IW Monitor User Guide, Release 2.2.0

First Published: 2025-08-08

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

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

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

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

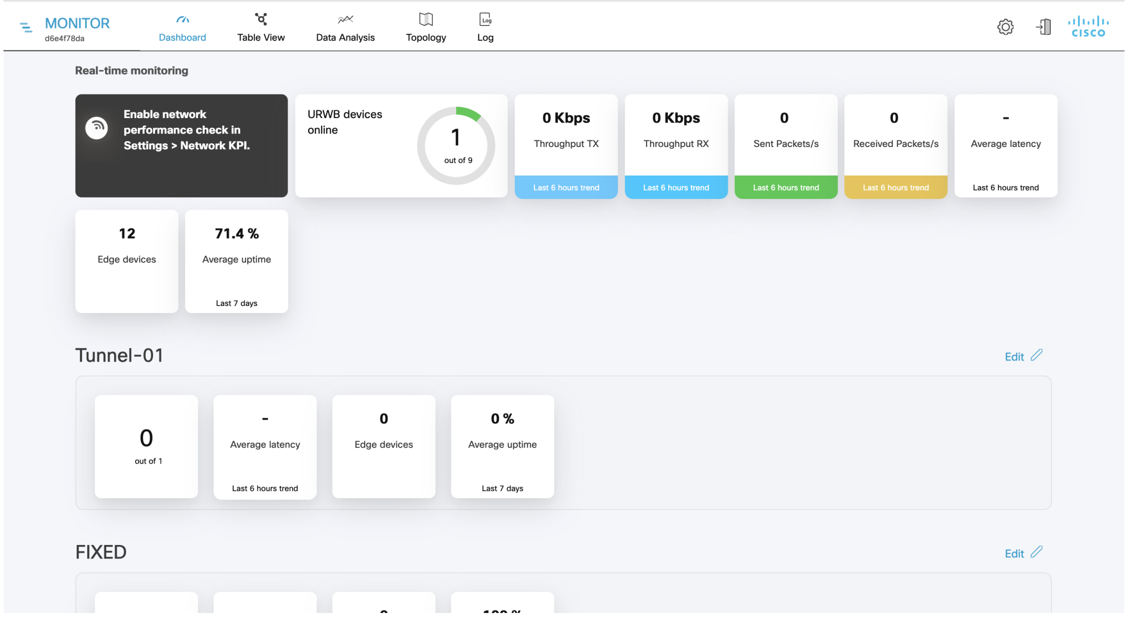
IW Monitor Overview

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:Text

- 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.



Real-time monitoring

Enable network performance check in Settings > Network KPI.

URWB devices online: 1 out of 9

0 Kbps Throughput TX – Last 6 hours trend

0 Kbps Throughput RX – Last 6 hours trend

0 Sent Packets/s – Last 6 hours trend

0 Received Packets/s – Last 6 hours trend

- Average latency – Last 6 hours trend

12 Edge devices

71.4 % Average uptime – Last 7 days

Tunnel-01 Edit

0 out of 1

- Average latency – Last 6 hours trend

0 Edge devices

0 % Average uptime – Last 7 days

FIXED Edit

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

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
IEC-6400	1.1.0.7 or later

CHAPTER 3

Installing IW Monitor Docker on Host

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 51.

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.

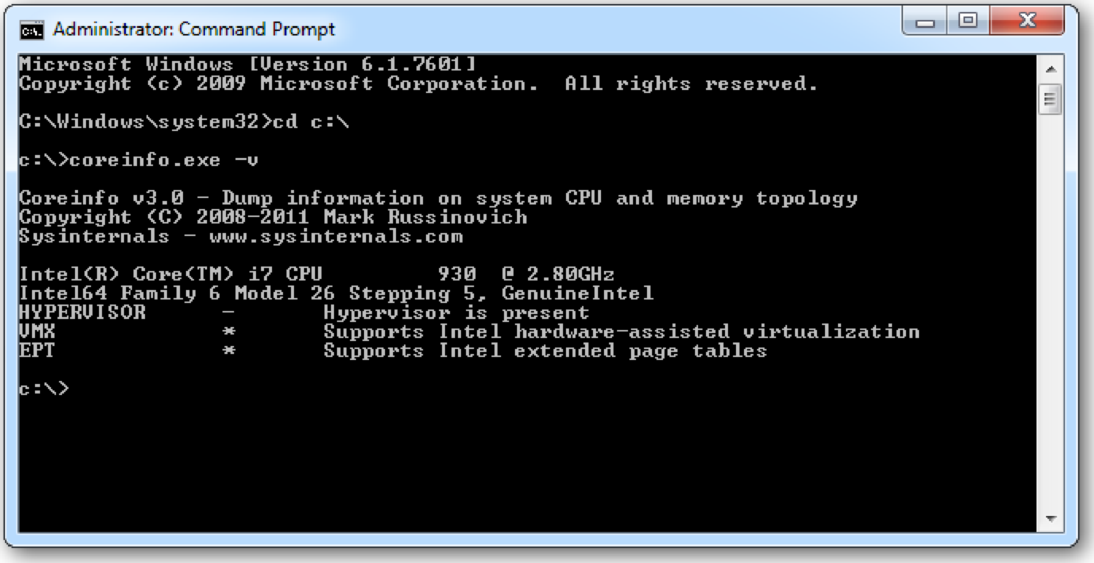
Prerequisites to install Docker on the IW Monitor host

