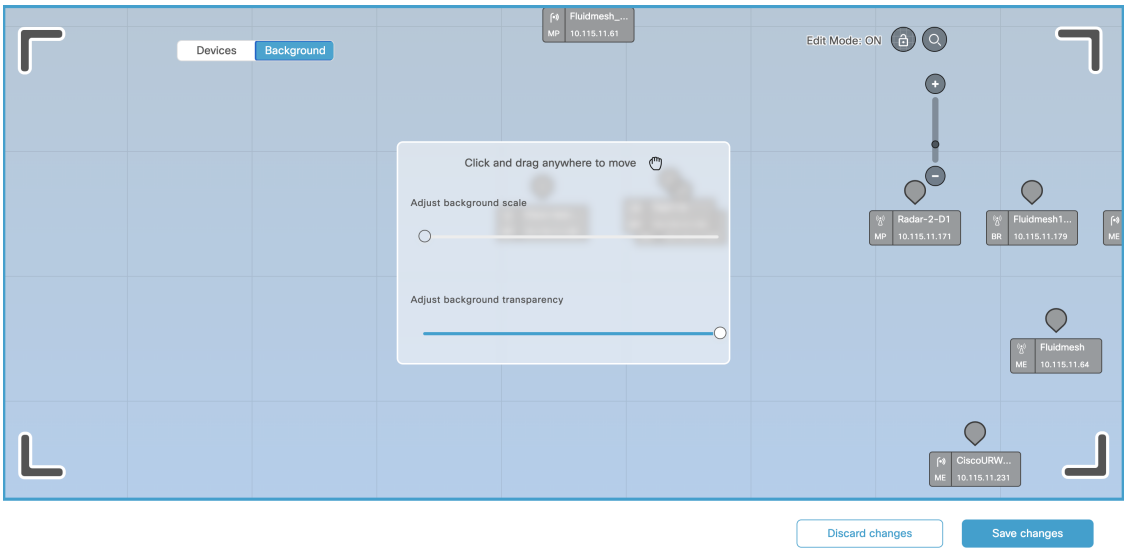


- **Coordinates (CSV file)** - You can upload a CSV file with the list of coordinates for each device (latitude and longitude). Then, position any two devices in the panel and all the other devices will be automatically positioned based on the geo coordinates in the CSV file.

Step 7 Click **Edit Mode** to modify device or background positions.

a) Click **Continue to Edit Mode** and make desired changes to devices or background..

- In **Devices** view, you will see the devices.
- In **Background** view, you can adjust the background scale and transparency to concentrate on a particular section of the topology view.



b) Click **Save changes** to apply modifications.

Step 8 Click **Zoom** to adjust the topology view.

Enable MPO processing to check in topology

Procedure

Step 1 Navigate to **Settings** > **MPO**.

Step 2 Enable **MPO Processing**.

Step 3 Select the time unit (Minutes or Hours) from the **TIME WINDOW** dropdown list.

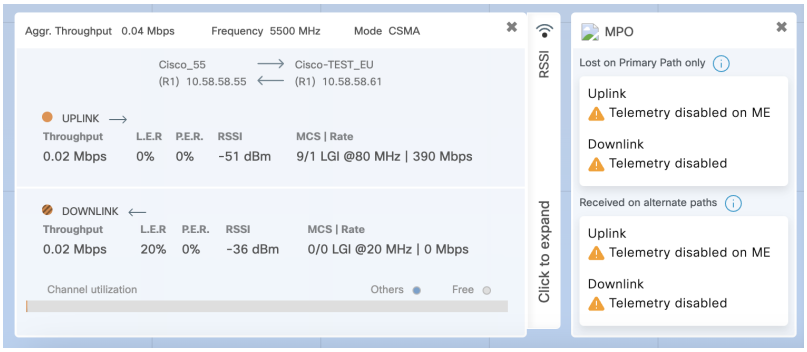
Step 4 Set the time window to compute the number of packets lost or received on the primary path. For example, 1minute to 59 minutes and 1hour to 24hours.

Step 5 Save your changes.

Enable MPO telemetry on both Mesh Ends and Fluidity. To use CLI commands, see the Software Configuration Guide.

Step 6 To view MPO telemetry metrics, go to the Topology screen and select **Fluidity Vehicle Unit**.

- If MPO telemetry is not enabled, a warning messages.



