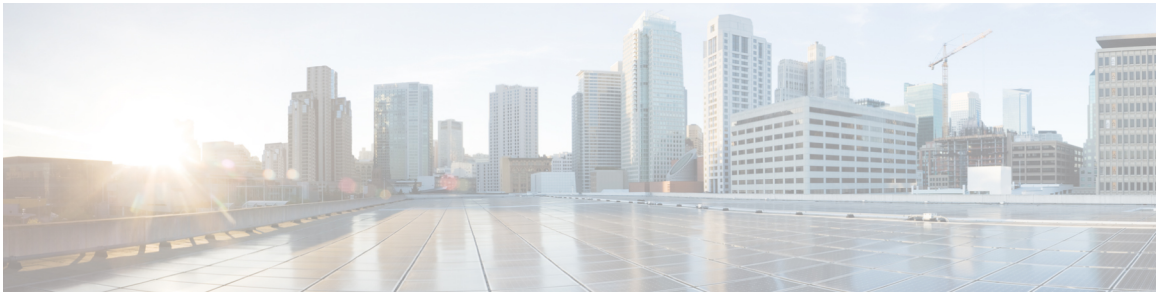


IW Monitor User Guide, Release 2.0.0

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

About this Guide v

Related Documentation v

Communications, Services, and Additional Information v

CHAPTER 1

Overview of the IW Monitor 1

IW Monitor Overview 1

CHAPTER 2

Supported Network Devices and Firmware for IW Monitor 3

Supported Network Devices and Firmware for IW Monitor 3

CHAPTER 3

Installing IW Monitor Docker on Host 5

Host and Network Requirements 5

Installing Docker on Host 7

Installing and Running Docker Container 8

Downloading and installing the Docker application 8

Downloading the IW Monitor Image 8

Loading the IW Monitor Image File to the IW Monitor Server 8

Running the Docker Container for the First Time 9

Logging to the IW Monitor for the First Time 10

CHAPTER 4

Adding Devices to the IW Monitor 19

Adding Devices to the IW Monitor 19

CHAPTER 5 **Managing Sections** 23

Creating a new Section 23

Editing a Section 24

Deleting a Section 24

CHAPTER 6 **Managing Devices** 25

Editing the Device Configuration Parameters using Configurator Interface 25

Detaching the Device from the IW Monitor 26

CHAPTER 7 **Monitoring Network Performance** 29

Viewing the Network Statistics 29

Viewing the Devices using Table View 30

Viewing the Uplink and Downlink Information for a Device 34

Viewing Device Statistics in Real Time 36

Viewing the Devices from Topology 39

Filtering and Viewing Network Events 43

Exporting a Network Event Log as a CSV File 45

CHAPTER 8 **Configuring IW Monitor Database Settings** 47

Defining Hard Disk Storage Capacity and Overwrite Cycle Period for the IW Monitor Statistics Database 47

Backing up the IW Monitor Statistics Database 49

Deleting the recent IW Monitor Statistics Data 50

CHAPTER 9 **Configuring IW Monitor Statistical Settings** 53

Changing the Interval at which Statistical Data is Logged 53

Customizing Event-Logging Settings 55

Setting Performance Thresholds 57

Setting Performance Thresholds for Each Section 58

CHAPTER 10 **Managing User Accounts** 61

Modifying an Existing User Account 61

Viewing, Adding, and Deleting Users 62

CHAPTER 11 **Updating IW Monitor** 63

Updating IW Monitor 63

CHAPTER 12 **Uninstalling IW Monitor** 65

Uninstalling IW Monitor 65



Preface

This preface describes this guide and provides information about how to use IW Monitor, and related documentation.

It includes the following sections:

- About this Guide, on page v
- Related Documentation, on page v
- Communications, Services, and Additional Information, on page v

About this Guide

This guide details Cisco Industrial Wireless (IW) Monitor, an on-premises monitoring tool for maintaining and monitoring one or multiple Ultra-Reliable Wireless Backhaul (URWB) networks. IW Monitor displays data and situational alerts from every URWB device in a network in real-time. This is the first release of IW Monitor, and it manages Industrial Wireless (IW) and Fluidmesh devices.

Related Documentation

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

Communications, Services, and Additional Information

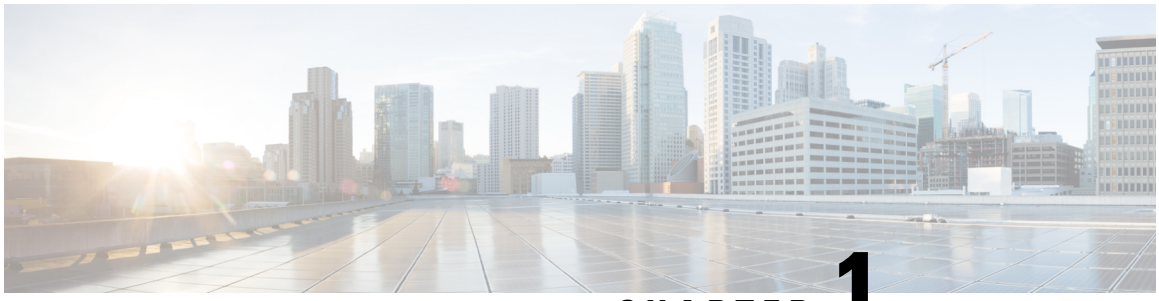
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with 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

Overview of the IW Monitor

- IW Monitor Overview, on page 1

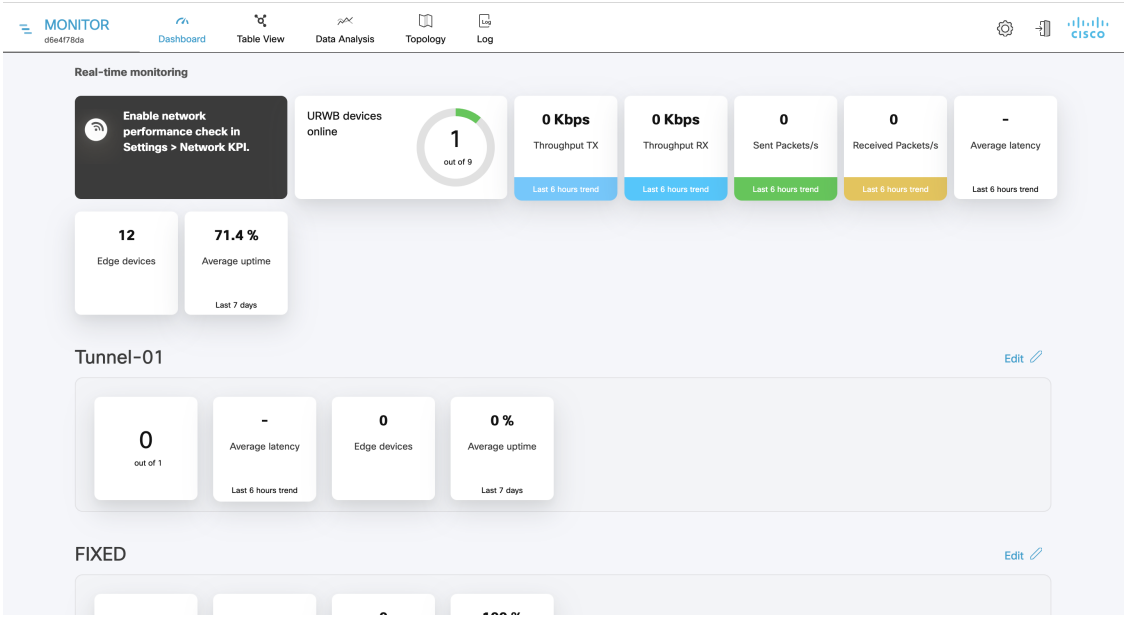
IW Monitor Overview

IW Monitor application is an on-premises monitoring tool for Industrial Wireless (IW) and Fluidmesh devices and it is designed to be used along with IoT Operations Dashboard (OD) with IW Service. The IW Service allows you to configure and provision the Industrial Wireless devices, whereas IW Monitor displays real-time data and alerts for URWB devices in the network. The functionality of the two interfaces differs as follows:

- IW Service is the cloud-based interface used to do online and offline configuration of IW devices.
- IW Monitor is a virtual-image-based diagnostic and analysis interface, with the virtual image installed in Docker format to monitor Fluidmesh and Industrial Wireless devices.

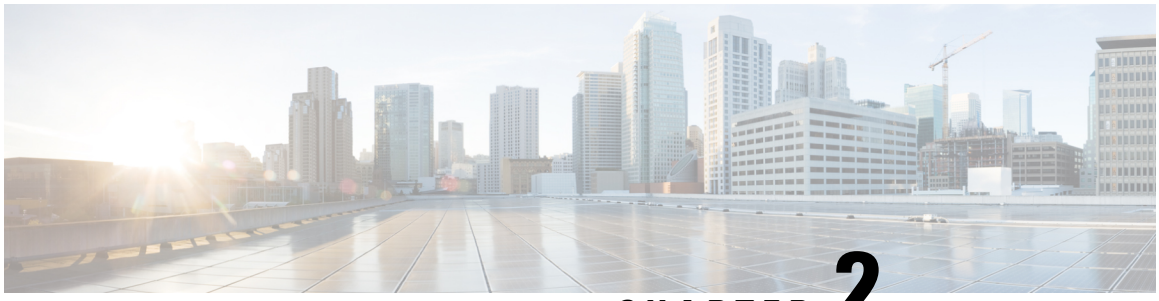
The functionalities of IW Monitor application are:

- 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 diagnostic and generate alerts if network related faults arise.
- Analyze network data, with the goal of increasing system uptime and maintaining optimum network performance.



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

- To add and configure devices using cloud-based IW Service, see IoT OD IW documentation.
- 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.



CHAPTER 2

Supported Network Devices and Firmware for IW Monitor

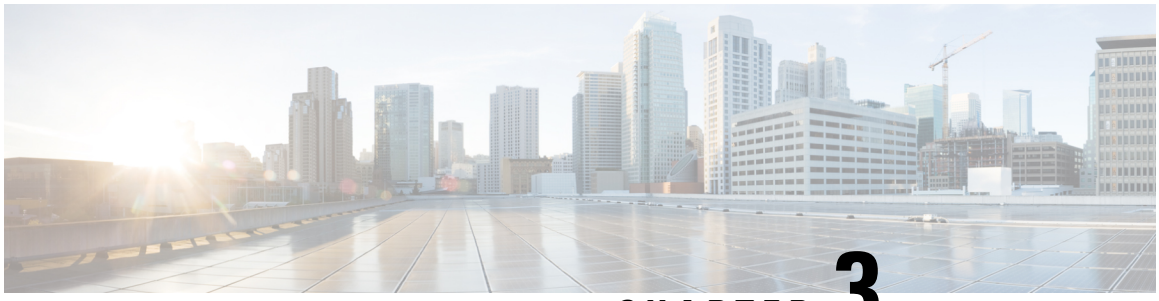
• Supported Network Devices and Firmware for IW Monitor, on page 3

Supported Network Devices and Firmware for IW Monitor

The following table shows the supported device models and the recommended firmware versions:

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

Supported Network Devices and Firmware for IW Monitor



CHAPTER 3

Installing IW Monitor Docker on Host

- Host and Network Requirements, on page 5
- Installing Docker on Host, on page 7
- Installing and Running Docker Container, on page 8
- Downloading and installing the Docker application, on page 8
- Downloading the IW Monitor Image, on page 8
- Loading the IW Monitor Image File to the IW Monitor Server, on page 8
- Running the Docker Container for the First Time, on page 9
- Logging to the IW Monitor for the First Time, on page 10

Host and Network Requirements

Host requirements

Note It is recommended to have a high-speed, high bandwidth internet connection for installation of Docker and the IW Monitor image file.

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, on page 8.

Make sure the following host requirements are met to run the Docker container:

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 Using a hard disk of at least 100 GB capacity is recommended. If a hard disk of less than 100 GB capacity must be used, adjust the maximum capacity available for statistics storage as mentioned in Defining Hard Disk Storage Capacity and Overwrite Cycle Period for the IW Monitor Statistics Database, on page 47.

Browser requirements

Use the latest version of a supported web browsers to access the IW Monitor:

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.

Installing Docker on Host

A Docker image is a standard, self-contained unit of software that packages code and its dependencies that lets the application run quickly and reliably from one computing environment to another. Docker images become containers at runtime when they run on the Docker engine.

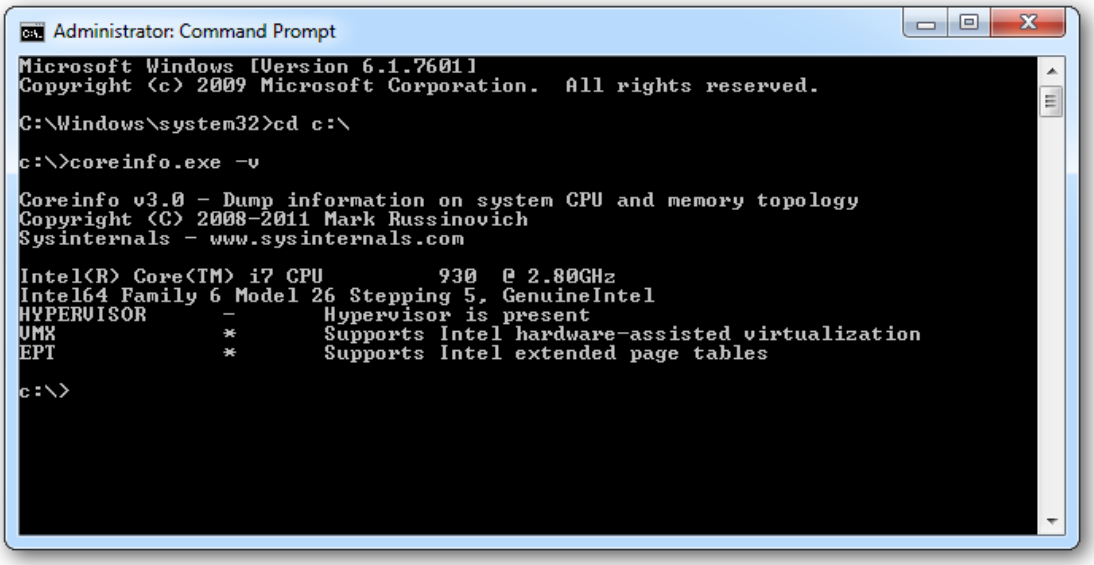
Prerequisites to install Docker on the IW Monitor host

When Docker is installed on the IW Monitor host, make sure that the host's CPU supports virtualization and second-level address translation (SLAT).

Note Intel's version of SLAT is called EPT (Extended page tables).

To check if the host's processor or processors meets the requirement:

1. Go to Microsoft Sysinternals, 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 (below):



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

To check if CPU supports SLAT:

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

Installing and Running Docker Container

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

Important Do not install the Docker container on your local computer. Docker must only be installed on the host assigned to run the IW Monitor. To view the minimum hardware specifications of the host, see Host and Network Requirements, on page 5.

Note Oracle VM VirtualBox is not supported.

Downloading and installing the Docker application

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.

Downloading the IW Monitor Image

Step 1 Go to software downloads.
Step 2 Download the IW Monitor image file (`iw-monitor-dockerv1. x.x.tar`).

Loading the IW Monitor Image File to the IW Monitor Server

Step 1 Open a command-line window.
Step 2 Enter the command: `docker load -i iw-monitor-dockerv1. x.x.tar`
Step 3 Enter the command to check if the IW Monitor image file is loaded: `docker images`

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

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. Make a note of the IMAGE ID value of the IW Monitor Docker image.

Running the Docker Container for the First Time

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 port numbers of the IW Monitor which runs on within the Docker container are:

- Port 8443 (https with SSL)
- Encryption / 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.

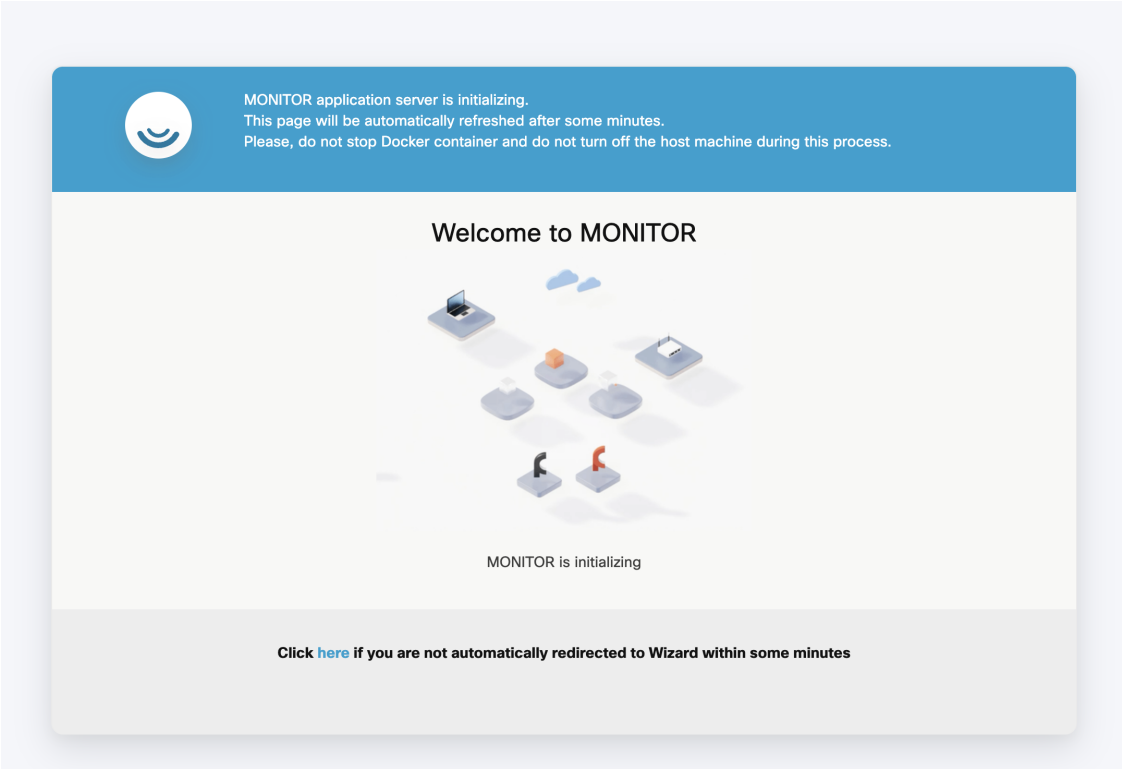
Note For example, a run command that specifies port 3000: `docker run -d --name iw_monitor -p 3000:8443 iw_monitor`

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 Adding Devices to the IW Monitor, on page 19.

Step 4 Open the web bowser.

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.