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):



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd c:\

c:\>coreinfo.exe -v

Coreinfo v3.0 - Dump information on system CPU and memory topology
Copyright (C) 2008-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Core(TM) i7 CPU         930  @ 2.80GHz
Intel64 Family 6 Model 26 Stepping 5, GenuineIntel
HYPERVISOR      -       Hypervisor is present
VMX             *       Supports Intel hardware-assisted virtualization
EPT             *       Supports Intel extended page tables

c:\>
```

   - 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.

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.

Downloading and installing the Docker application

Procedure

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

Procedure

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

Procedure

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

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

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

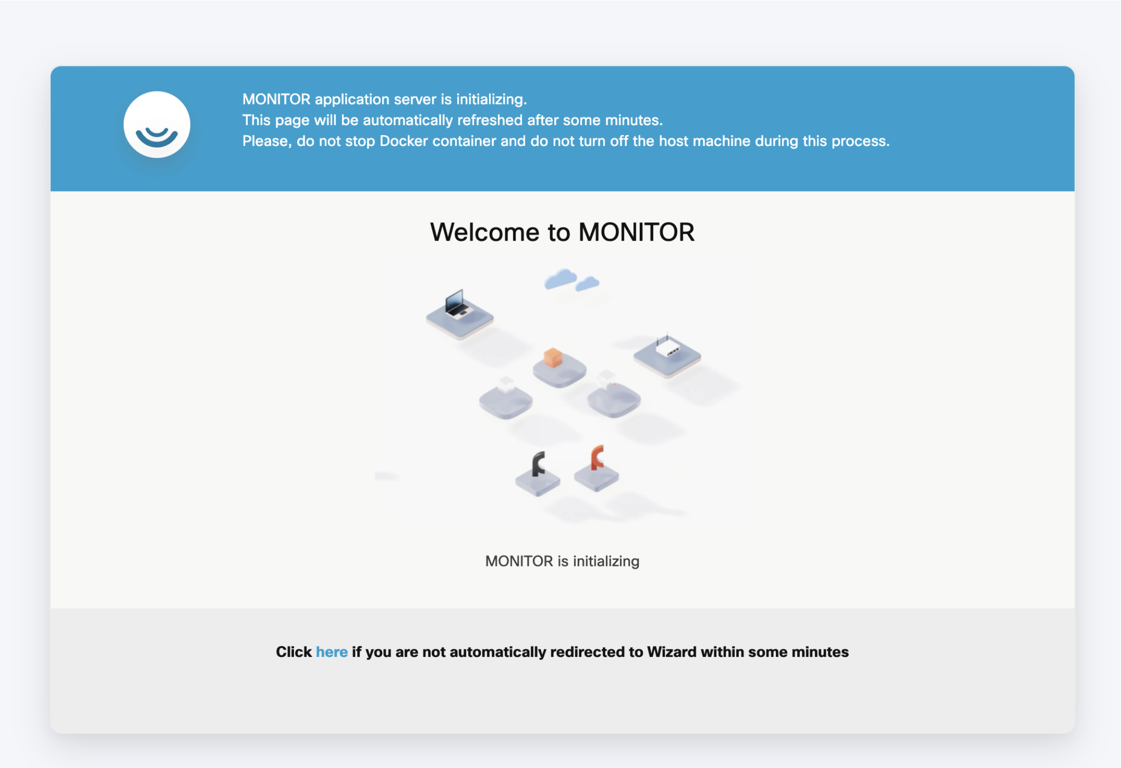
Note
If you fail to use the default host port numbers due to security policy settings or the needed host port is assigned to another service, modify the `docker run` command to include an unused host port.

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



MONITOR application server is initializing.
This page will be automatically refreshed after some minutes.