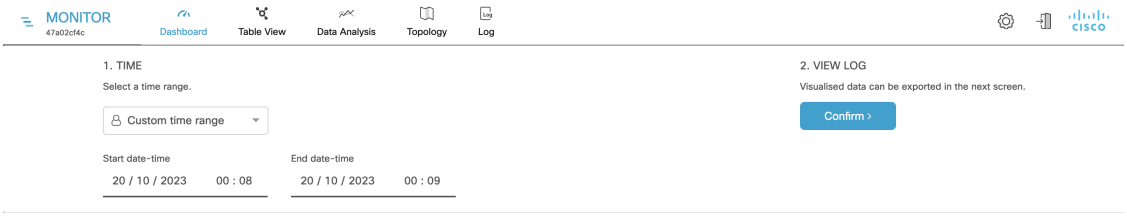
- If MPO telemetry is enabled, these metrics appear:

Metrics	Description
Lost on Primary Path only	These metrics provide details about the number of packets lost or received out of order on the primary MPO path, divided by the total number of packets sent on the primary path.
Received on alternate paths	These metrics provide details about the number of packets accepted on any MPO alternate path divided by the number of packets sent on all paths.

View network event logs

Procedure

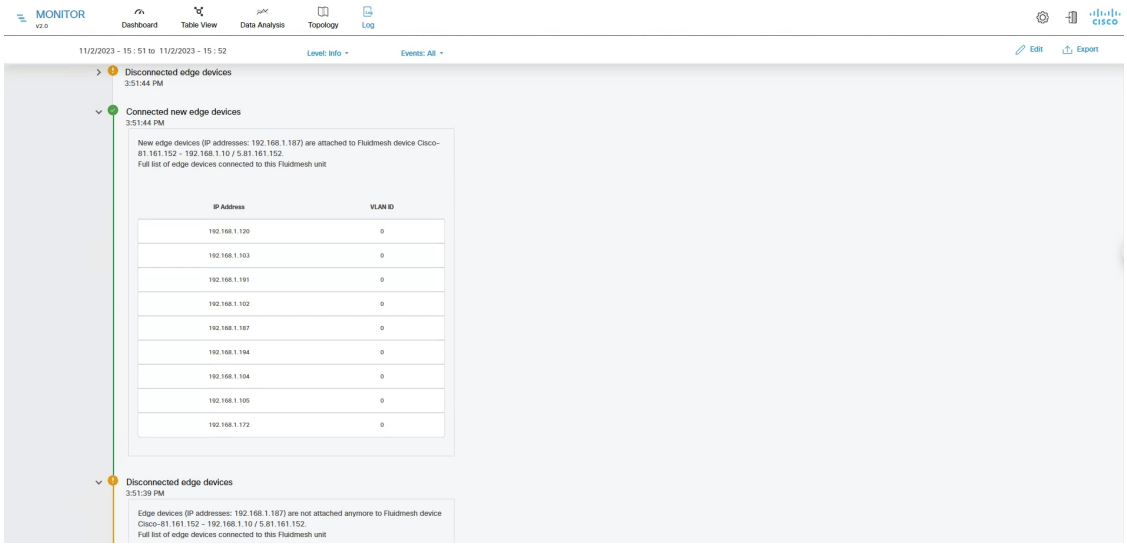
Step 1 Access the **Log** to view network events for the current device.



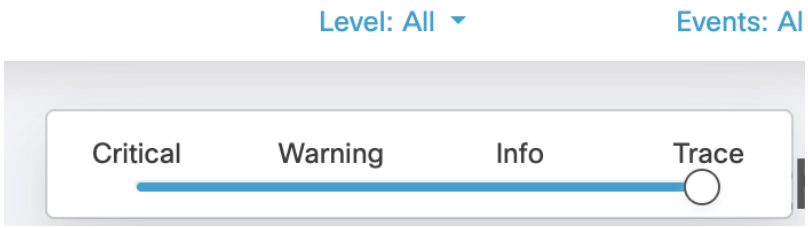
Step 2 In the **Custom time range** field, set the start and end dates and times for the range.

Step 3 Click **Confirm** to proceed.

A log of network related events is shown for the chosen date/time range.