IW Monitor Docker container is successfully launched and the welcome page is shown as below:

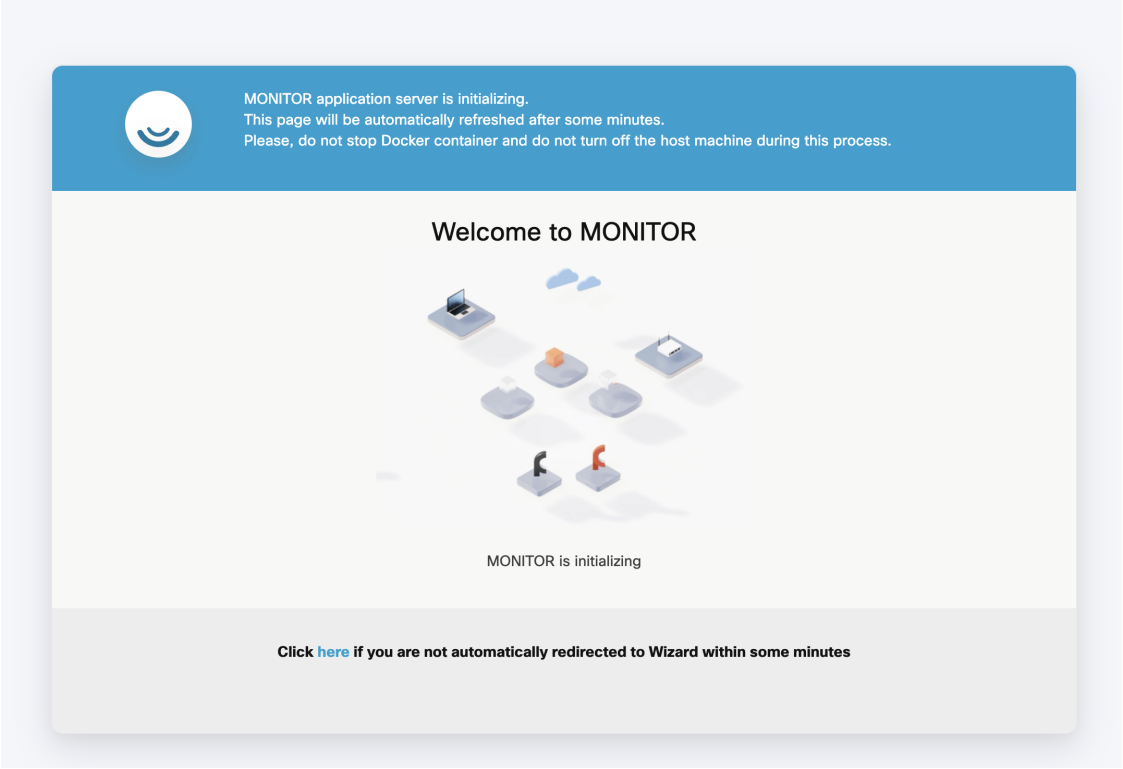


Logging to the IW Monitor for the First Time

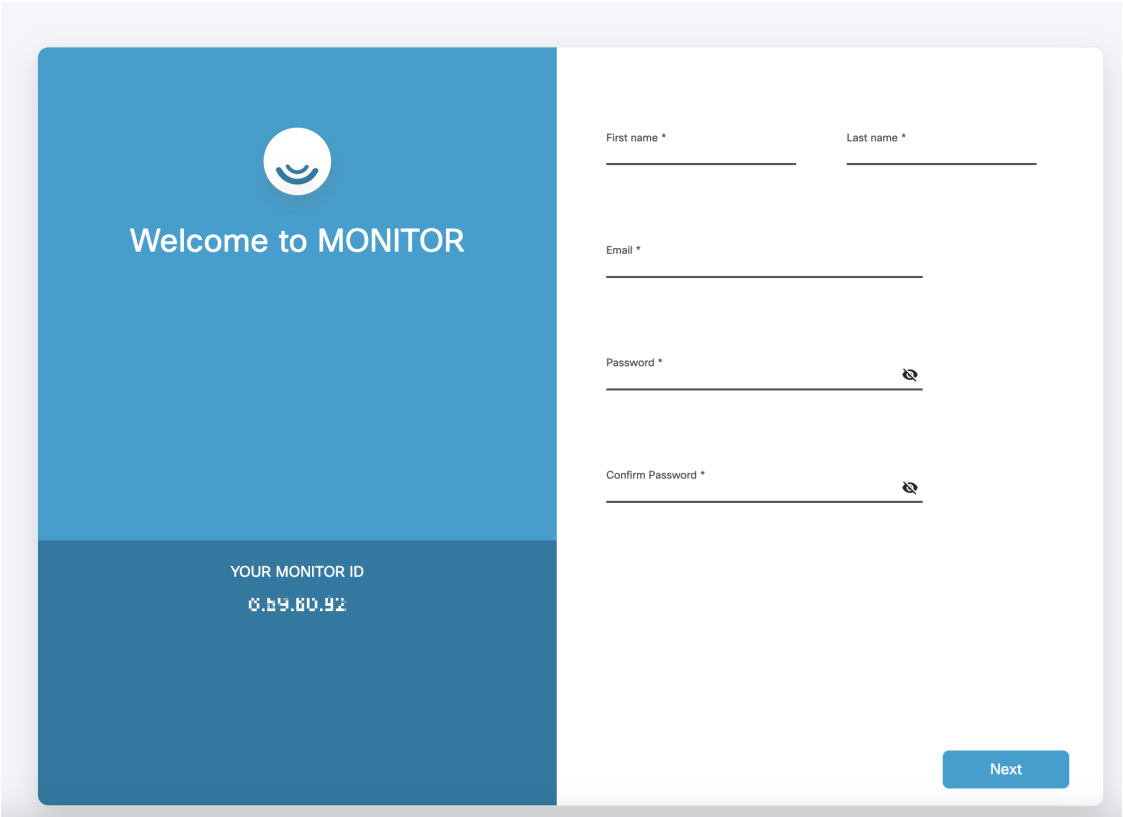
Step 1 Open the web browser.

Step 2 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, the following initialization page appears:

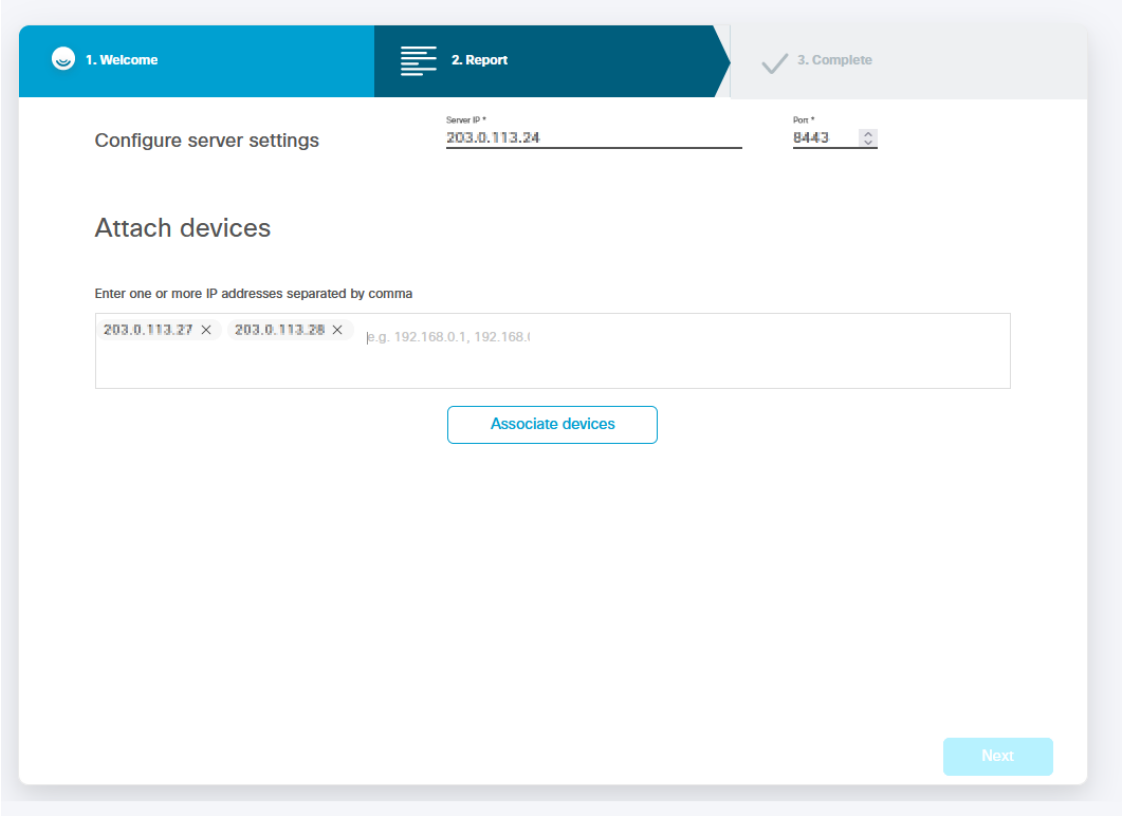


Step 3 Fill your first name, last name, e-mail address and login password in the respective fields.



Step 4 Click **Next**.

The **Add new device** screen appears.



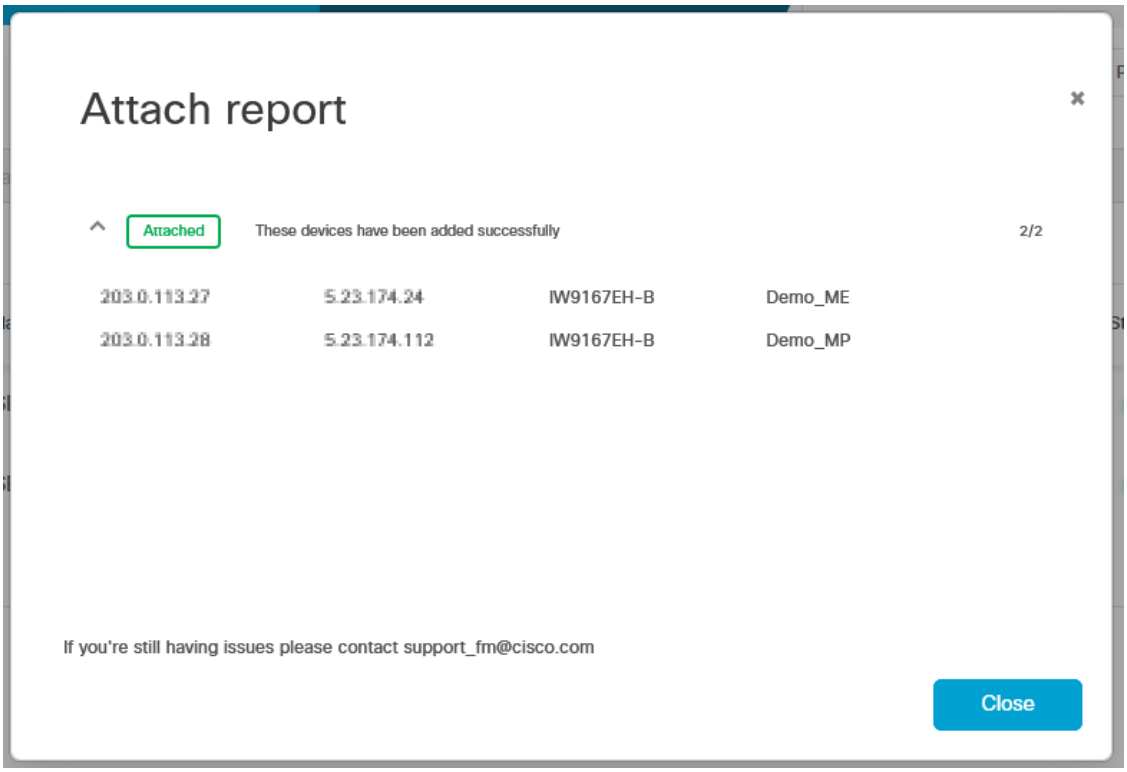
Step 5 (Optional) If required, fill the IP address of the IW Monitor server in the **Server IP** field and port number in **Port** field.

Step 6 Fill the IP addresses of all the devices that you want to monitor in the **IP addresses** field.

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

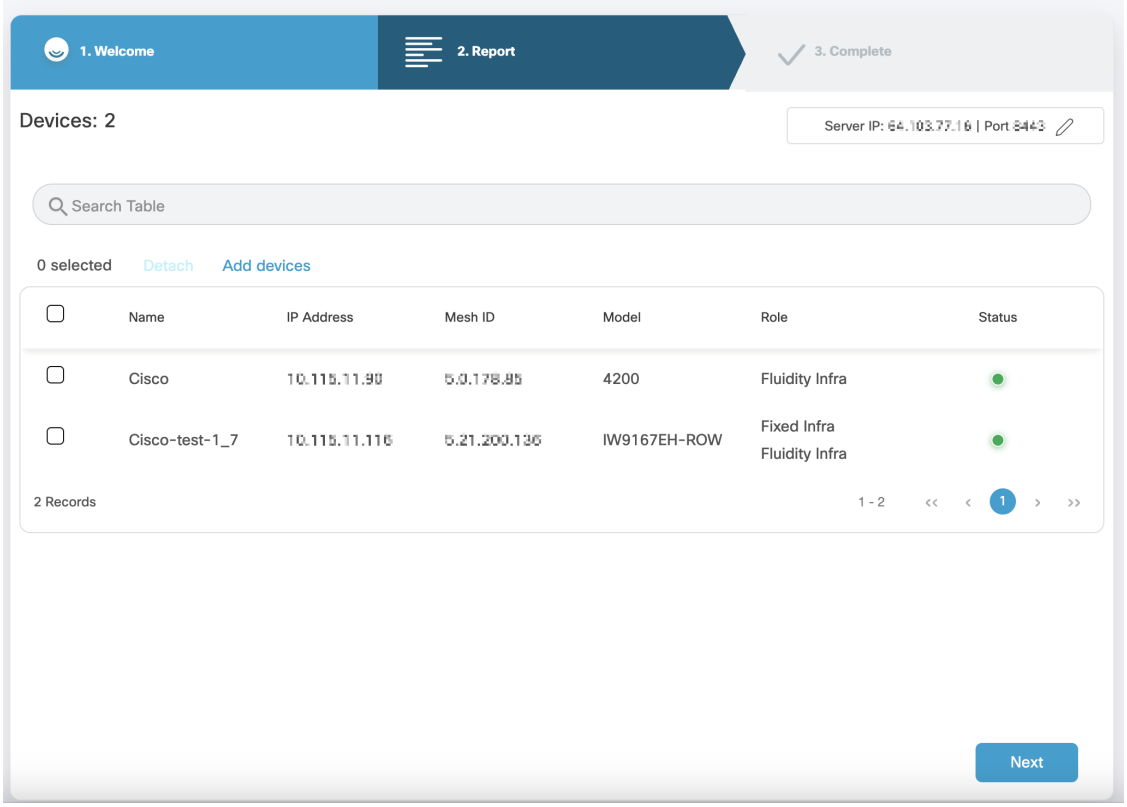
Step 7 Click **Associate devices**.

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



Step 8 Click **Close**.

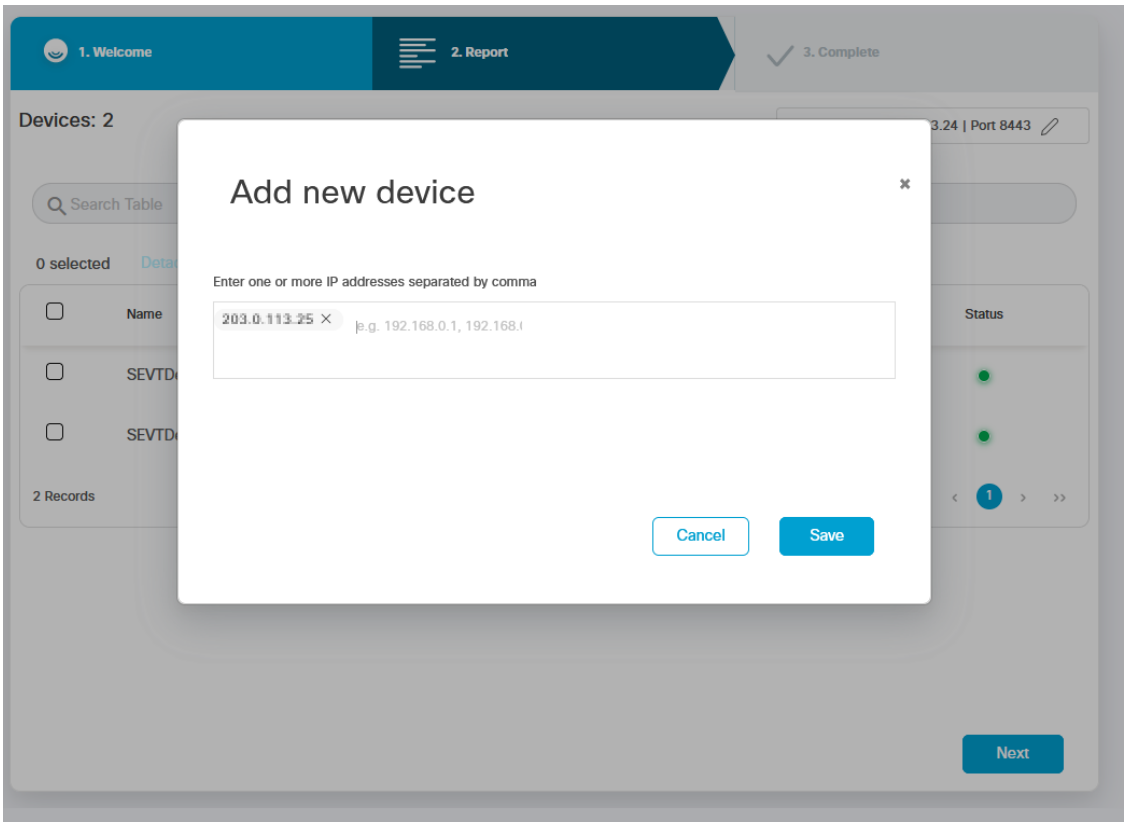
The list of devices associated with the IW Monitor interface are shown as below:



Step 9 Make sure that all the devices are listed on the screen. If any device is missing, follow the steps to add the device:

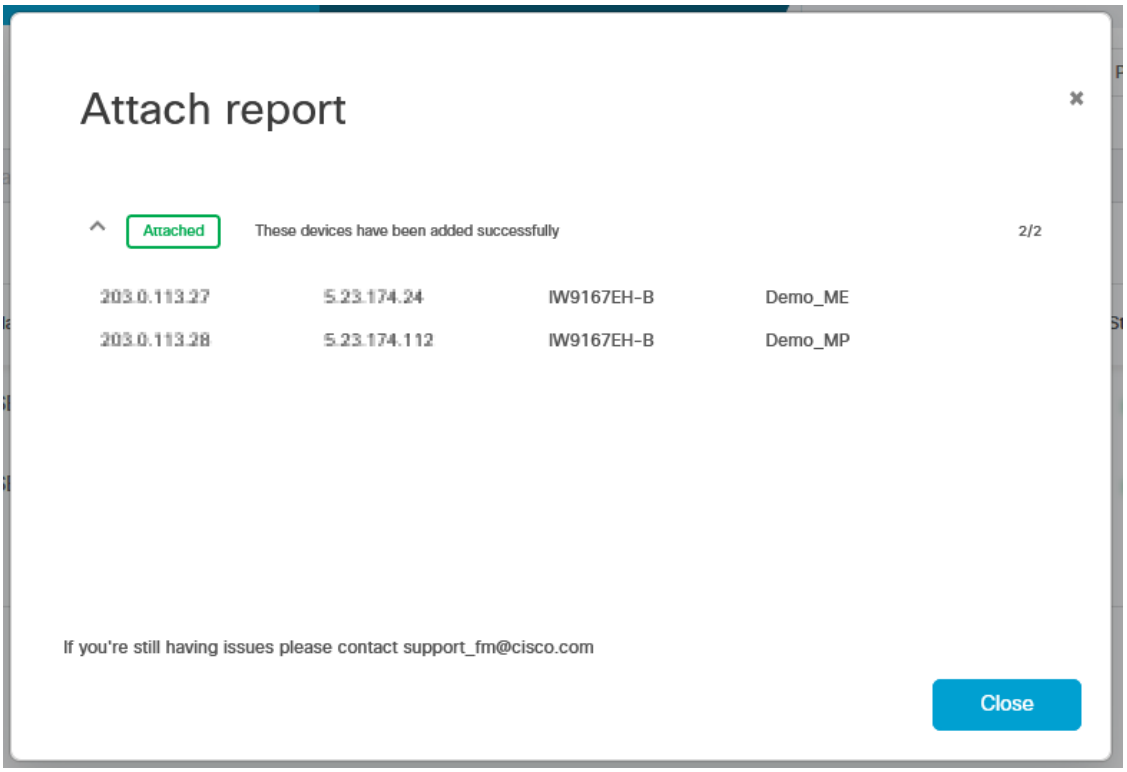
a) Click **Add Device**.