Please, do not stop Docker container and do not turn off the host machine during this process.

Welcome to MONITOR

MONITOR is initializing

Click here if you are not automatically redirected to Wizard within some minutes

below:

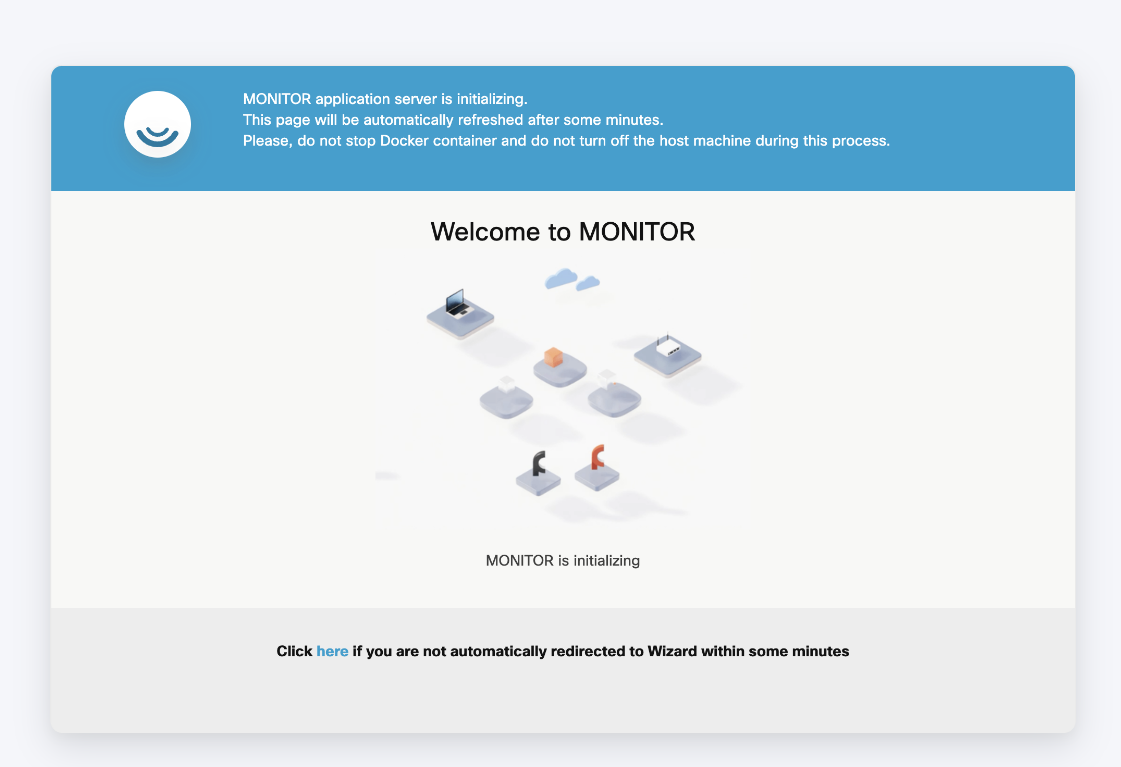
Logging to the IW Monitor for the First Time

Procedure

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:



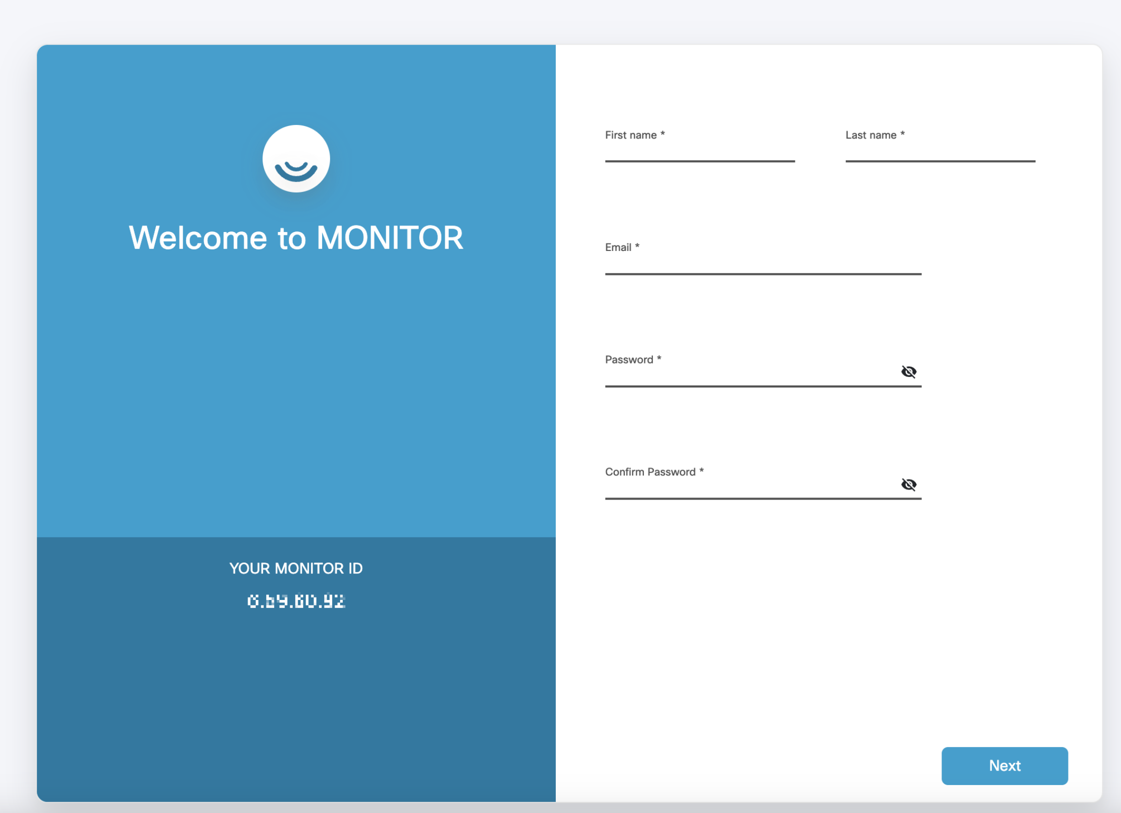
MONITOR application server is initializing.
This page will be automatically refreshed after some minutes.
Please, do not stop Docker container and do not turn off the host machine during this process.

Welcome to MONITOR

MONITOR is initializing

Click here **if you are not automatically redirected to Wizard within some minutes**