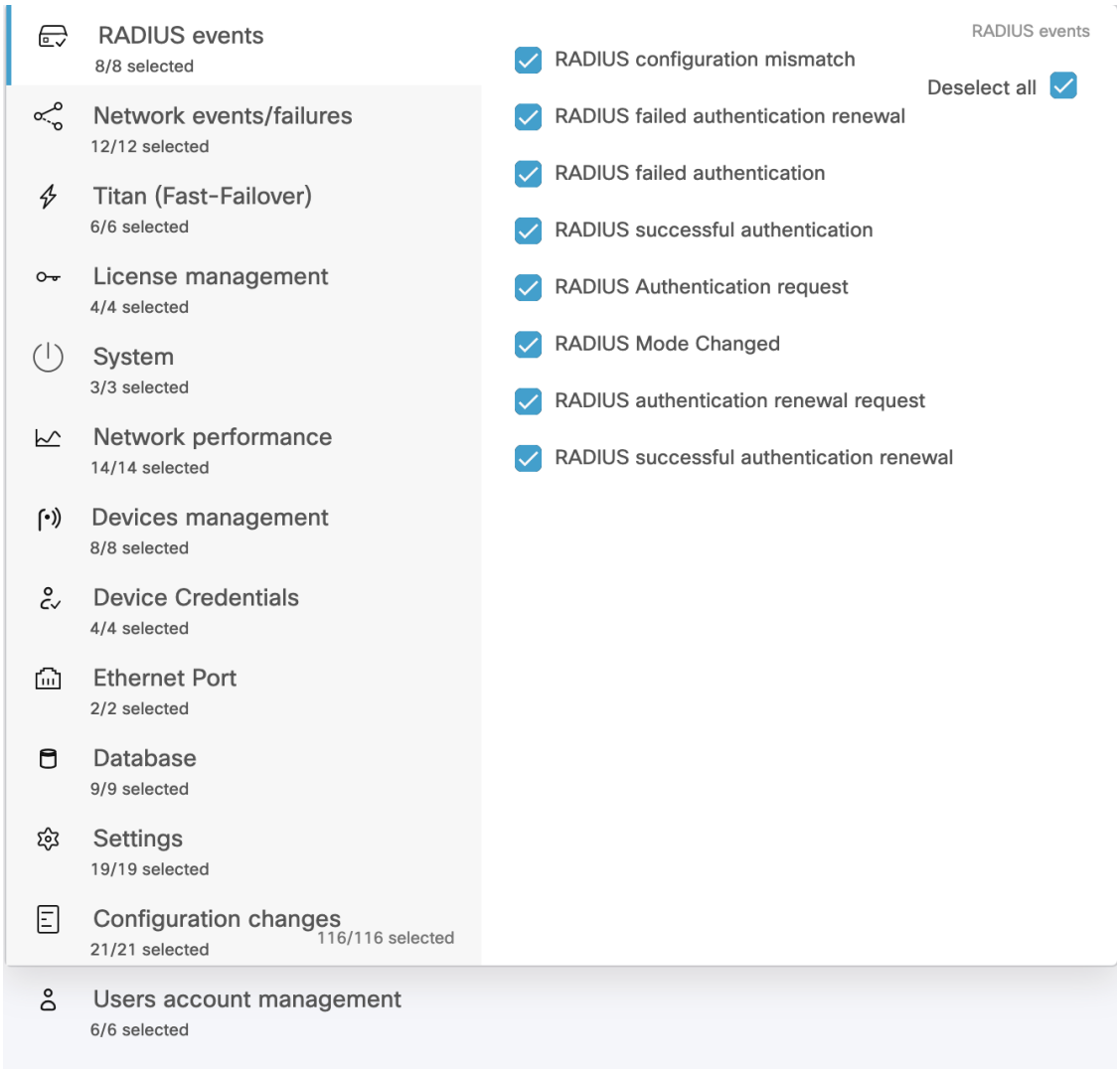


Step 4 In the **Level** dropdown, choose the level of criticality of network events.



- **Critical** - Critical level events have an immediate, negative impact on system performance or on system integrity and must be addressed immediately.
- **Warning** - Warning level events have a potentially negative impact on system performance and should be addressed as soon as practically possible.
- **Info** - Info level events are normal system events. This is the default event display level.
- **Trace** - Trace level events are considered trivial, but can be useful for diagnostic troubleshooting.

Step 5 In the **Events** dropdown, select the relevant category from the left pane and then select the checkboxes for the required network event.

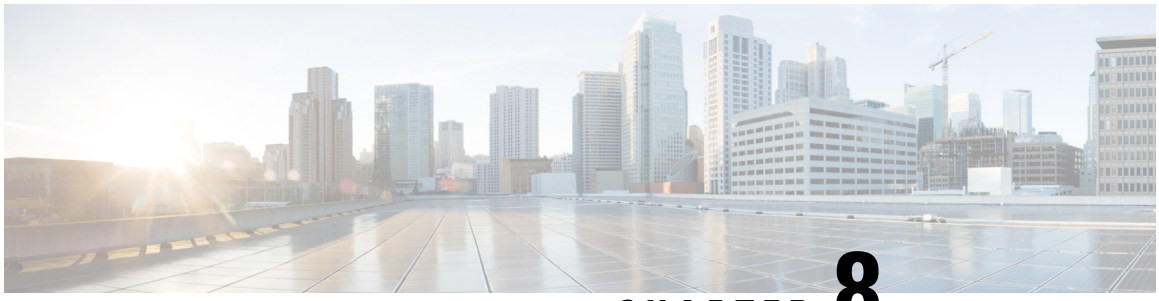


a) (Optional) To clear the applied filters, click **Clear Filters**.
b) (Optional) To edit the time range of the log, click **Edit**.