The **Add new device** screen appears.



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

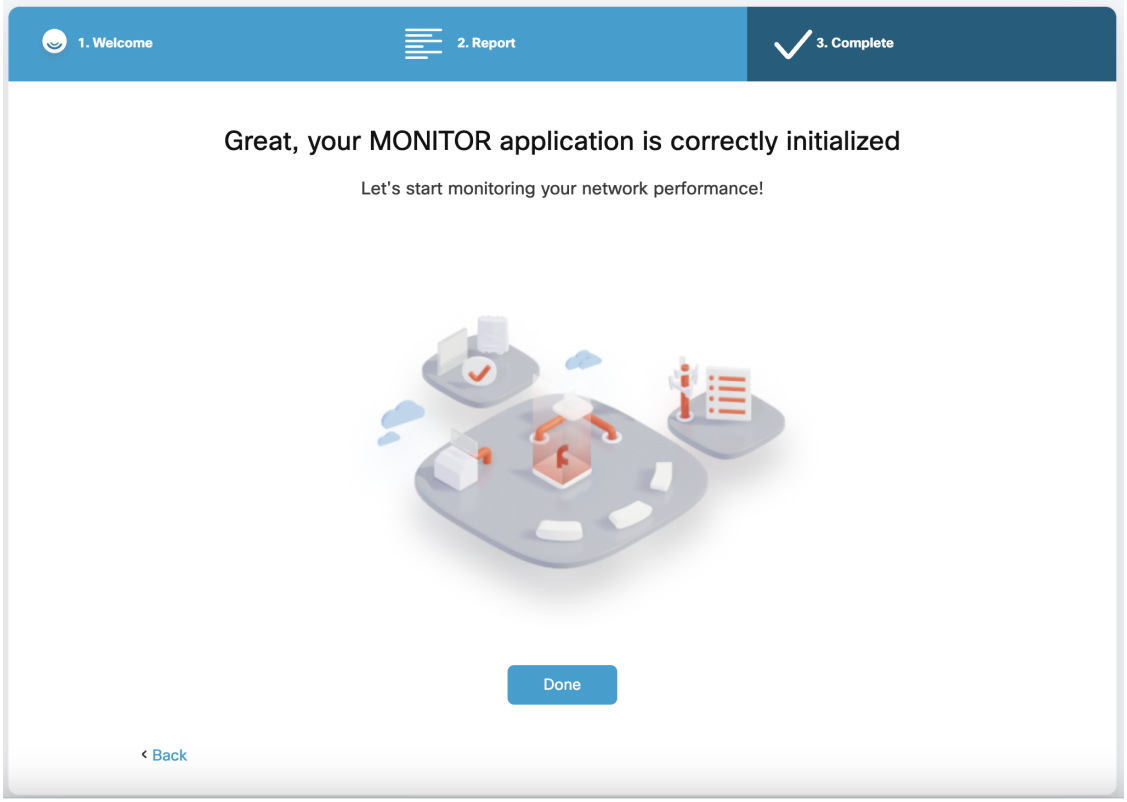
A confirmation screen appears showing that the devices are associated with the IW Monitor interface.



d) Click **Close**.

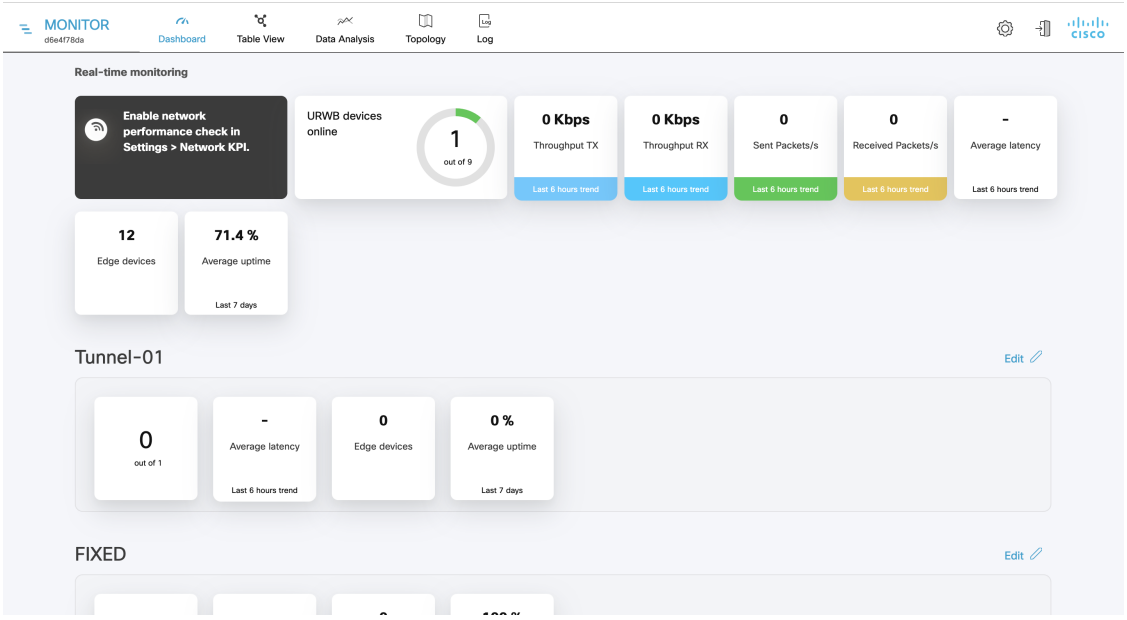
Step 10 Click **Next**.

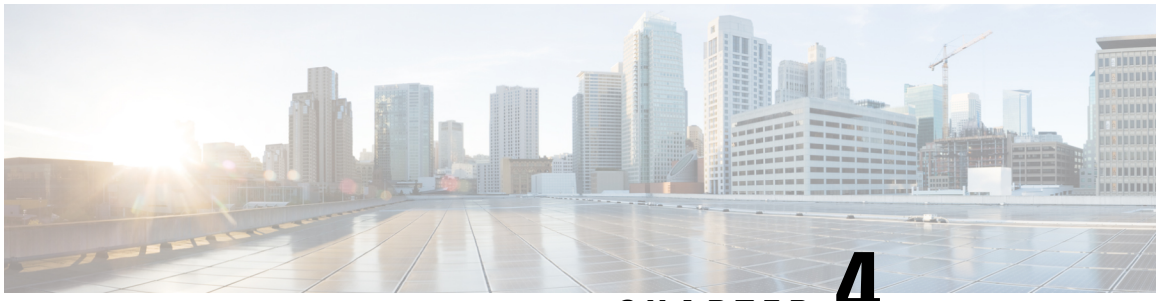
The IW Monitor analyzes the network and once the network analysis is complete and then the **Complete** screen appears:



Step 11 Click **Done** to complete the network setup.

The IW Monitor dashboard appears:





CHAPTER 4

Adding Devices to the IW Monitor

• Adding Devices to the IW Monitor, on page 19

Adding Devices to the IW Monitor

Step 1 Click on the **settings** icon at the top right.

A new settings screen is shown.

Step 2 Click **Devices**.

A table with the list of configured devices are shown.

Step 3 Click on the **edit** icon at the top right to configure the IP address of the main server of the network.

A pop-up appears.

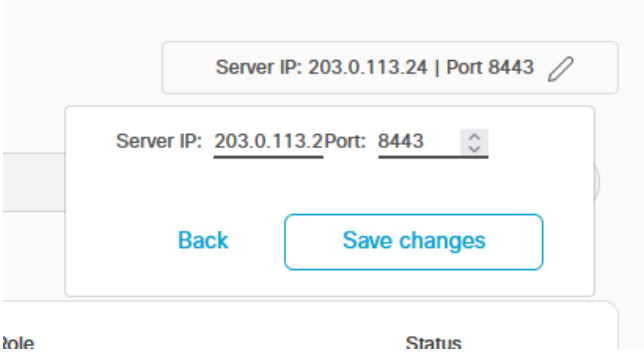
Step 4 If needed, add the server IP address in the **Server IP** field.

Step 5 If the IW Monitor host is configured to use HTTPS (secure socket layer) data transfer, enable the SSL.

Step 6 Fill the correct port number of the Docker container in the **Port** field.

For example:

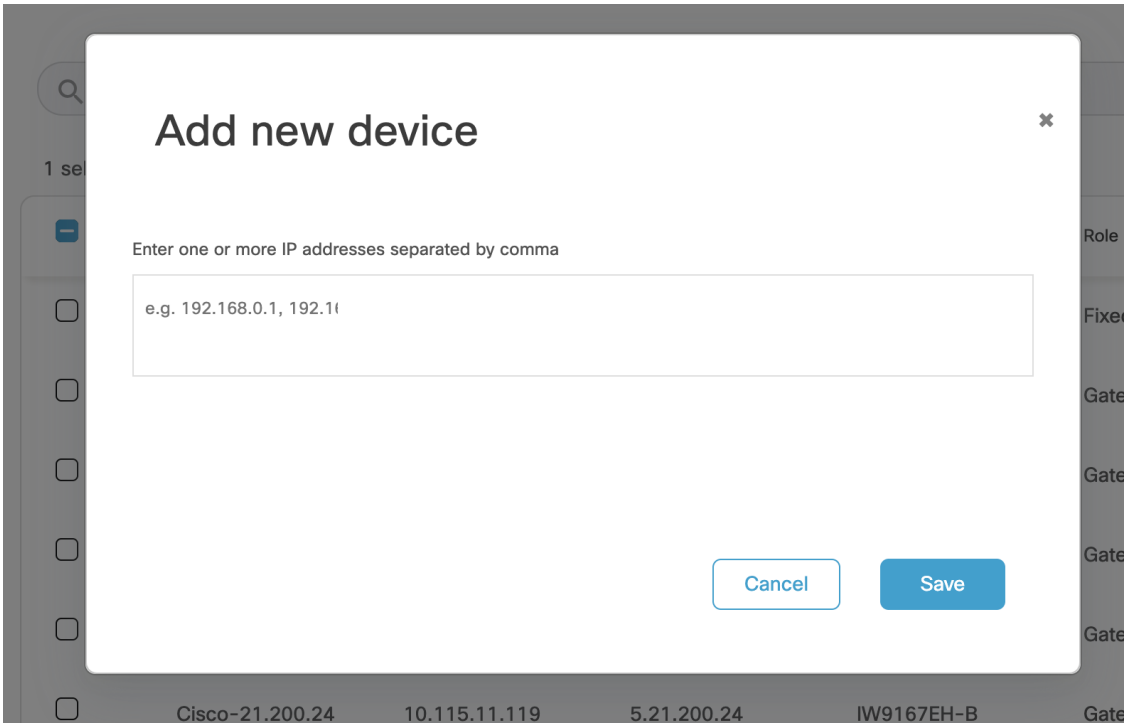
- **-p 8443:8443** maps to Port 8443
- **-p 443:8443** maps to Port 443
- **-p 3000:8443** maps to Port 3000



Step 7 Click **Save changes**.

Step 8 Click **Add Devices**.

A new pop-up **Add new device** appears to add the IP addresses of the devices.



Step 9 Add the IP addresses of the devices, separated by comma and a space. Alternatively, open an Excel file and add all the IP addresses in a column. Copy the whole column and paste it.

For example: 192.168.0.1, 192.168.0.2, 192.168.0.3

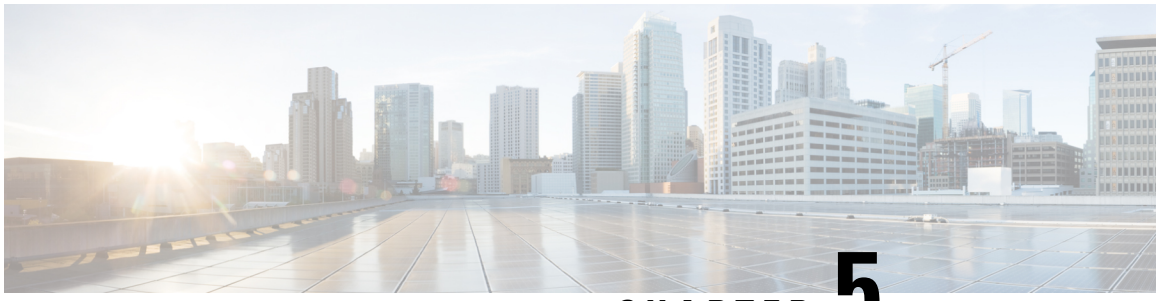
Note If the IP address is not reachable, an error shows that the devices failed to attach appears. Check if the IP address is correct and reachable and/or if any firewall is blocking.

If you try to add an already associated device, an error shows that the device failed to add.

Step 10 Click **Save**.

The newly added devices appear in the table.

Adding Devices to the IW Monitor



CHAPTER 5

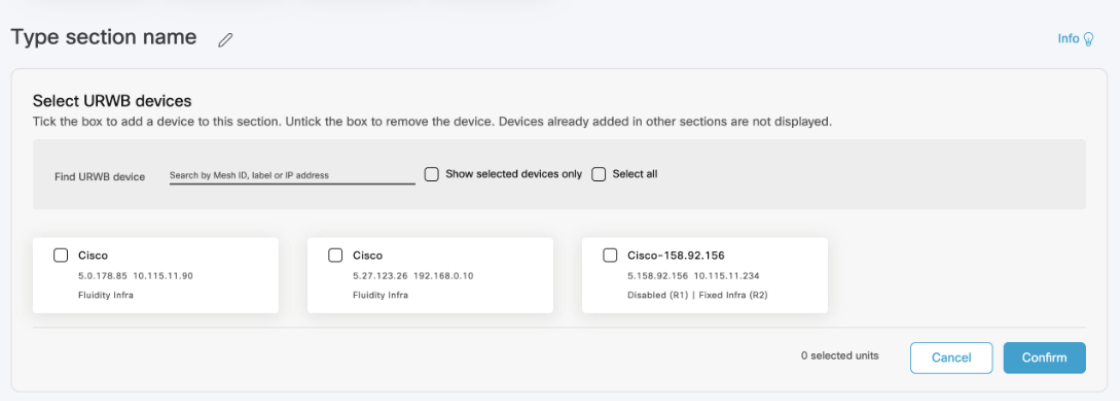
Managing Sections

- Creating a new Section, on page 23
- Editing a Section, on page 24
- Deleting a Section, on page 24

Creating a new Section

Step 1 Click the **+ ADD SECTION** at the bottom of the home screen.

A new screen appears as below:



Step 2 Click on the **edit** icon to add a name for the new section.

Step 3 Search for the device using the mesh ID number, assigned device name (label), or the device's IP address.

Step 4 Select the devices that you want to add to the section. You can also select the devices from the uncategorized list and check **Show selected devices only** checkbox.

The uncategorized devices are devices that are not yet assigned to any section. These uncategorized devices are shown independently as shown below.

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



Step 5 Click **Confirm**.

The selected devices are added to the new section.

Editing a Section

Step 1 Click on the **edit** icon of the section that you want to edit.

A detailed screen appears.

Step 2 Update the required fields like name of the section and/or list of devices.

Step 3 Click **Confirm**.

Deleting a Section

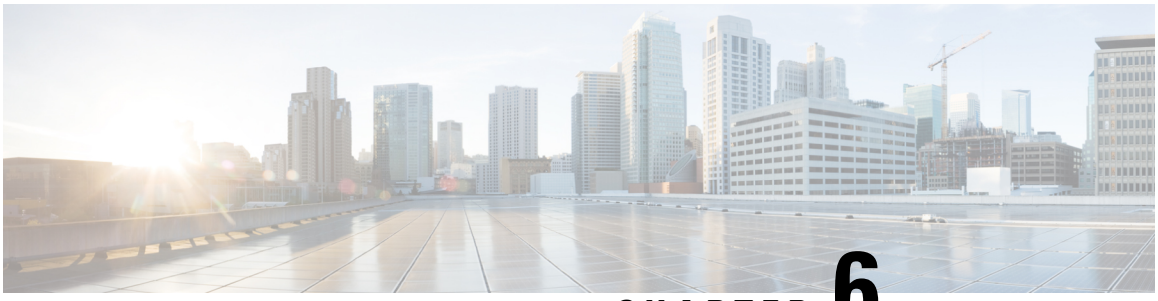
Step 1 Click on the **edit** icon of the section that you want to delete.

A detailed screen appears.

Step 2 Click Delete Section which is on the top right corner of the section.

A confirmation pop-up appears.

Step 3 Click **Delete**.