Export a network event log

Procedure

Step 1 Click **Export**.
Step 2 Review and confirm the date/time range in **Export Log** pop-up screen. Then click **Export** again.
Step 3 Select the save location.



CHAPTER 8

Configure IW Monitor Database Settings

• Configure database storage, back up, and clean IW Monitor statistics data, on page 45

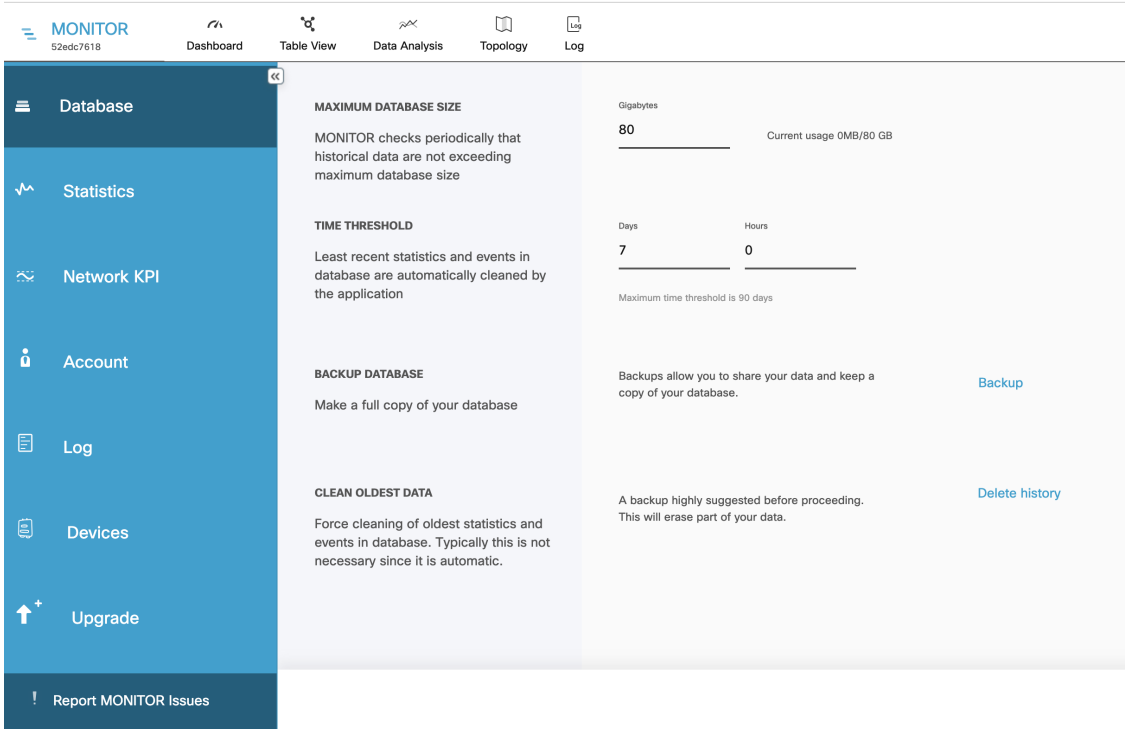
Configure database storage, back up, and clean IW Monitor statistics data

Before you begin

- Ensure that the hard disk has sufficient capacity (at least equal to the current database size and does not exceed total disk capacity).
- Use a hard disk with at least 100 GB; if using less, allocate no more than 75% of its capacity.
- Consider backing up data before deleting historical records.

Procedure

Step 1 Go to **Settings** > **Database**.



Step 2 Set the **MAXIMUM DATABASE SIZE** value.

The IW Monitor periodically checks whether the historical data remains within the defined maximum database value.

Note
If the network statistics data stored on the hard disk reaches the specified value before the period specified by the TIME THRESHOLD is complete, the IW Monitor overwrites old data with new data in real time.

Step 3 Set the **TIME THRESHOLD** value for data retention.

The time threshold indicates how long network statistics are recorded before older data is overwritten.