CHAPTER 6

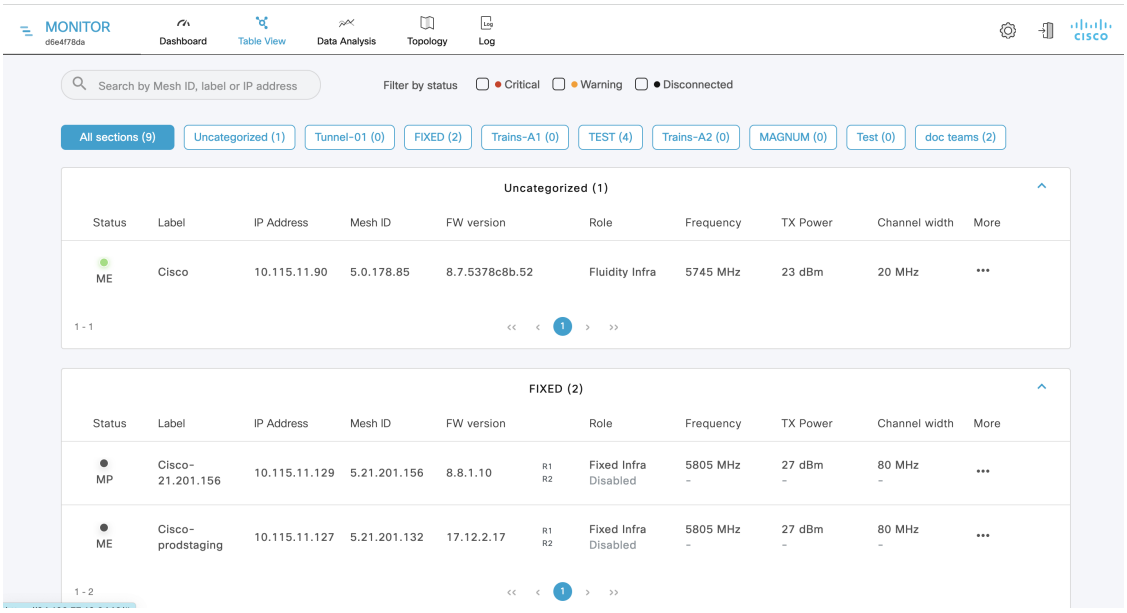
Managing Devices

- Editing the Device Configuration Parameters using Configurator Interface, on page 25
- Detaching the Device from the IW Monitor, on page 26

Editing the Device Configuration Parameters using Configurator Interface

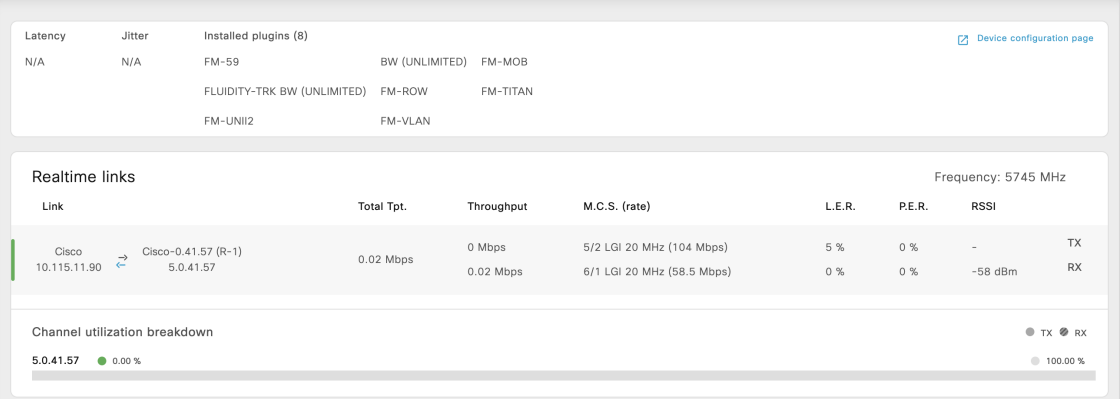
Step 1 Click **Table View** to see the list of devices.

A new screen as below appears:



Step 2 In the **More** column, click ••• of the device for which you want to edit the configuration parameters.

A detailed section appears:



Step 3 Click **Device Configuration page**.

The web browser opens a new page with a prompt to enter the device's user name and password.

Step 4 Enter the correct user name and password and click **Enter**.

The offline web interface (Configurator) opens for the device. To edit device configuration parameters using Configurator interface, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide.

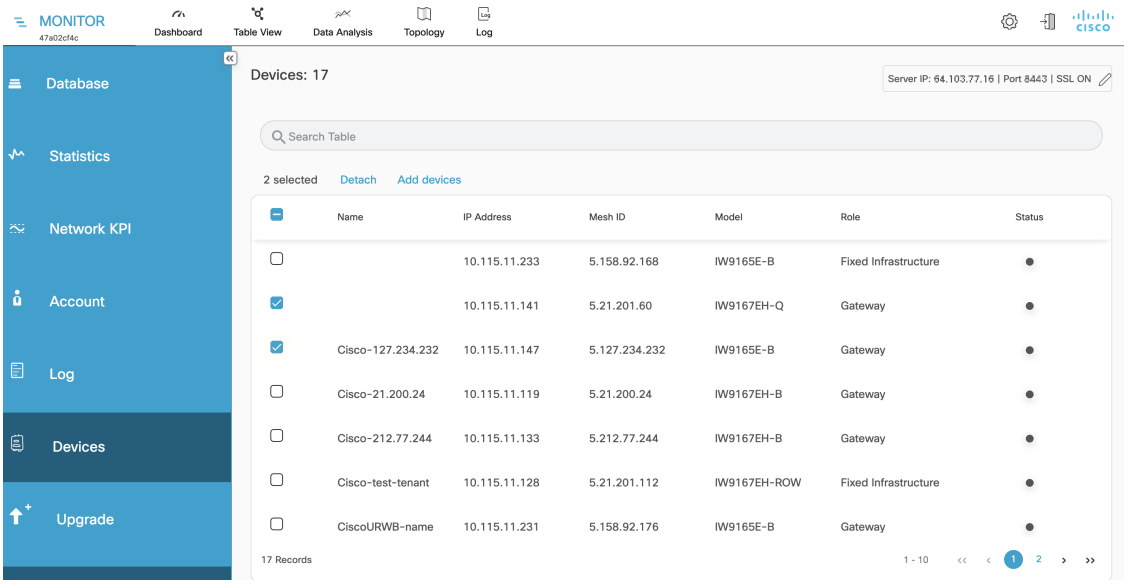
Detaching the Device from the IW Monitor

Step 1 Click on the **settings** icon at the top right.

A new settings screen is shown.

Step 2 Click **Devices**.

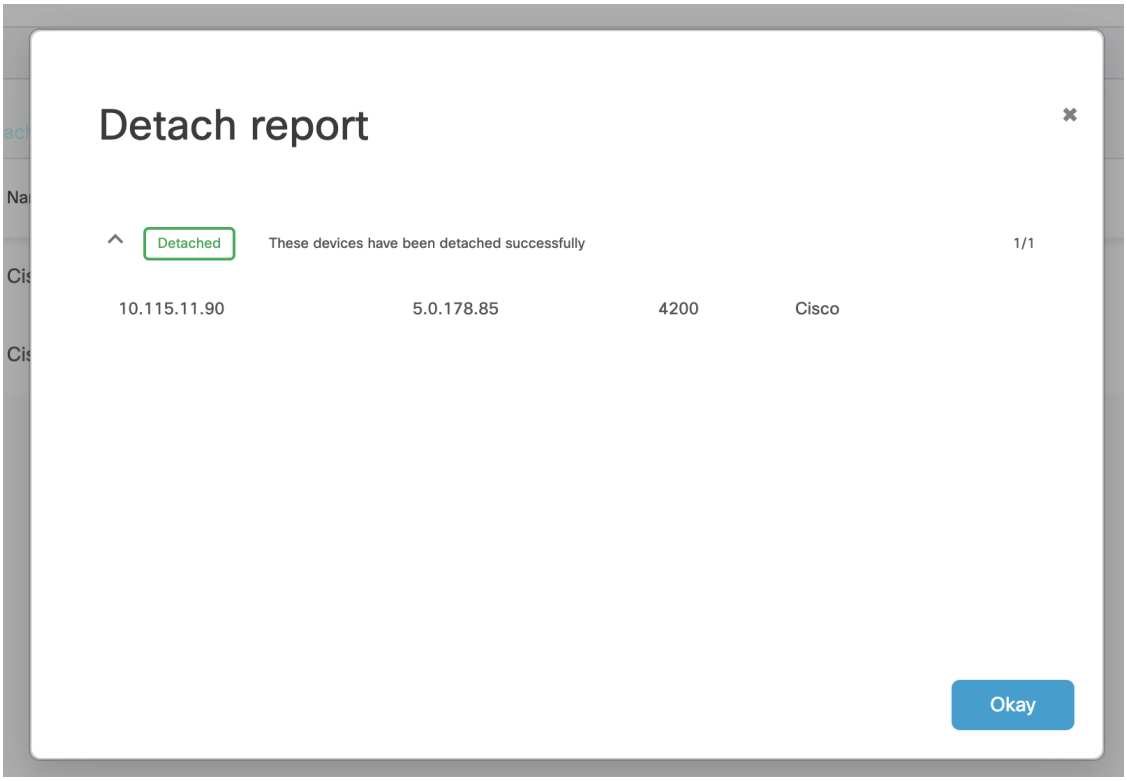
A table with the list of attached devices are shown.



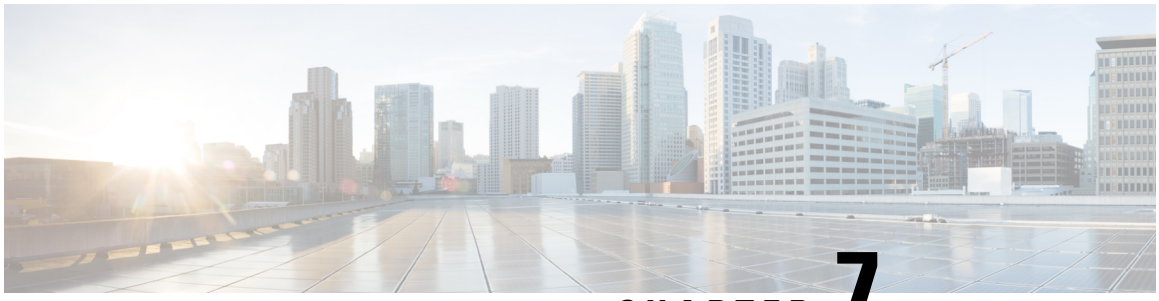
Step 3 Search for the device using the mesh ID number, assigned device name, device model, or the device's IP address. Or, select the device(s) you want to detach from the IW Monitor.

Step 4 Click **Detach**.

The selected devices are successfully detached with the following confirmation pop-up:



Step 5 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.

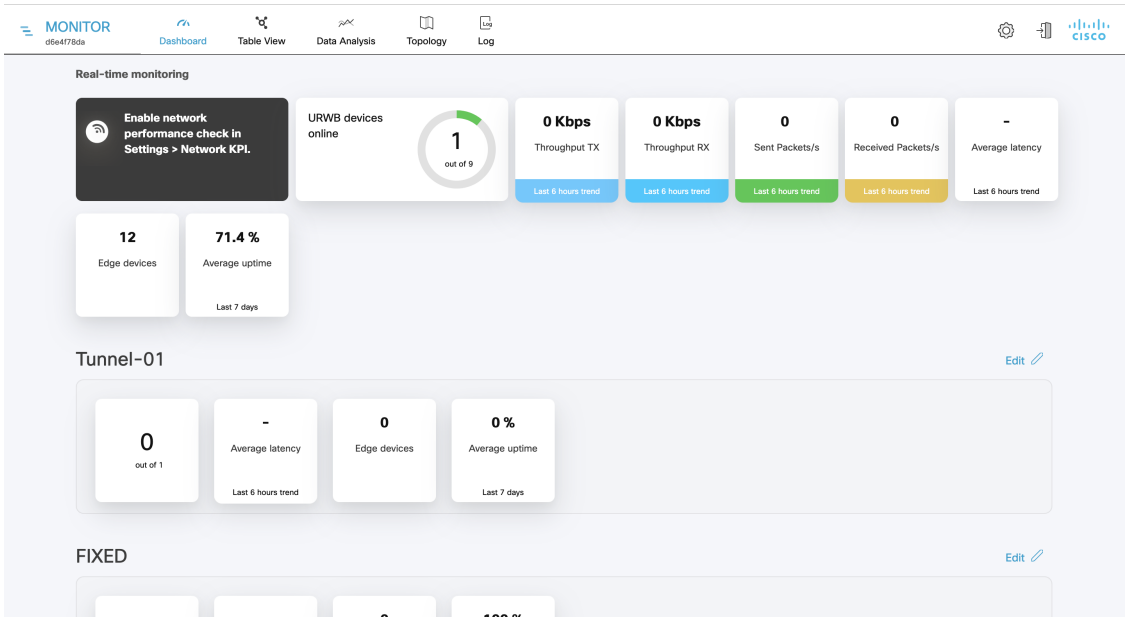


CHAPTER 7

Monitoring Network Performance

- Viewing the Network Statistics, on page 29
- Viewing the Devices using Table View, on page 30
- Viewing the Uplink and Downlink Information for a Device, on page 34
- Viewing Device Statistics in Real Time, on page 36
- Viewing the Devices from Topology, on page 39
- Filtering and Viewing Network Events, on page 43
- Exporting a Network Event Log as a CSV File, on page 45

Viewing the Network Statistics

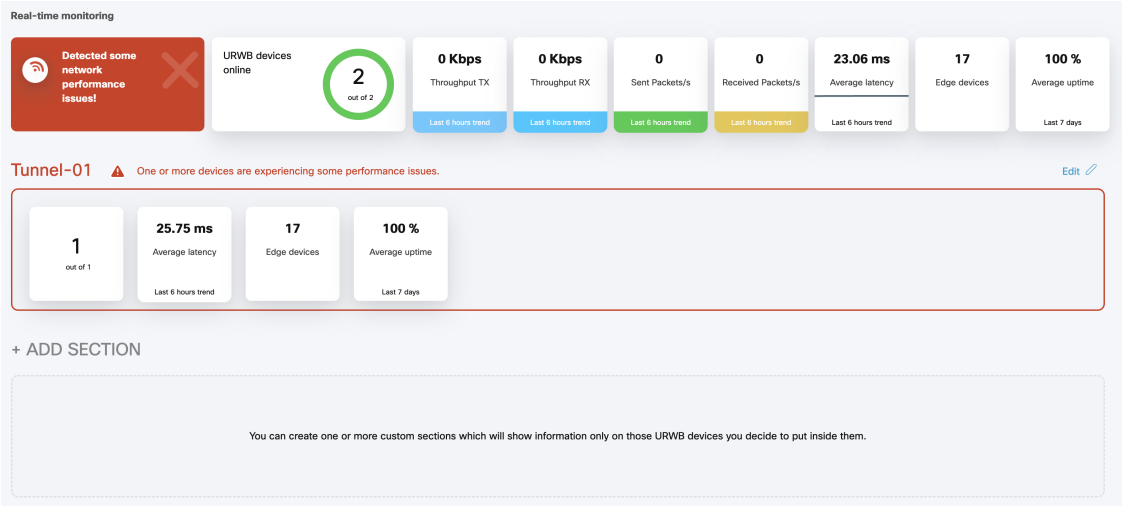


The real-time monitoring shows the performance of the combined network. Each box shows information about performance of a specified network section. In each network section, the blocks show operating parameters of the devices in the network such as:

- Number of devices currently connected to IW Monitor, in relation to the total number of devices associated to 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.

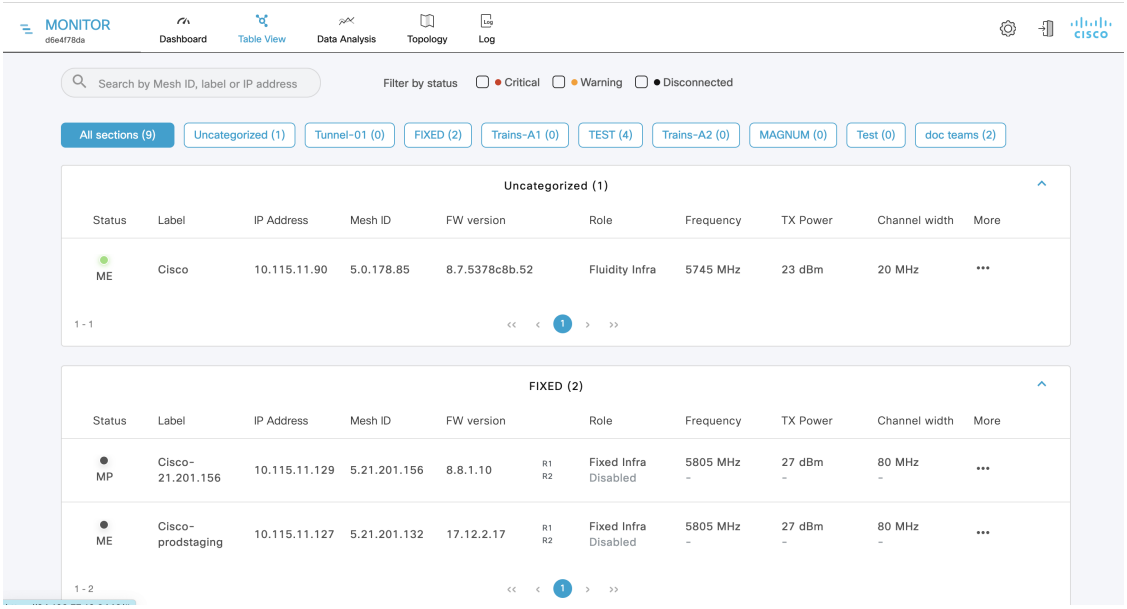
A thin red box appears around the section if any performance-related faults arise and need immediate investigation. The **+ ADD SECTION** at the bottom allows you to customize the section with the device information you want to monitor. To add a new section to an existing network, see Creating a new Section, on page 23.



Viewing the Devices using Table View

Step 1 Click **Table View** to see the list of devices.

A new screen as below appears:



- All the devices that are not assigned to any specific sections are shown under **Uncategorized**. To add uncategorized devices to a specific section, see Creating a new Section, on page 23.
- The devices that are assigned to specific network sections are shown in the relevant section.
- Following table describes each column:

Parameter	Description

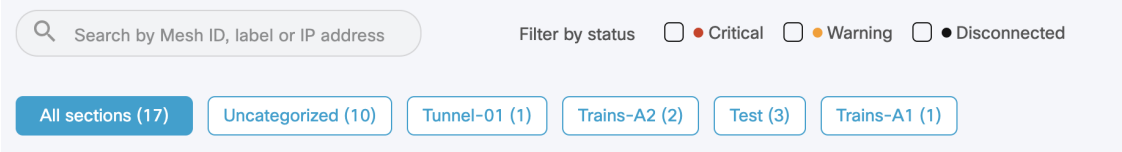
Status (icon color and designation)	Icon colors represent the following device status:
	• **Green**: Device is online and connected to an IW Monitor with all the performance levels in an acceptable range.
	• **Gray**: Device is disconnected from IW Monitor.
	• **Orange**: Device is online and connected to the IW Monitor but has one or more problems that cause it to perform at a lower-than-optimal level.
	• **Red**: Device is online and connected to IW Monitor but has one or more problems that cause unacceptably low performance. If a device icon is **orange** or **red**, the device may have one or more of the following problems:
	  • Unusually high packet error rate
	  • Unusually high link error rate
	  • Unusually low received signal strength
	  • Unusually high traffic latency
	
	Icon designation are as follows:
	• **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**: This is applicable only for FM PONTE devices.
	• **GGW**: Gateway is configured as a Global Gateway.

Label	This is the 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	Every device has a unique, factory set mesh identification number. for example: 5.a.b.c • If the device is set as the primary vehicle-mounted network device, then letter **P** is mentioned next to the Mesh ID. • If the device is set as a secondary device (a subordinate device within a vehicle-mounted network), then the letter **S** is mentioned next to the Mesh ID.
FW Version	Shows value of the firmware release number.
Role	Role designations represent the following device status: • **Fixed Infra**: Device is part of a fixed based infrastructure. • **Fluidity Vehicle**: Device is part of a Fluidity network, and installed in a moving vehicle. • **Fluidity Infra**: Device is part of a Fluidity network, and installed as part of a fixed infrastructure. **Note** For Cisco Catalyst IW9165 and IW9167 devices, the **Role** parameter is specified for each radio interface. If the radio interface is disabled, it shows as **Disabled**.
Frequency	Shows the device's current operating frequency. **Note** For dual-radio devices, the **Frequency** parameter is shown for each radio interface.
TX Power	Shows the user-defined value of the radio device's maximum transmission power level. **Note** For dual-radio devices, the **TX Power** parameter is shown for each radio interface.
Channel width	Shows the value of the radio device's operating channel width. **Note** For dual-radio devices, the **Channel width** parameter is shown for each radio interface.

Step 2 Search for any device using the mesh ID number, assigned device name, or the device's IP address.

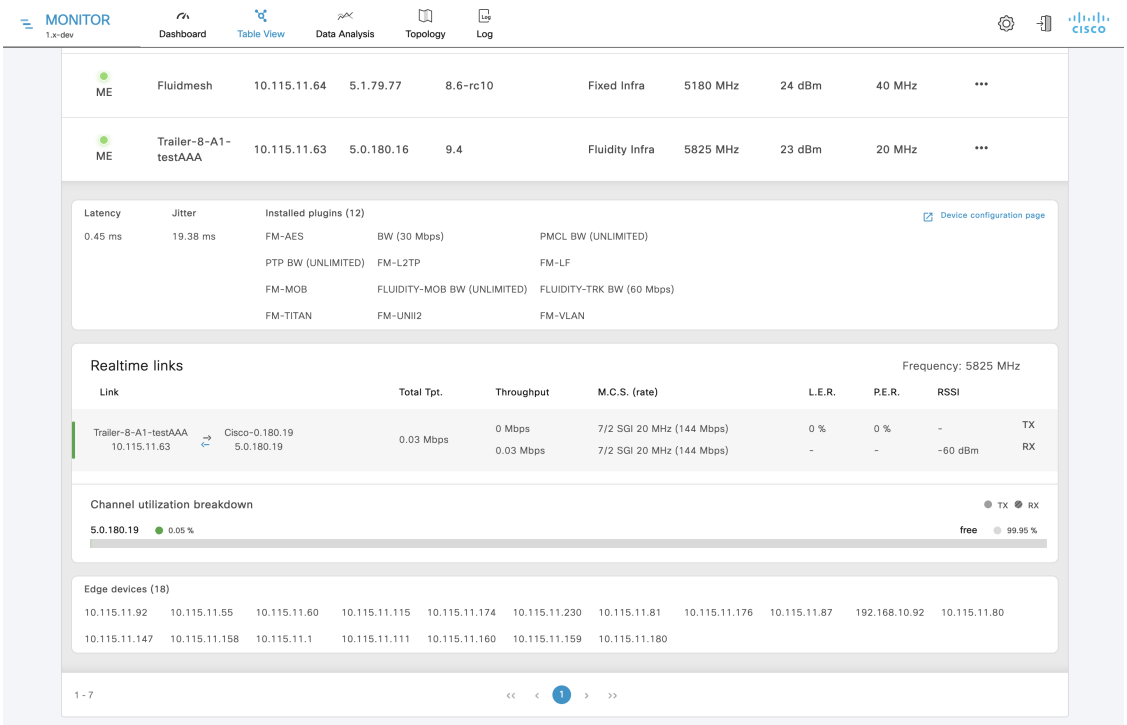
Step 3 Or, filter the devices based on status such as **Critical**, **Warning**, **Disconnected**. Also, you can select the tabs for a quick view of the section.



- The **Critical** filter allows you to view the list of devices for which the thresholds are beyond the upper threshold limit.
- The **Warning** filter allows you to view the list of devices for which the thresholds are between the upper and lower threshold limits.
- The **Disconnected** filter allows you to view the devices which are disconnected from IW Monitor.

Viewing the Uplink and Downlink Information for a Device

In the **More** column, click (**…**) of the device to view more detailed uplink and downlink information.



Following table describes each column with detailed explanation:

Parameter	Description
Installed plugins	List of the software plug-ins currently installed on the device, and it is only applicable for the legacy Fluidmesh products.
License	Shows the device's license level and is applicable only for Catalyst IW9165, IW9167, and IEC-6400 gateway. The **License** level can be **Essential**, **Advantage**, or **Premier**.
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).
Link	Shows the two endpoints of the wireless link.
Role	Role designations are as follows: • **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.
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.

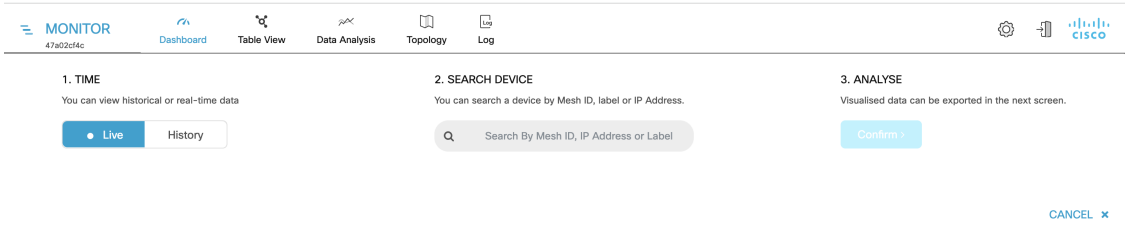
Parameter	Description
Channel utilization breakdown	• The total width of the bar represents the total bandwidth of the channel carrying the uplink and downlink. • The solid portion represents the portion of bandwidth currently being used to transmit data. • The striped portion represents the portion 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 also given for transmission, reception and non utilization.
Attached devices	This is a list of devices that are part of the section.

Viewing Device Statistics in Real Time

IW Monitor has network statistics that allow you to view the network-related performance of any device in the current network. The statistical details for a device can be viewed in real-time as they occur. You can also view a performance graph that displays the device's previous performance on a historical timeline.

Step 1 Click **Data Analysis**.

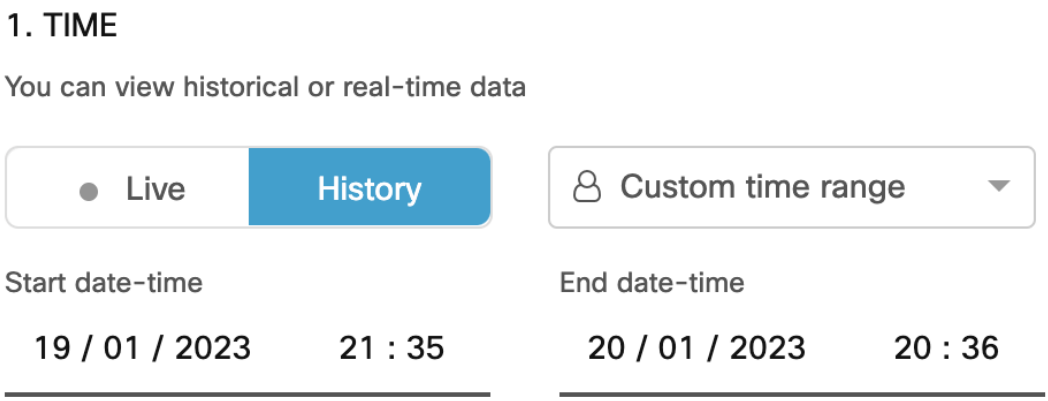
A new screen extends as shown below:



Step 2 For step 1: **TIME**, you can switch between real (live) and historical data for the data analysis.

a) To view statistics of a device for a particular period, select **History** tab.

From and **To** time fields and **Custom time range** field appears.

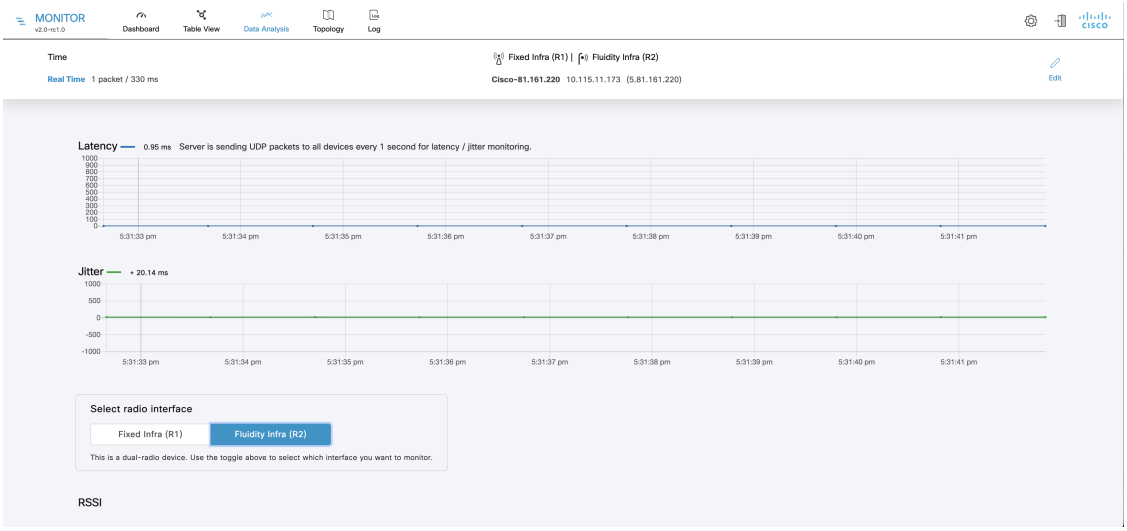


b) Select the date and time for both **From** and **To** fields.

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

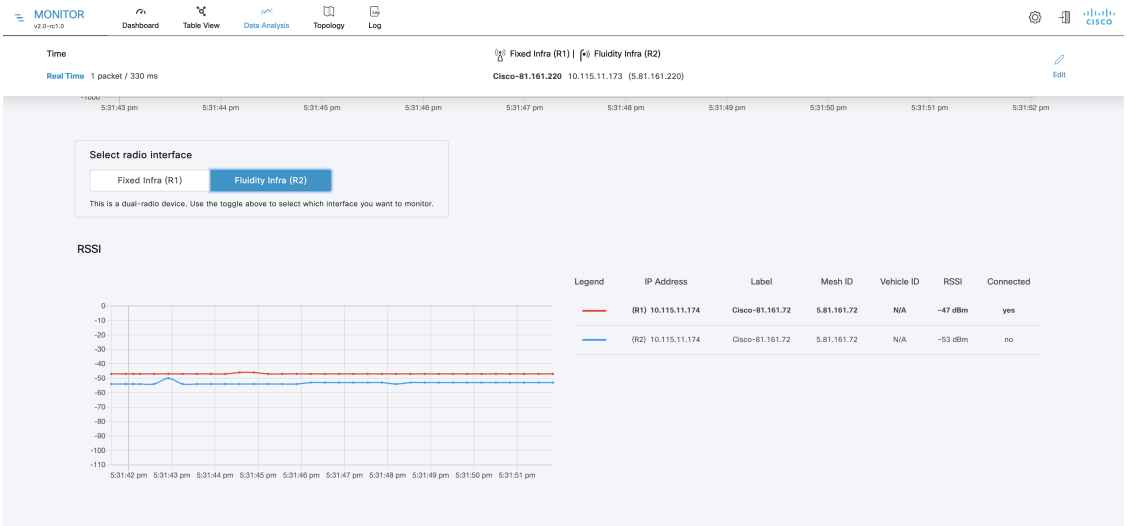
Step 3 For step 2: **SEARCH DEVICE**, search for the device using the mesh ID number, assigned device name, or the device's IP address.

Step 4 For step 3: **ANALYSE**, click **Confirm**.



A real-time statistical view of the device appears. For **History** tab selection, a time slider for the chosen period also appears.

a. The first graph shows received signal strengths of the device and other radio units that the device could potentially connect with:

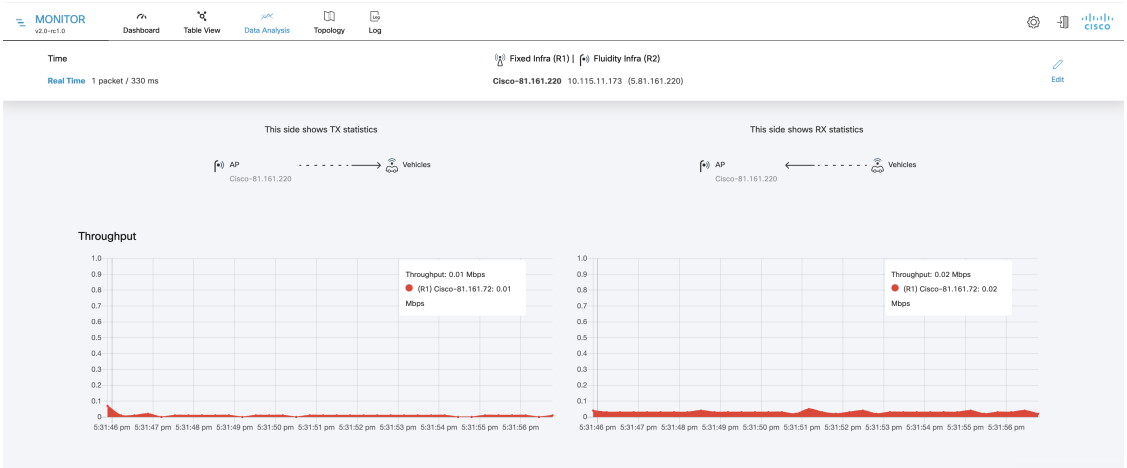


- The upper left corner of the graph shows whether the device currently accepts handoff requests.
- If the chosen device is currently connected to a Fluidity-enabled (vehicle-mounted) radio unit, a thick, dashed black line is superimposed over the Fluidity device's RSSI line. This line is the RSSI envelope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

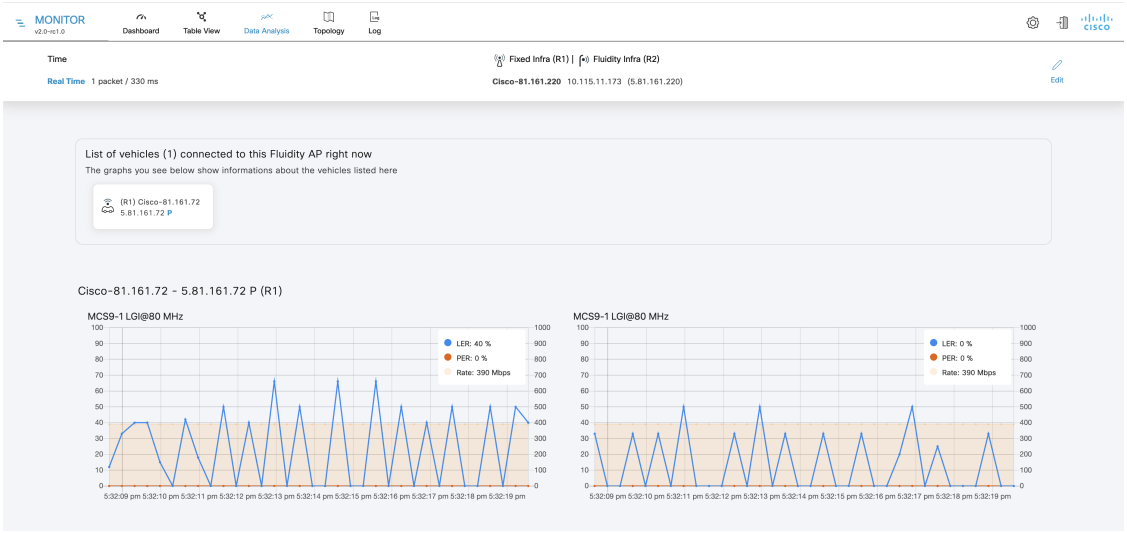
b. The Throughput graphs show the throughput statistics as a function of Mbps/time. The throughput is shown for the selected device and the device to which the chosen device is currently connected.

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 shows the current link error and packet error rates (expressed in percentages over time) and the comparative signal modulation rates. LER and PER are shown for the selected device and the device to which the selected device is currently connected.

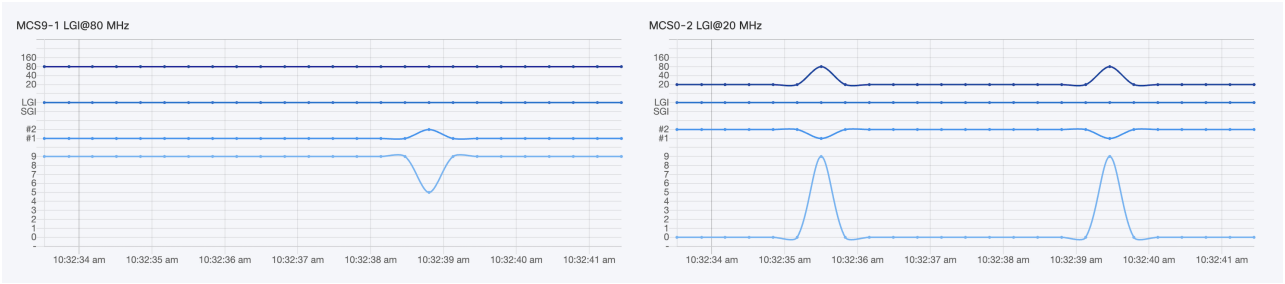
Note The left graph shows uplink statistics (data flow from the current device), while the right graph shows downlink statistics (data flow to the current device).



d. The graphs in the fourth row shows the modulation and coding schemas (MCS) for the selected device and the device to which the selected device is currently connected.

Note The left graph shows uplink statistics (MCS of the current device), while the right graph shows downlink statistics MCS of 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.



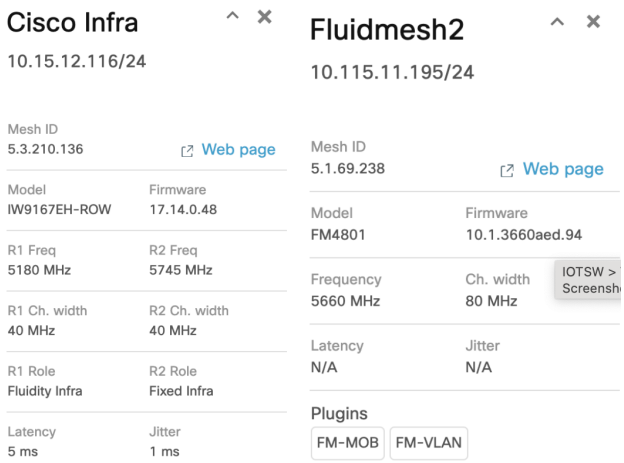
Note This graph is shown only for vehicles.

Step 5 Click **Edit** to view the statistical view for another device.

Viewing the Devices from Topology

Step 1 Click Topology **Topology**.

Step 2 Click on the device for more details.