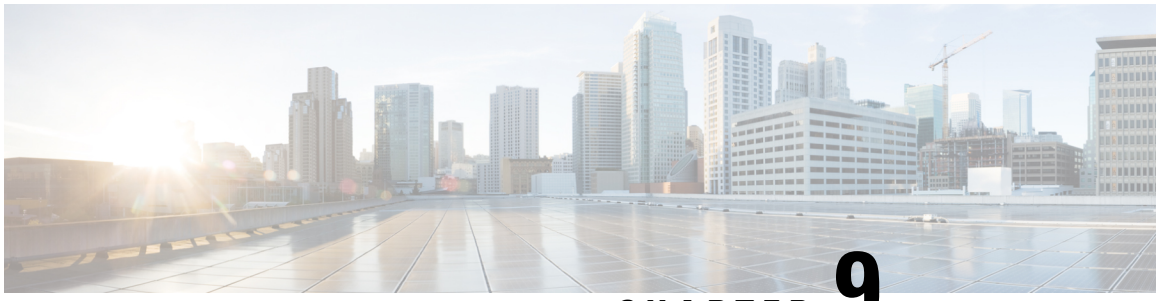
Note
The minimum storage period for time-related network statistics before overwrite is one hour; the maximum is 90 days.

Step 4 To back up the database, in **BACKUP DATABASE**, click **Backup**. After the backup completes, click **Download** to save the backup file.

Step 5 To delete the oldest data, in **CLEAN OLDEST DATA** , Click **Delete history** .

Note
The system deletes the oldest 10% of stored statistics data only if the database exceeds either the size or time threshold.

Note
Deleted data cannot be recovered. Always back up data before deletion.



CHAPTER 9

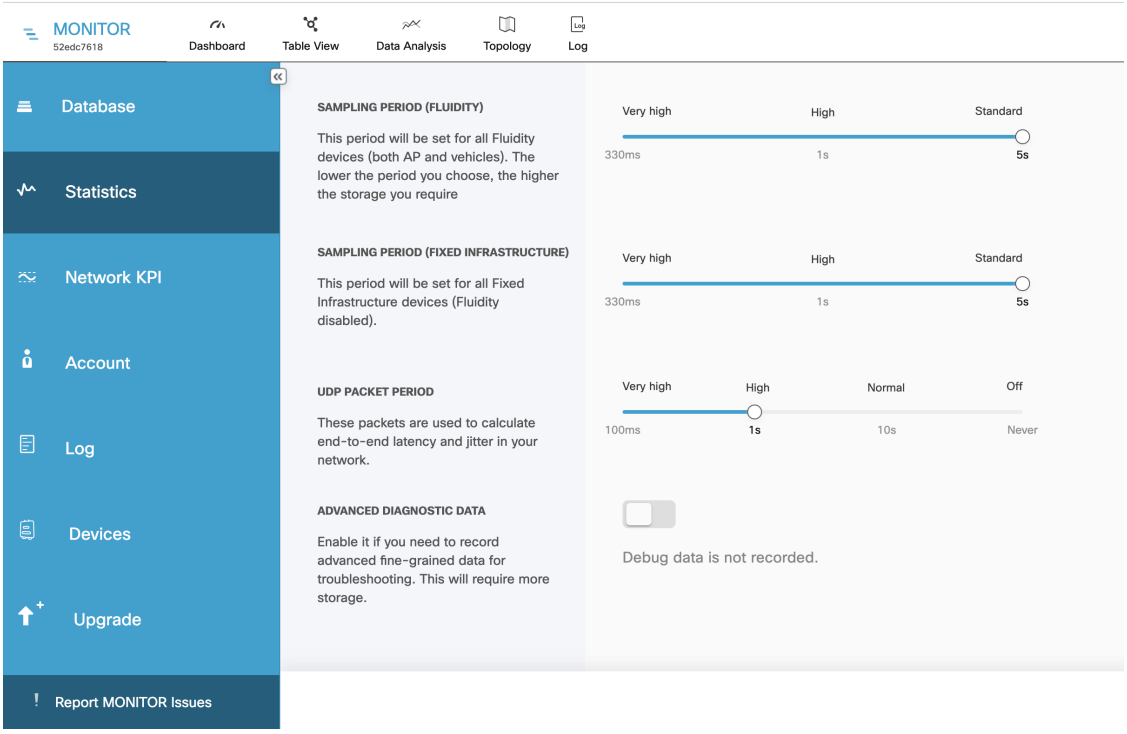
Configure IW Monitor Statistical Settings

- Change the interval at which statistical data is logged, on page 47
- Configure event log settings, on page 48
- Set performance thresholds, on page 50
- Set performance thresholds for each section, on page 51

Change the interval at which statistical data is logged

Procedure

Step 1 Go to **Settings** > **Statistics** .



Step 2 Set the **SAMPLING PERIOD (FLUIDITY)** and **SAMPLING PERIOD (FIXED INFRASTRUCTURE)** value to change the time interval at which statistical data is logged.

The recommended data-logging frequency intervals are:

- 330 ms for Fluidity
- 5 s for Fixed

Note
Logging data at a higher-than-normal frequency increases the rate at which the IW Monitor database occupies the hard disk space.