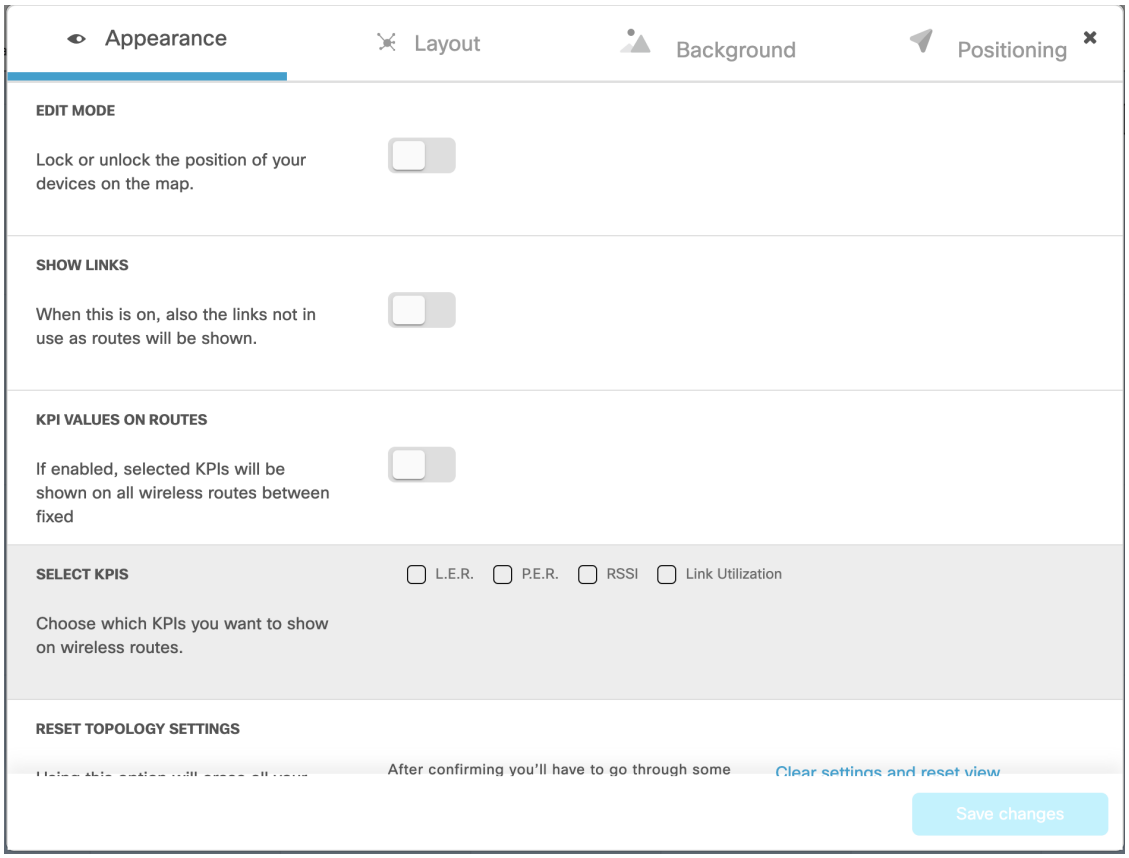


Step 3 Click on **Web page** and it redirects to the respective web interface (Configurator) of the device.

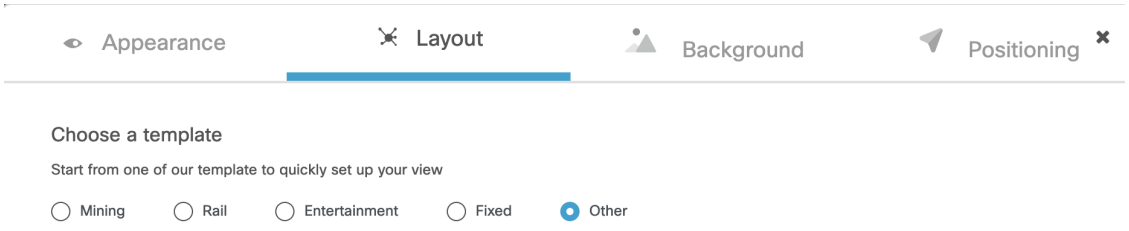
Step 4 Click **Settings** to change the information displaying in the topology view:

a) In the **Appearance** tab, you can edit the following:

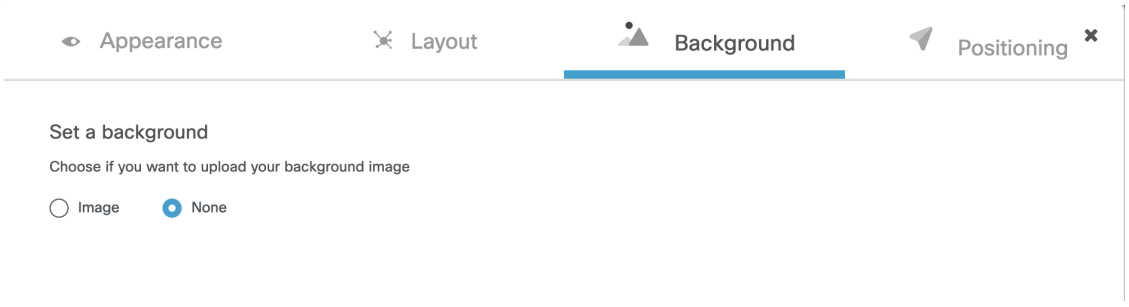
- **EDIT MODE**: The toggle button allows you to lock or unlock the position of any device on the topology map.
- **SHOW LINKS**: If the toggle button is enabled, the links not in use as routes are shown.
- **KPI VALUES ON ROUTES**: If the toggle button is enabled, the selected KPIs (**L.E.R**, **P.E.R**, **RSSI**, and **Link Utilization**) mentioned below will be shown for all wireless routes.
- **RESET TOPOLOGY SETTINGS**: Click **Clear Settings and reset view** to clear all the topology settings.



b) In the **Layout** tab, you can choose a predefined template to set up the view based on the use case.

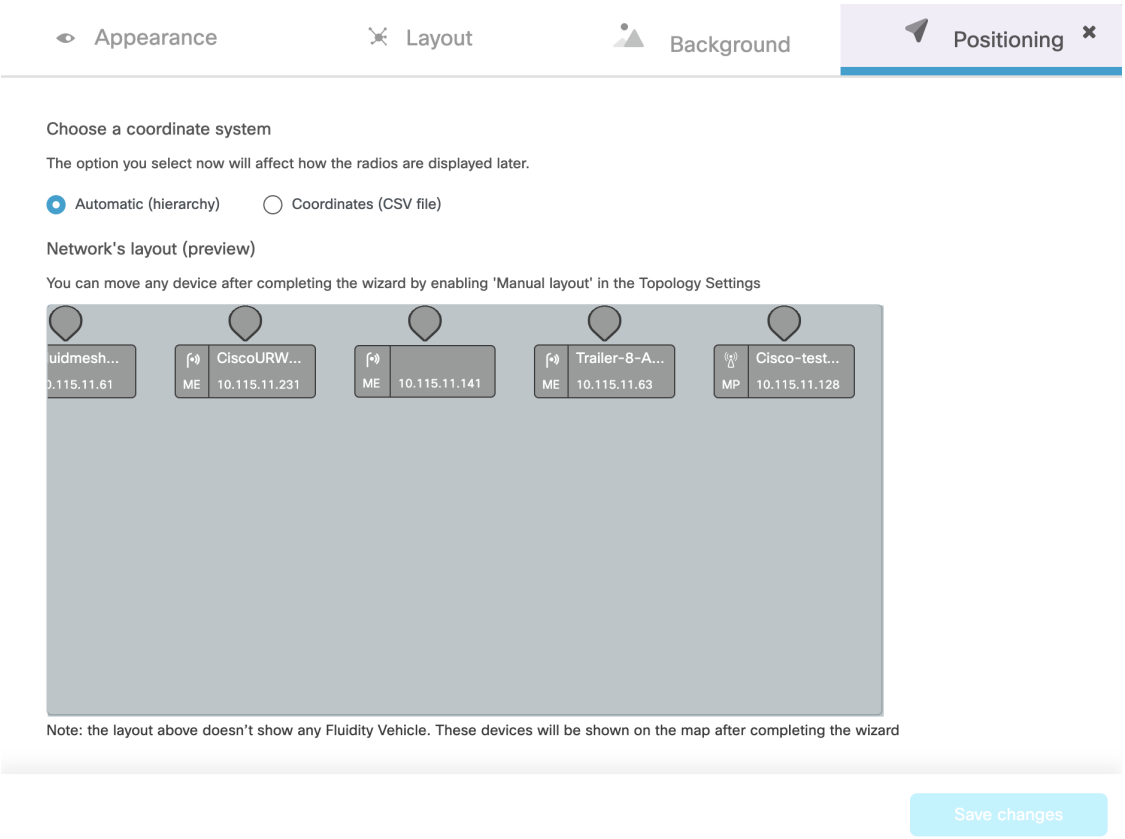


c) In the **Background** tab, you can customize the background of the topology view.



d) In the **Positioning** tab, you can choose between the two below options:

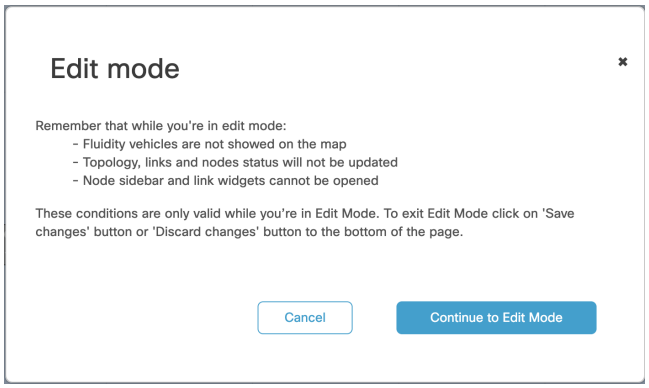
- **Automatic (hierarchy)** - Allows the devices to automatically positioned as a tree.
- **Coordinates (CSV file)** - You can upload a CSV file with the list of coordinates for each device (latitude and longitude). Then, position any two devices in the panel and all the other devices will be automatically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



Step 5 Click **Edit Mode** to change the topology view based on devices or background.

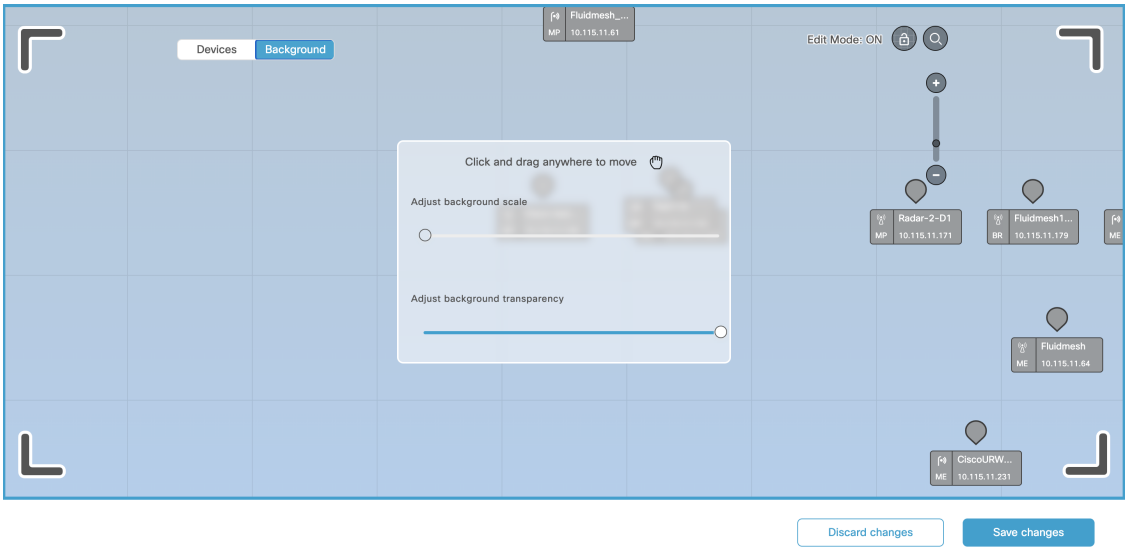
The following pop-up appears once you click on **Edit Mode**:

a) Click **Continue to Edit Mode**.



- 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.



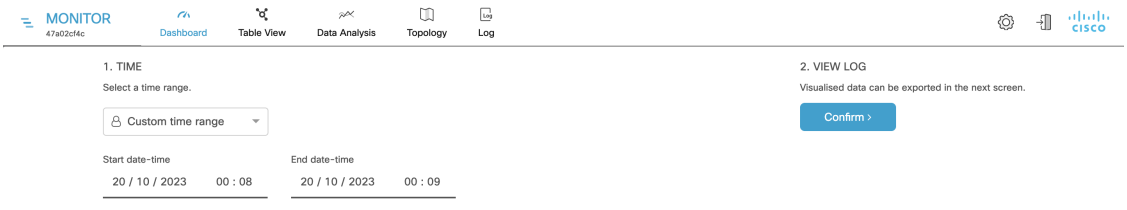
b) Click **Save changes**.

Step 6 Click **Zoom** to zoom in/out the topology view.

Filtering and Viewing Network Events

Step 1 Click Log to view a log of network events for the current device.

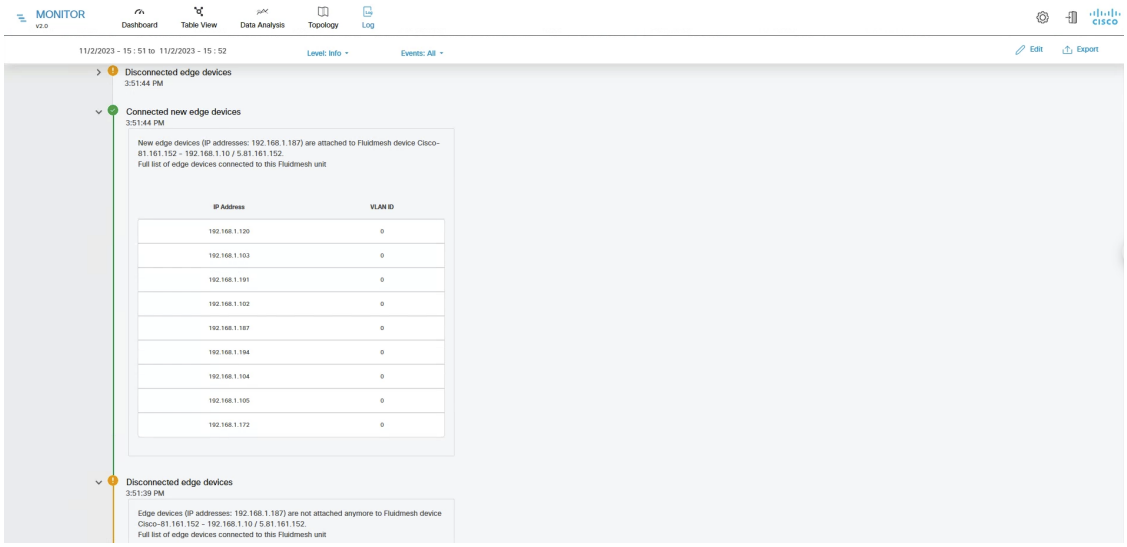
A new screen extends as shown below:



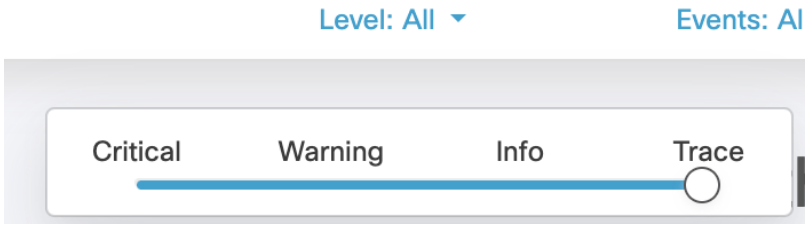
Step 2 For step 1: Select the available time range options from the **Custom time range** drop-down list or set the start date and time and end date and time as required.

Step 3 For step 2: Click **Confirm**.

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



Step 4 If required, click **Level** to choose the overall criticality level of the shown list of network events.



The levels are as below:

- **Critical** - Critical level events have an immediate, negative impact on system performance and/or 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.

Note Criticality levels are inclusive of the chosen level, and all levels below the chosen level. For example:

- If you select **Critical**, only **Critical** events are shown.
- If you select **Warning**, then **Critical** and **Warning** events are shown.
- If you select **Info**, then **Critical**, **Warning** and **Information** events are shown.
- If you select **Trace**, then **Critical**, **Warning**, **Information** and **Trace** events are shown.

Step 5 Choose the specific network event types as below:

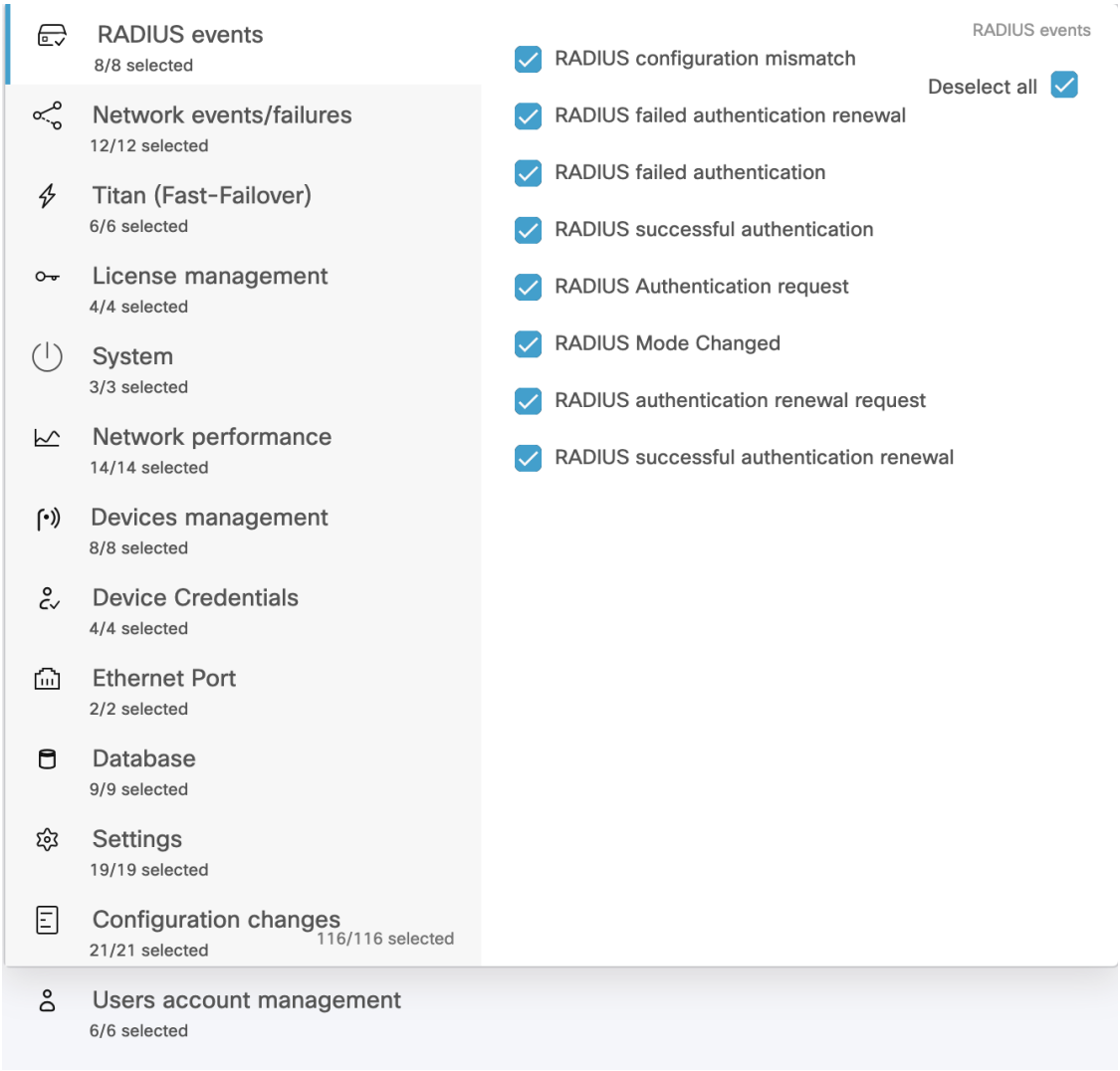
a) Click **Events**.

A pop-up appears.

b) In the pop-up, click the relevant category from left pane, and select the check-boxes for the required network event.
c) Click **Apply**.

All the specified network-related events are shown in descending chronological order (more recent events are shown at the top of the log).

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



Exporting a Network Event Log as a CSV File

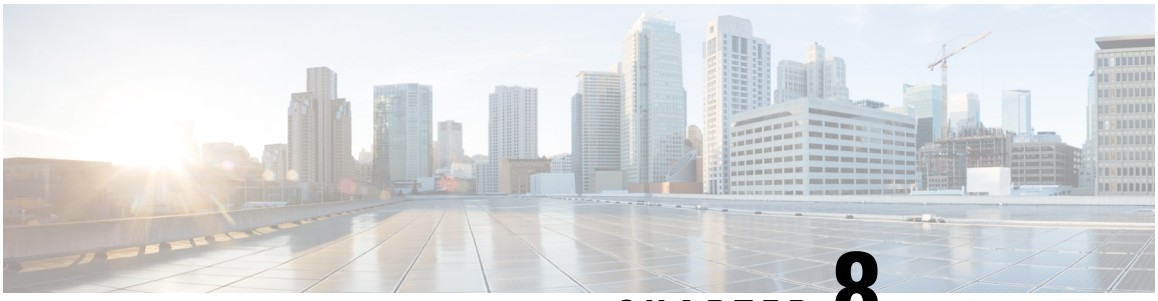
Step 1 Request the log of network events as mentioned in Filtering and Viewing Network Events, on page 43.

Step 2 Click Export.

A **Export Log** pop-up appears.

Step 3 Check the date/time range shown in the **Export Log** pop-up, and click **Export**.

Step 4 Select the location in your computer to save the file.



CHAPTER 8

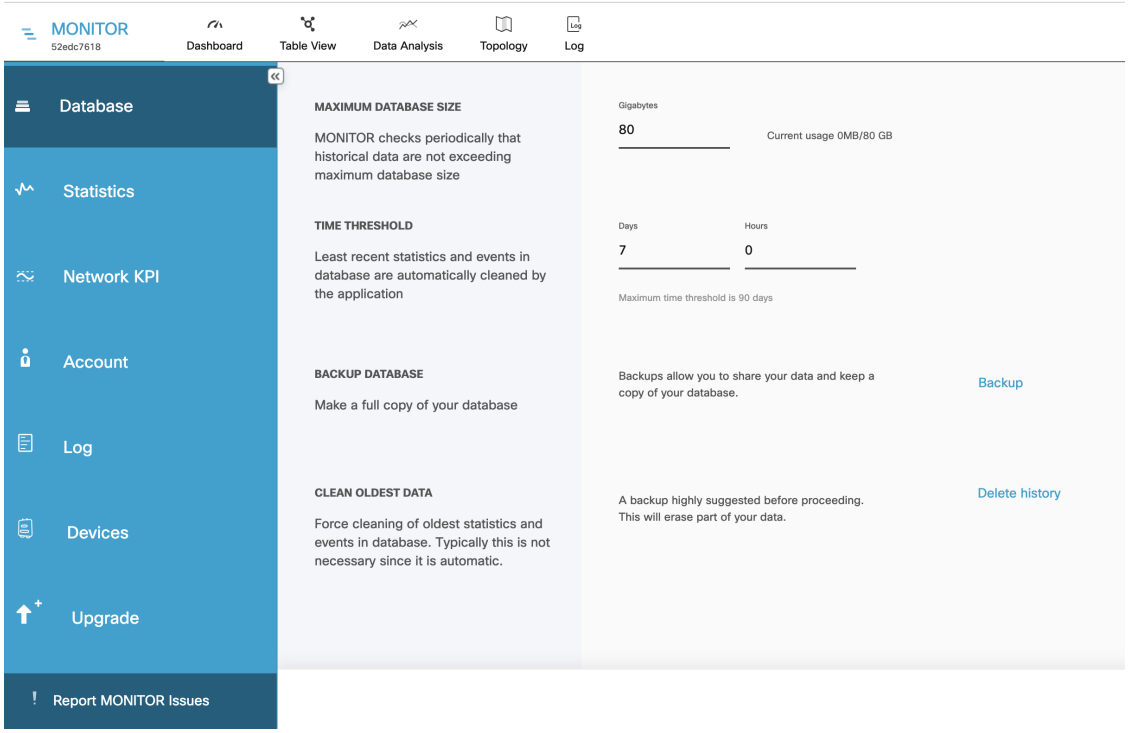
Configuring IW Monitor Database Settings

- Defining Hard Disk Storage Capacity and Overwrite Cycle Period for the IW Monitor Statistics Database, on page 47
- Backing up the IW Monitor Statistics Database, on page 49
- Deleting the recent IW Monitor Statistics Data, on page 50

Defining Hard Disk Storage Capacity and Overwrite Cycle Period for the IW Monitor Statistics Database

Step 1 Click **Settings** in the top right corner.

The database settings page is shown.



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

The IW Monitor periodically checks the historical data is within this defined maximum database value.

Important The allocated hard disk space cannot be less than the amount of currently occupied hard disk space or more than the hard disk's total capacity.

Note If the amount of network statistics data currently stored on the hard disk reaches the specified value but is recorded over less than the time specified by the **TIME THRESHOLD** value, the IW Monitor will overwrite the old data with the new data in real-time.

It is highly recommended that you use a hard disk of at least 100 GB capacity for network statistics storage. If you must use a hard disk of less than 100 GB capacity, assign no more than 75% of the drive's free capacity to network statistics storage. IW Monitor may encounter performance issues if you assign more than this amount.

Step 3 Set the **TIME THRESHOLD** value manually.

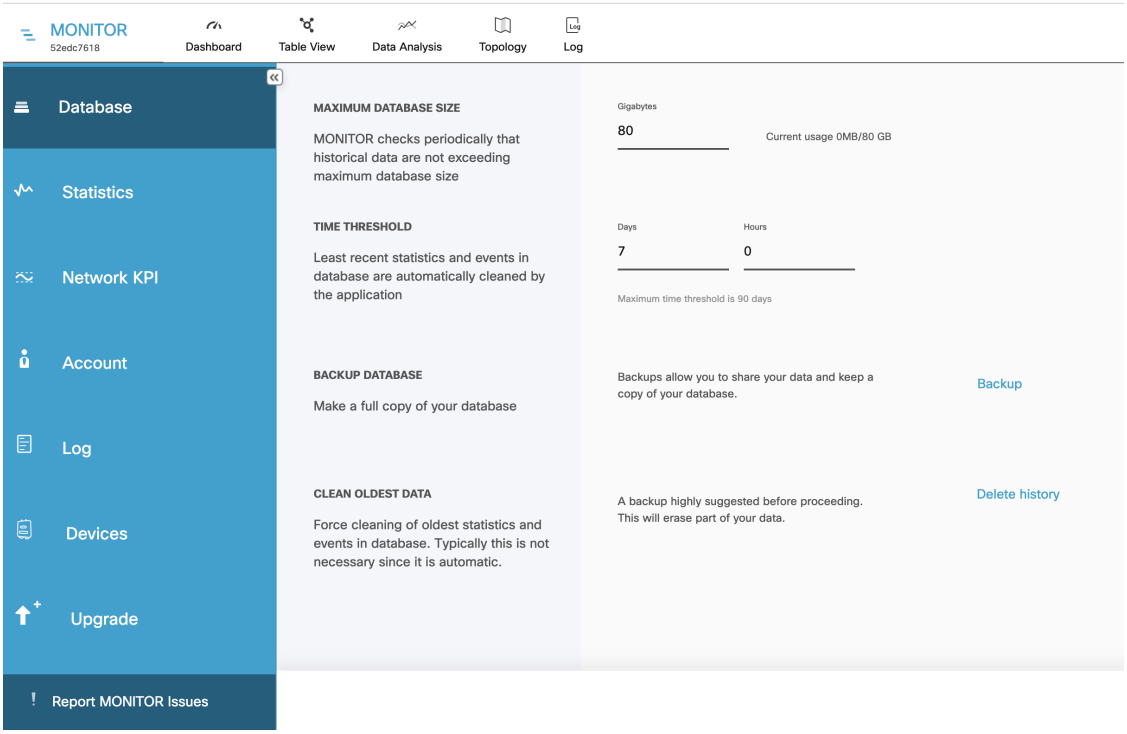
The time threshold shows the time period for which network statistics are recorded before the old statistics data is overwritten.

Note The minimum amount of time-related network-statistics data that can be stored before overwrite is one hour, and the maximum amount of time-related data that can be stored before overwrite is 90 days.

Backing up the IW Monitor Statistics Database

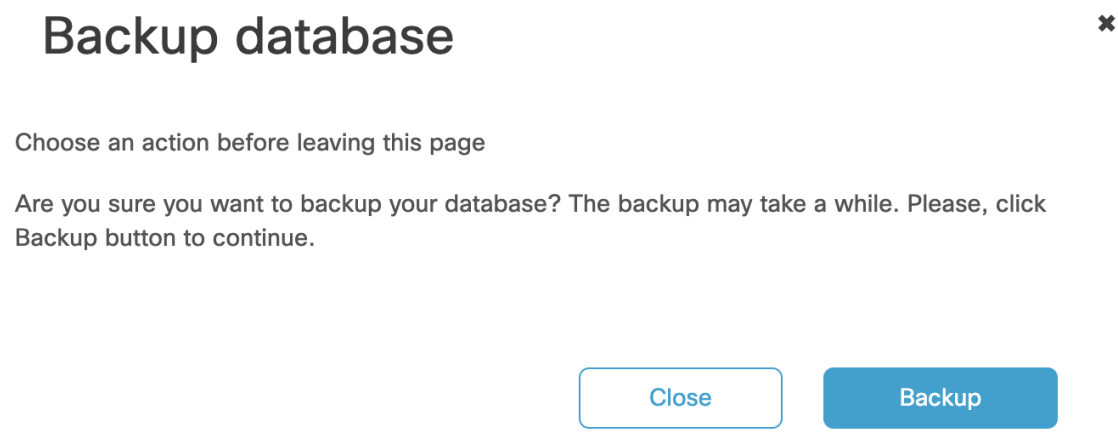
Step 1 Click **Settings** in the top right corner.

The database settings page is shown.



Step 2 In the **BACKUP DATABASE**, click **Backup**.

A confirmation pop-up appears.



Step 3 In the pop-up, click **Backup**.

Step 4 After successful backup, click **Download** to download the backup to your computer.

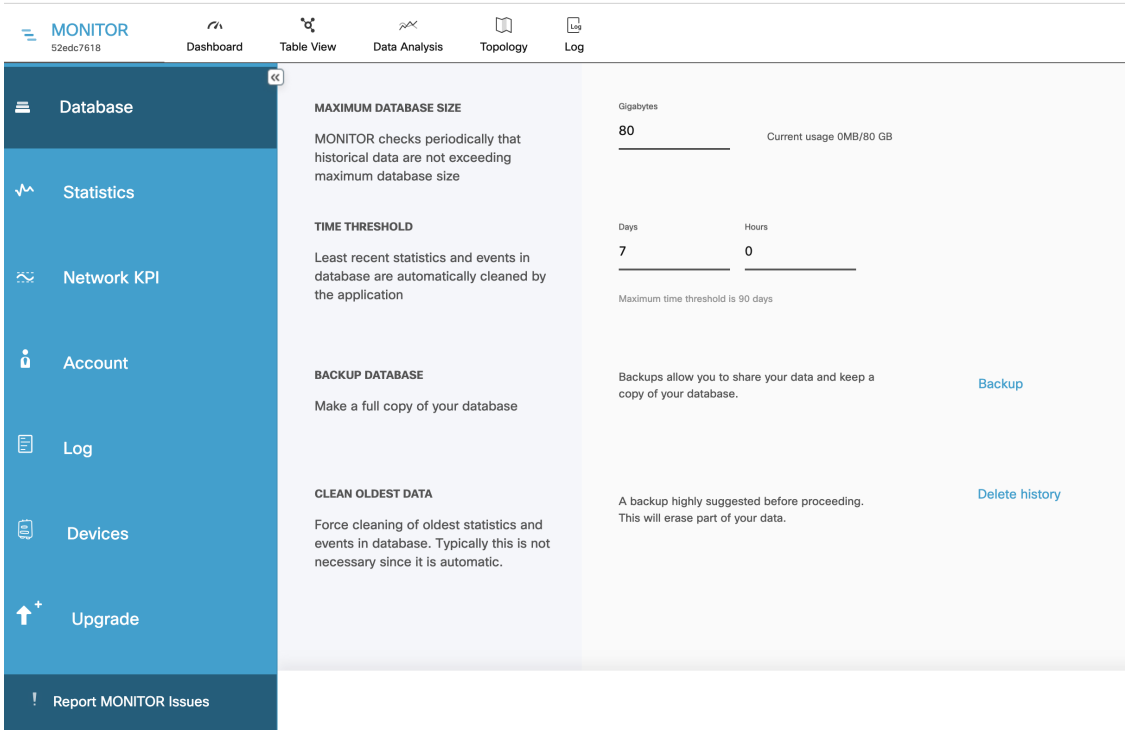
Deleting the recent IW Monitor Statistics Data

You can manually delete the oldest statistics and event data in the IW Monitor database if you feel that excessive amounts of network statistics data are being written to the hard disk in short periods of time.

Important It is strongly recommended that you back up the database before you delete the statistics data. If the current network statistics record is deleted, it cannot be retrieved. For more information on how to back up, see Backing up the IW Monitor Statistics Database, on page 49.

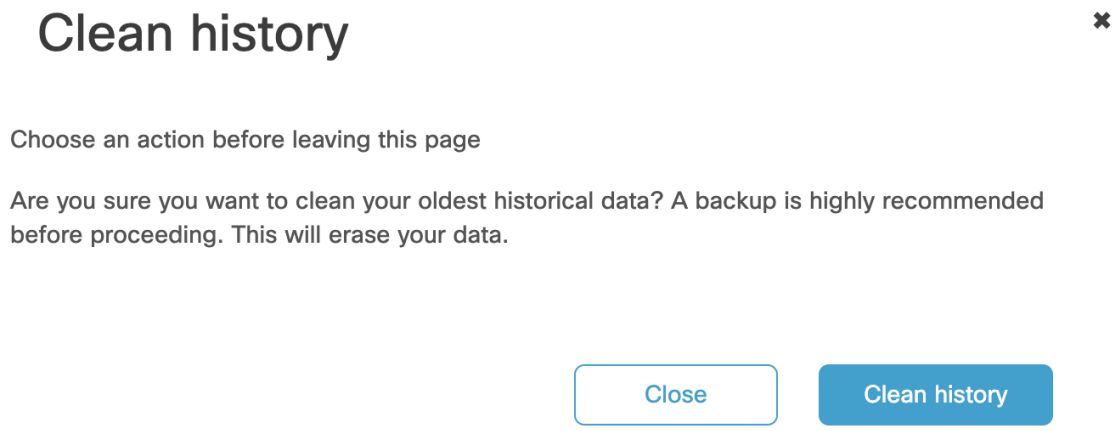
Step 1 Click **Settings** in the top right corner.

The database settings page is shown.



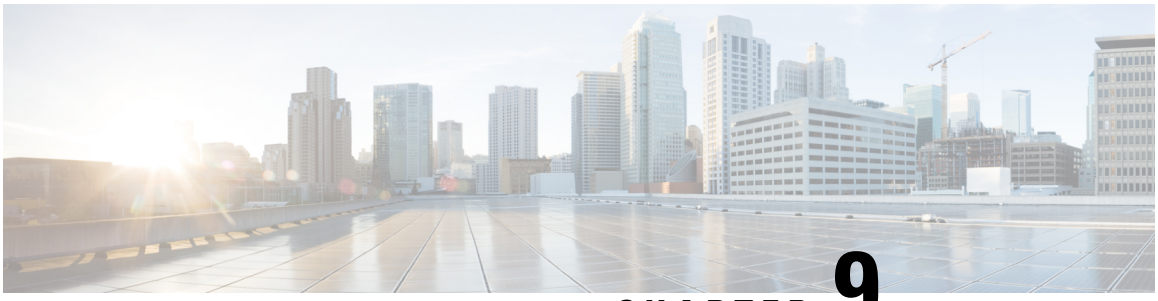
Step 2 Click **Delete history**.

A confirmation pop-up appears.



Step 3 In the pop-up, click **Clean history**.

Note The network statistics data is only deleted if the amount of stored data exceeds the thresholds set by the **MAXIMUM DATABASE SIZE** and/or the **TIME THRESHOLD**. In this case, the oldest 10% of the currently stored network statistics data will be deleted.