- Higher data-logging frequency provides a more detailed statistical log and reduces the chance of missing errors.
- Lower data-logging frequency conserves hard disk space.

Step 3 Set the **UDP PACKET PERIOD** value to increase the accuracy with which the IW Monitor host calculates network latency and jitter in the network.

a) To disable the UDP packet transmission, set the slider to Off.

The higher UDP packet frequency sampling gives more accurate latency and jitter readings, and the lower UDP packet frequency sampling helps reduce network congestion.

Note
The minimum interval at which UDP packets are sent is every 100 ms, and the maximum interval at which UDP packets are sent is every 10 s.

Step 4 Enable **ADVANCED DIAGNOSTIC DATA** to log debugging data for faster, more detailed information for technical support. This requires more storage.

Configure event log settings

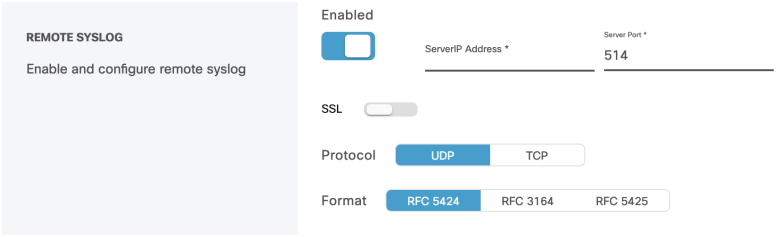
Procedure

Step 1 Go to **Settings** > **Log**.

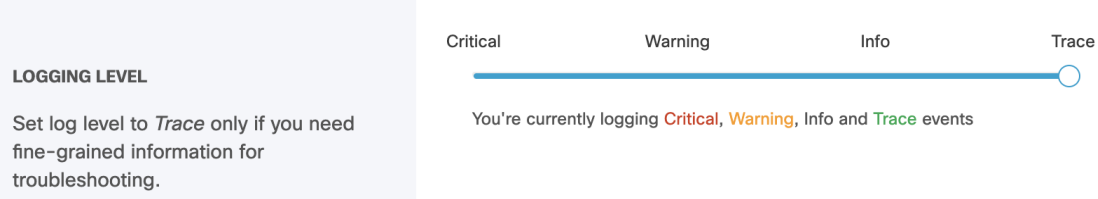
Step 2 Enable **LOG STORAGE** to view your network log.

Step 3 Enable **REMOTE SYSLOG** to collect system logs from a remote location.

a) On the Remote Syslog screen, enter the remote syslog **server IP address** and **port** . Set SSL, Protocol, and remote syslog format as needed.



Step 4 Select the desired **LOGGING LEVEL**.



- **Trace** - Trace-level events are considered trivial, but can be useful for fine-grained information for troubleshooting.
- **Info** - Info-level events are normal system events. This is the default event display level.
- **Warning** - Warning-level events are those that have a potentially negative impact on system performance, and should be addressed as soon as practically possible.
- **Critical** - Critical-level events are those that have an immediate, negative impact on system performance and/or system integrity, and should be addressed immediately.

Step 5 In the **Event** section, check and uncheck the type of events you want to log.

All network event types are grouped into these categories:

- Users account management
- RADIUS events
- Devices credentials
- Network events and failures
- Settings
- Device management
- Configuration changes
- Network performance
- License management
- Database
- System
- Titan (Fast-Failover)
- Ethernet Port

Step 6 Click **Save Changes** .

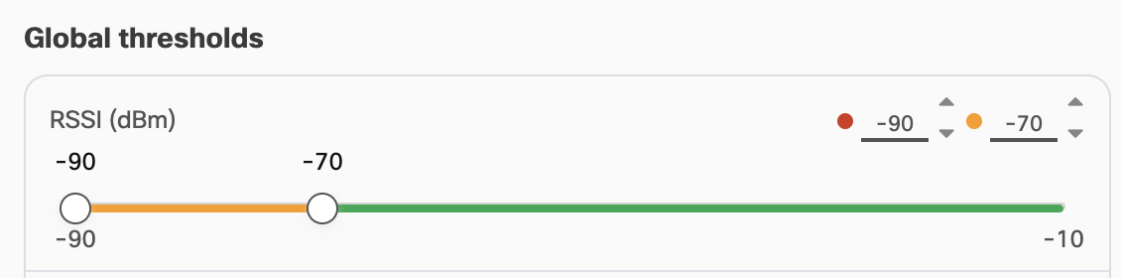
Set performance thresholds

Procedure

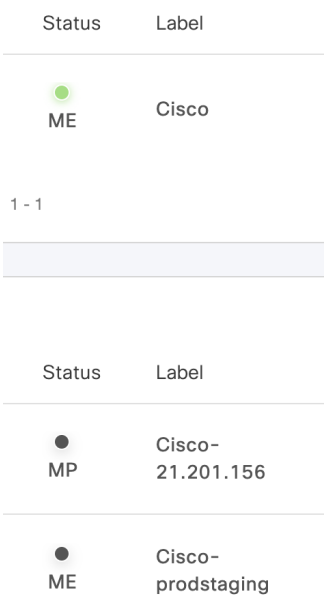
If you want to apply the same performance-alert thresholds to all sections that are part of the network, adjust the performance thresholds by doing these steps:

Each performance threshold slider has two buttons that can be clicked and dragged.

a) Click-and-drag the left-side button to set the lower performance threshold. If the relevant parameter falls below this threshold, the relevant **Status** icons will turn red.
b) Click-and-drag the right-side button to set the upper performance threshold. If the relevant parameter falls below this threshold, the relevant **Status** icons will turn yellow.



If radio signal strength, link error rate, packet error rate, or network latency drop below the specified levels, the **Status** icons of individual devices in the table view display the relevant status.



Set performance thresholds for each section

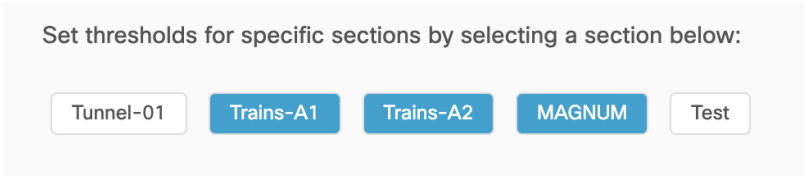
Procedure

Step 1 Go to **Settings** > **Network KPI** .

Step 2 Enable **PERFORMANCE CHECK** to display the default thresholds section.

Step 3 Ensure the current network is divided into at least two sections. For information about partitioning the network, see Create a new section, on page 21 .

Step 4 When the network is partitioned, tabs appear for each network section under the **Global Thresholds**.



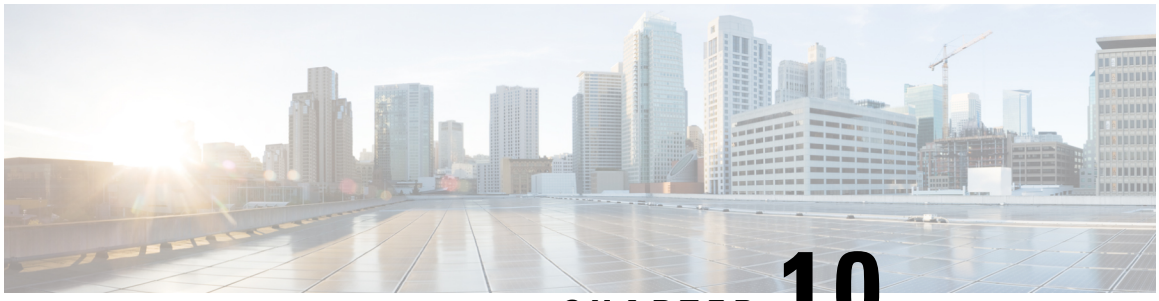
Step 5 Select the network section for which you want to alter the performance thresholds.

A separate group of performance-alert threshold sliders will be shown for the specified network section. For more information about thresholds, see Set performance thresholds, on page 50 .



Step 6 Click-and-drag the sliders to adjust the performance-alert thresholds for the specified network.

Step 7 Repeat these steps for each network section.



CHAPTER 10

Manage User Accounts

- Update a user account, on page 53
- View, add, and delete users, on page 53

Update a user account

Procedure

Step 1 Go to **Settings** > **Account** .

Step 2 To change your first name and/or last name, update the **First name** and **Last name** and click **Save Changes** .

Note
You cannot change the listed e-mail address using the user account settings page.

Step 3 To change your access password details, perform these steps:

a) Enter your current access password in the **Current password** field.

Note
Passwords are case-sensitive.

b) Enter the new access password in the **New password** field.

Note
The new passwords must be a minimum of eight characters, and must include at least one uppercase letter, one lowercase letter, and one digit.

c) Click **Save Changes** .

View, add, and delete users

Use the Settings menu in IW-MONITOR to manage user accounts, including viewing, adding, and deleting users.

Procedure

Step 1 Go to **Settings** > **Account**.

Step 2 To add a new user, follow these steps:

a) Fill the new user's e-mail address in the **Email** field.
b) Fill the new user's first name in the **First name** field.
c) Fill the new user's last name in the **Last name** field.
d) Confirm that the details are correct and click the **Add** .

The new user will be added to the **Other users** list. The status of the new user listing will be shown as **Pending** .

Note
A random access password will be generated for the new user.

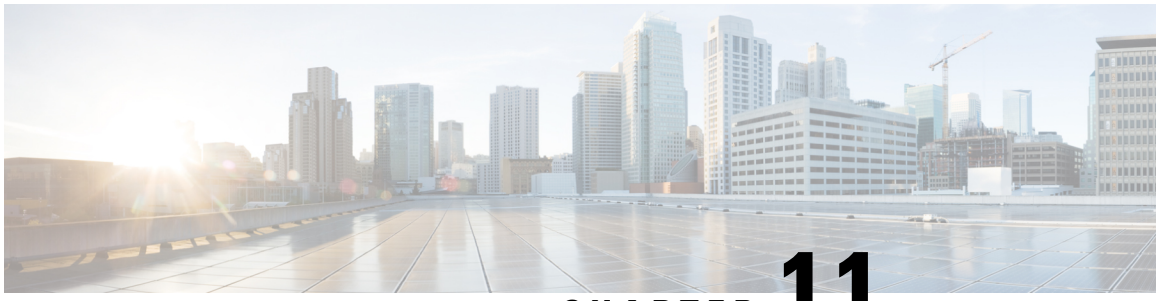
e) Click  (eye icon) to view the generated password for the new user.
f) Send the generated password to the new user. The system prompts the user to change the password when they log in for the first time.

Step 3 To delete a user, do the following steps:

a) View the list of existing user accounts in the **Other users** section.
b) Click on the **X** to the right of the user listing.

A **Remove User** pop-up appears for confirmation.

c) Click **Remove** .



CHAPTER 11

Update IW Monitor

• Update the IW Monitor, on page 55

Update the IW Monitor

For best performance, always use the latest version of the IW Monitor application. Updates may provide new features, improve operation, and fix bugs.

Procedure

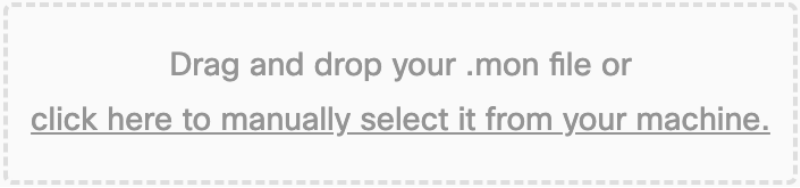
Step 1 Go to software downloads.

Step 2 Download the latest IW Monitor image file (**iw-monitor-upgrade-tovX.Y.Z.mon**).

Step 3 Log in to the IW Monitor.

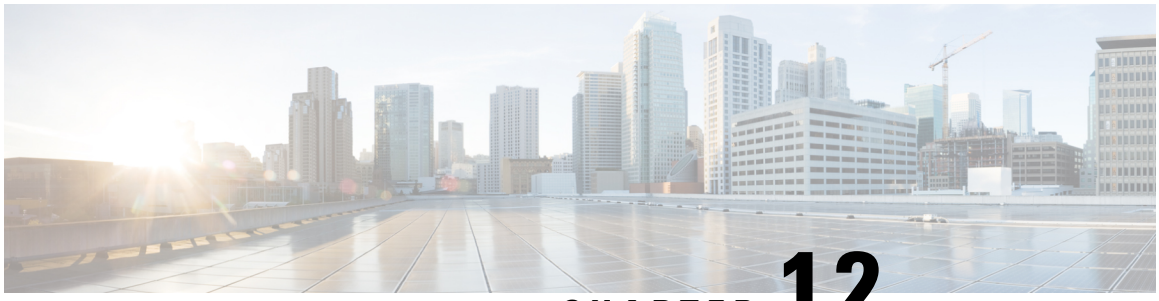
Step 4 Go to **Settings** > **Upgrade** .

Step 5 Locate the correct image file on your computer or drag and drop the image file.



Note
The image files have an *.MON file extension.

The IW Monitor server initialization page opens and the IW Monitor application is updated.



CHAPTER 12

Uninstall IW Monitor

• Uninstall IW Monitor, on page 57

Uninstall IW Monitor

Procedure

Step 1 Open a command-line window on the IW Monitor host.

Step 2 Enter the command: `docker ps -a`

The command-line interface shows the **CONTAINER_ID** value of the IW Monitor installation.

Step 3 Enter the command: `docker rm -f <CONTAINER_ID>`

The Docker container is removed from the IW Monitor host.

Step 4 Enter the command: `docker images`

The command-line interface shows the **IMAGE_ID** value of the IW Monitor Docker image.

Step 5 Enter the command: `docker rmi -f <IMAGE_ID>`

The IW Monitor Docker image is removed from the IW Monitor host.

Uninstall IW Monitor

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.