CHAPTER 9

Configuring IW Monitor Statistical Settings

- Changing the Interval at which Statistical Data is Logged, on page 53
- Customizing Event-Logging Settings, on page 55
- Setting Performance Thresholds, on page 57
- Setting Performance Thresholds for Each Section, on page 58

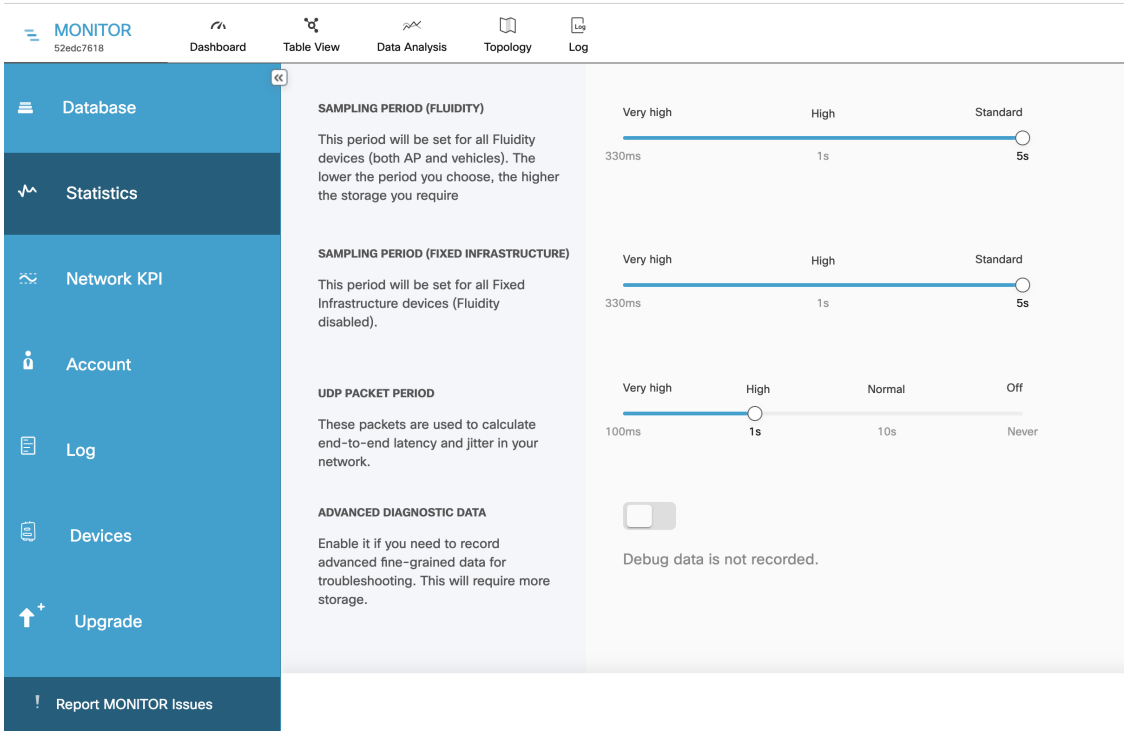
Changing the Interval at which Statistical Data is Logged

Step 1 Click **Settings** in the top right corner.

A new settings page is shown.

Step 2 Click Statistics.

A new statistics settings page is shown.



Step 3 To change the time interval at which statistical data is logged, click-and-drag the **SAMPLING PERIOD** (Fluidity devices) slider and/or the **SAMPLING PERIOD** (Fixed infrastructure) slider.

The recommended data-logging frequency intervals are:

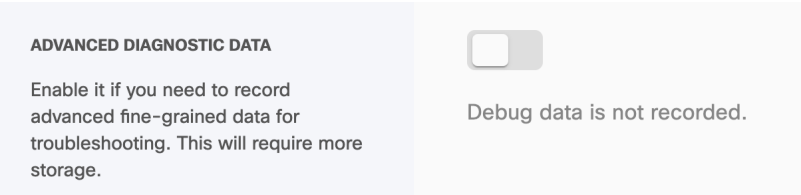
- 330 ms (Fluidity)
- 5 s (Fixed)

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 gives a more detailed statistical log with less possibility of missed errors.
- Lower data-logging frequency uses less hard disk space.

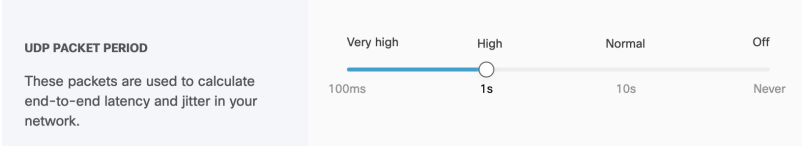
Step 4 To collecting debugging data:

a) Enable **ADVANCED DIAGNOSTIC DATA** to log debugging data for quicker and more advanced technical support.



Step 5 To increase the accuracy with which the IW Monitor host calculates network latency and jitter:

a) Click-and-drag the **UDP PACKET PERIOD** slider.



b) To disable the UDP packet transmission, click-and-drag the **UDP PACKET PERIOD** 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.

Customizing Event-Logging Settings

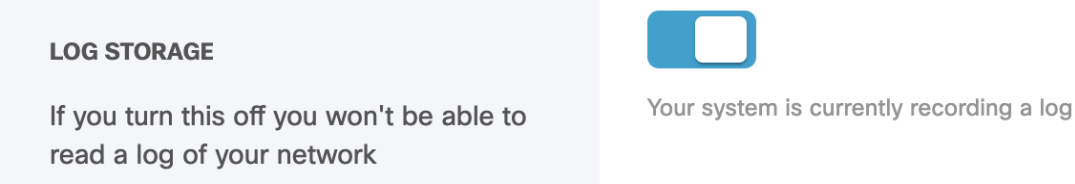
Step 1 Click **Settings** in the top right corner.

A new settings page is shown.

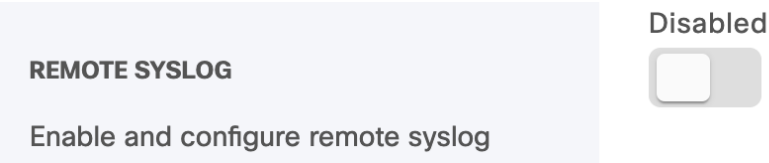
Step 2 Click .

The log settings page is shown.

Step 3 Enable the **Log Storage** toggle.

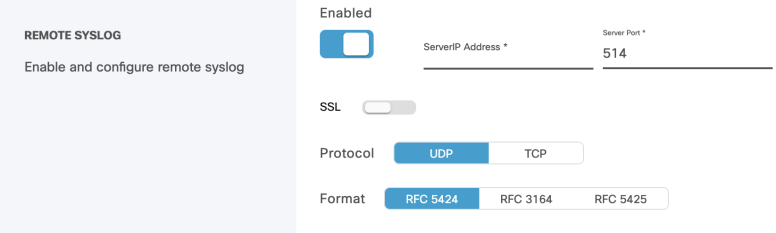


Step 4 Enable the **Remote Syslog** to collect the system logs remotely.

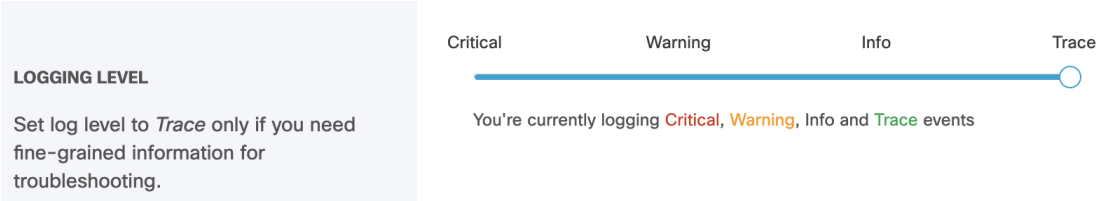


A new screen with **Remote Syslog** settings appears.

a. Fill the remote syslog **server IP address**, **port**, and change the settings based on the requirement.



Step 5 Click-and-drag the **LOGGING LEVEL** slider based on the required logging level.



The four logging levels are:

- **Trace** - Trace-level events are considered trivial, but can be useful for diagnostic 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 6 In the **Event** section, check and uncheck the type of events you want to log.

All network event types are grouped into one of the following categories:

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

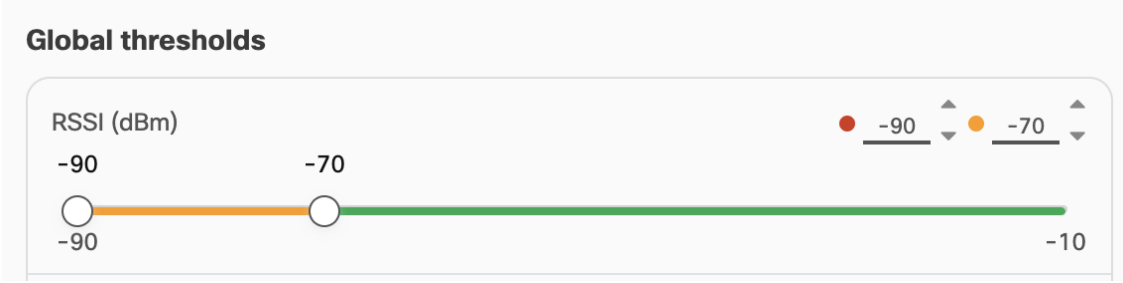
Step 7 Click **Save Changes**.

Setting Performance Thresholds

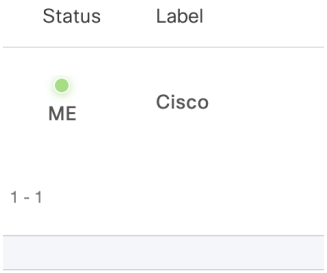
If you want to apply the same performance-alert thresholds to all sections that are part of the network, adjust the performance thresholds by doing the steps that follow:

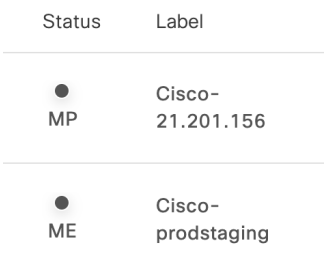
Each performance threshold slider has two buttons that can be clicked and dragged.

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 shows the relevant status.





Setting Performance Thresholds for Each Section

To apply different performance thresholds to different sections of the network, follow these steps:

Step 1 Click **Settings** in the top right corner.

A new settings page is shown.

Step 2 Click Network KPI.

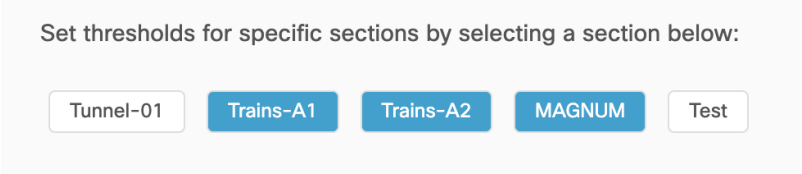
The network KPI settings page is shown.

Step 3 Enable the **PERFORMANCE CHECK** switch to **On**.

The default thresholds section is shown.

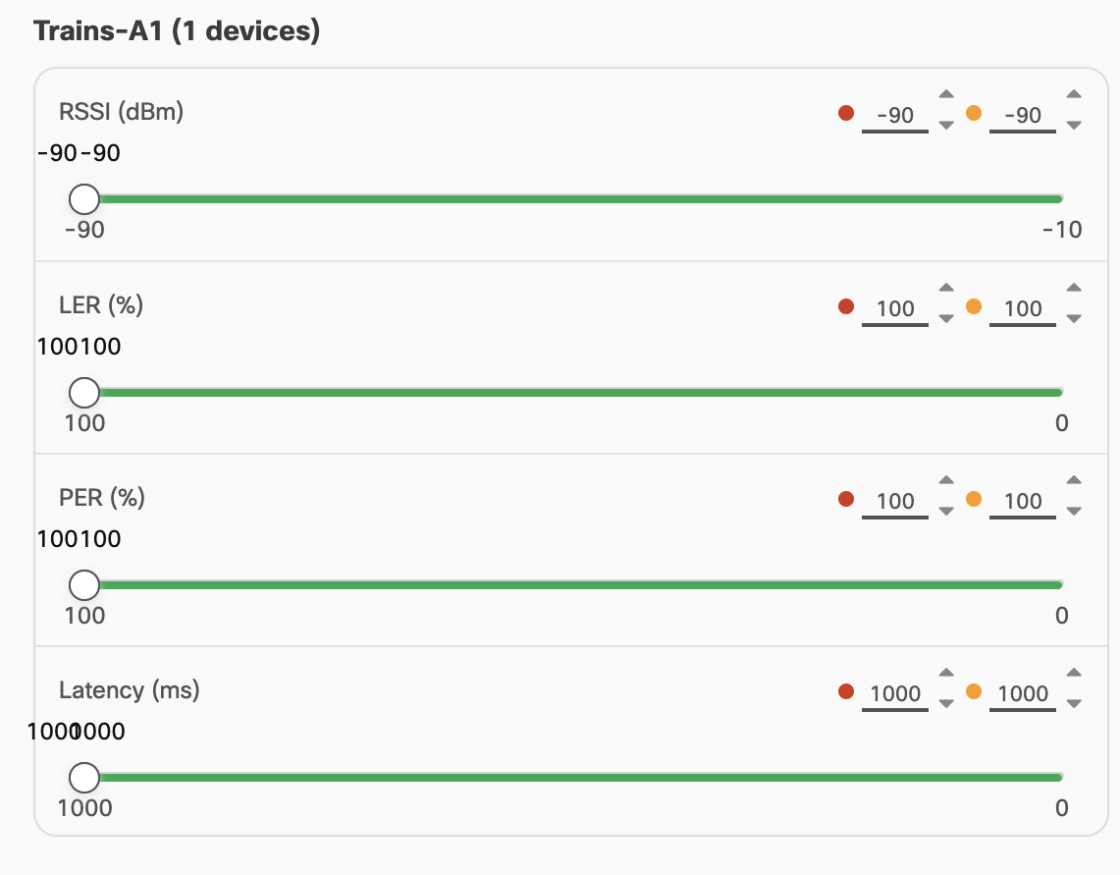
Step 4 Make sure that the current network is partitioned into two or more sections. To know more on how to partition the network into sections, see Creating a new Section, on page 23.

Step 5 If the network is partitioned, tabs are created for each network section under **Global Thresholds** sliders as shown below:



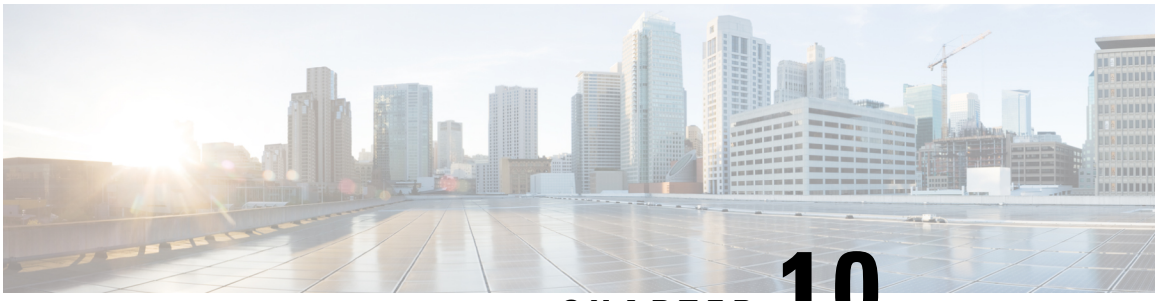
Step 6 Select the network section for which you want to alter the performance thresholds.

A separate group of performance-alert threshold sliders will be shown for the specified network section. For more information about thresholds, see Setting Performance Thresholds, on page 57.



Step 7 Click-and-drag the sliders to adjust the performance-alert thresholds for the specified network.

Step 8 Repeat the steps above for all network sections.



CHAPTER 10

Managing User Accounts

You can update your details, access password, and also add other users to the IW Monitor.

- Modifying an Existing User Account, on page 61
- Viewing, Adding, and Deleting Users, on page 62

Modifying an Existing User Account

Step 1 Click **Settings** in the top right corner.

A new settings page is shown.

Step 2 Click Account.

The user account settings page is shown.

Step 3 To change your first name and/or last name details, do the following steps:

a) Update the **First name** and **Last name** fields as required.

b) Click **Save Changes**.

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

Step 4 To change your access password details, do the following 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**.

Viewing, Adding, and Deleting Users

Step 1 Click **Settings** in the top right corner.

A new settings page is shown.

Step 2 Click Account.

The user account settings page with the list of existing user accounts is shown.

Step 3 To add a new user, do the following 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) Make a note and send the password details to the new user's password. The user must use their randomly generated password to log in to their new user account.

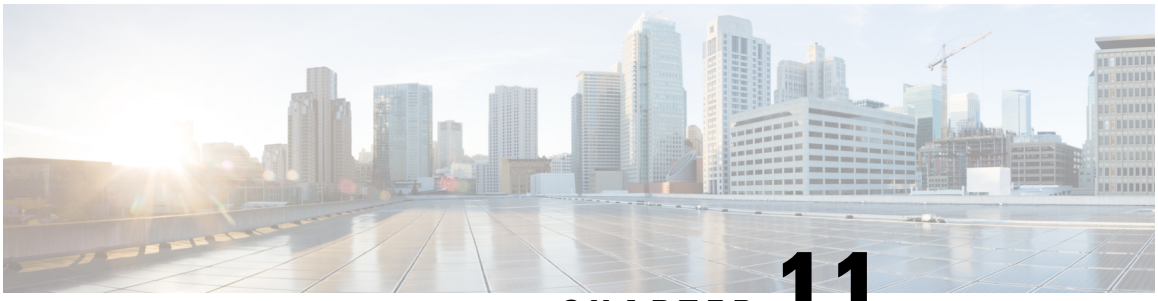
When the new user logs in to their user account for the first time, the new user will see a notification advising them to change the randomly generated password to a new password.

Step 4 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

Updating IW Monitor

• Updating IW Monitor, on page 63

Updating IW Monitor

For best performance, it is recommended that you always use the latest version of IW Monitor application. Updated versions may include new features, improved operation, and bug fixes.

Step 1 To download the latest image file:

a) Go to software downloads.

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

Step 2 Log in to the IW Monitor.

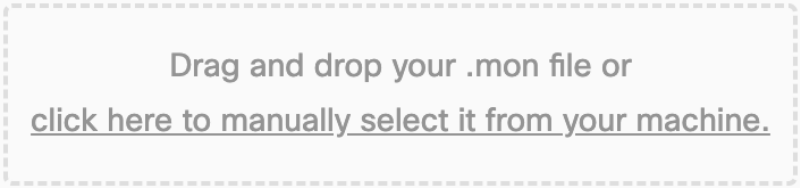
Step 3 Click **Settings** in the top right corner.

A new settings page is shown.

Step 4 Click Upgrade.

The upgrade page is shown.

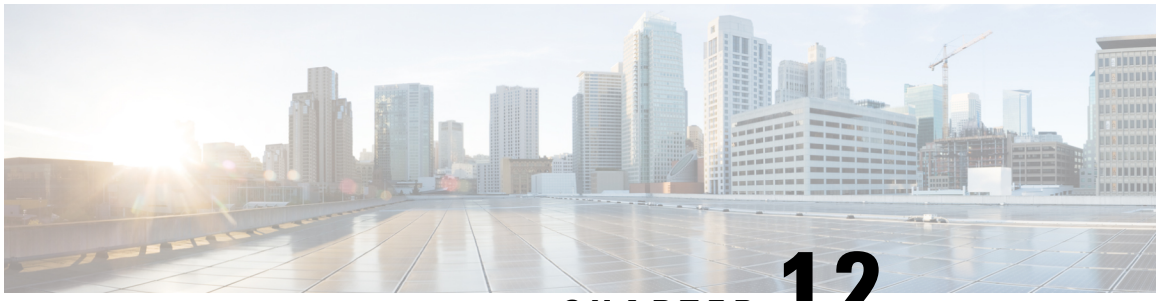
Step 5 Locate the correct image file on your computer or drag and drop the image file.



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

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

Updating IW Monitor



CHAPTER 12

Uninstalling IW Monitor

• Uninstalling IW Monitor, on page 65

Uninstalling IW Monitor

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.

Uninstalling 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.