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



Welcome to MONITOR

YOUR MONITOR ID

[redacted]

First name *

Last name *

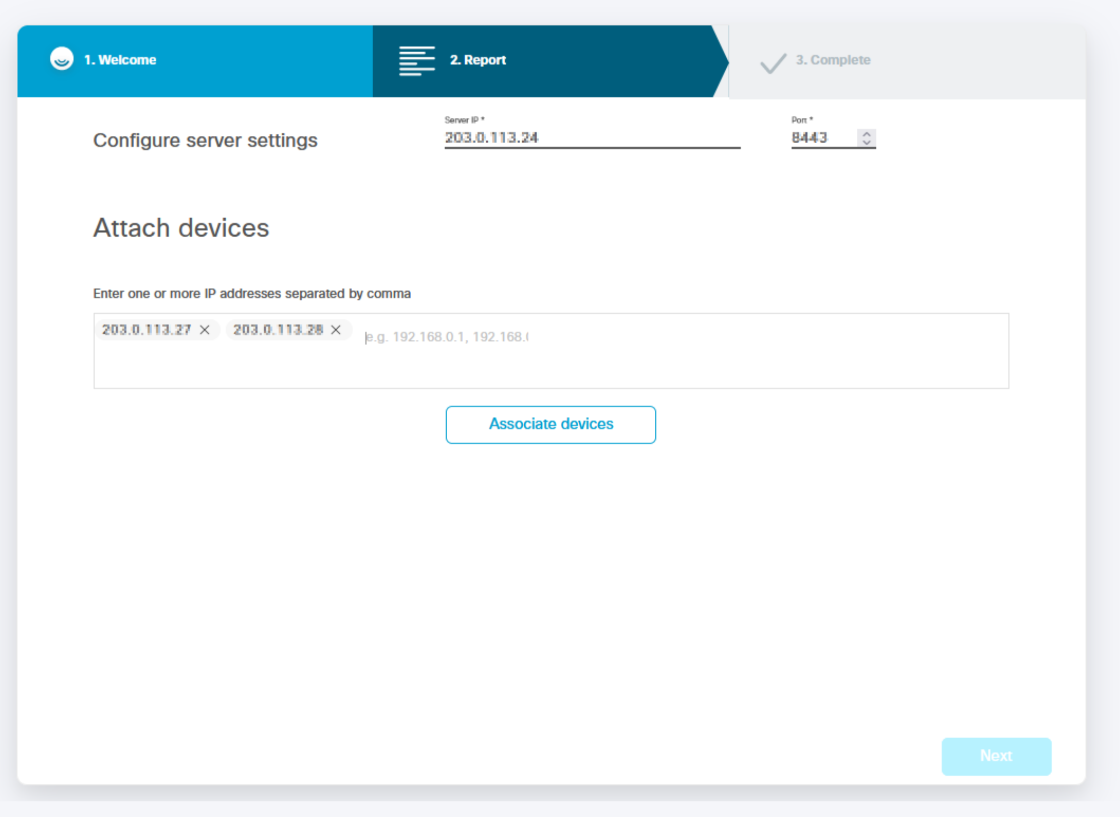
Email *

Password *

Confirm Password *

Step 4 Click **Next**.

The **Add new device** screen appears.



Configure server settings

Server IP * 203.0.113.24

Port * 8443

Attach devices

Enter one or more IP addresses separated by comma

203.0.113.27 ✕ 203.0.113.28 ✕ e.g. 192.168.0.1, 192.168.(

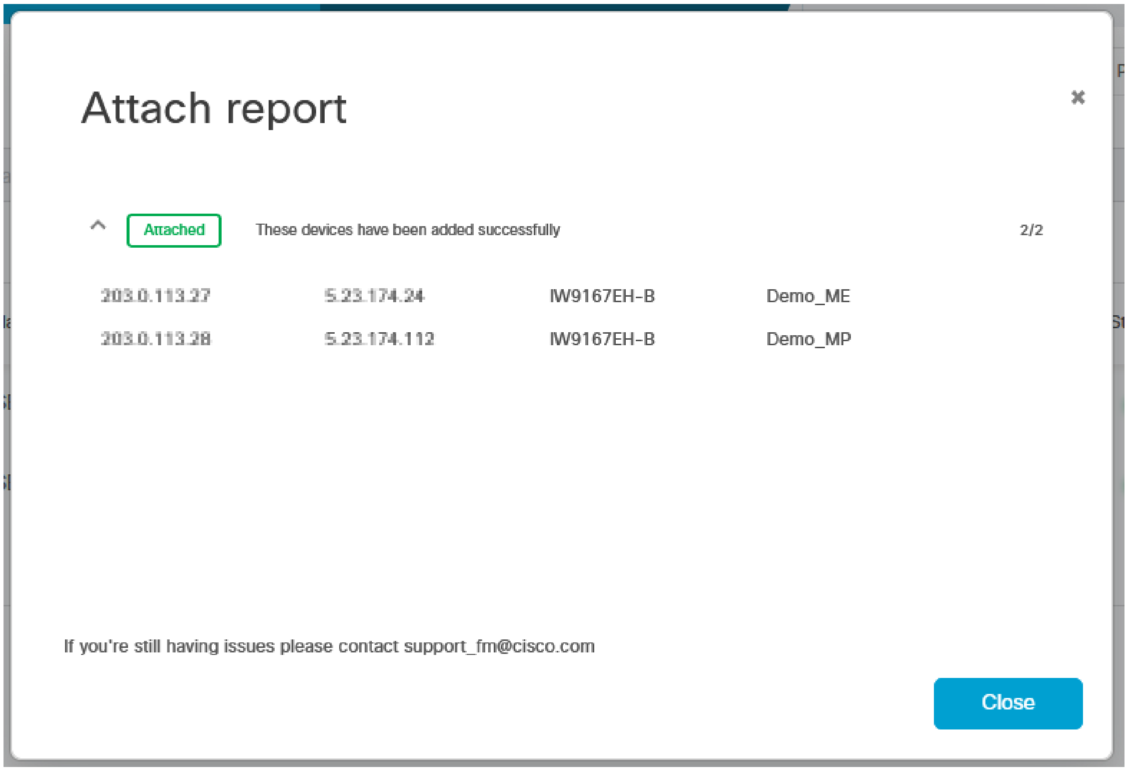
Step 5 (Optional) If required, fill the IP address of the IW Monitor server in the **Server IP** field and port number in **Port** field.

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.



Attach report

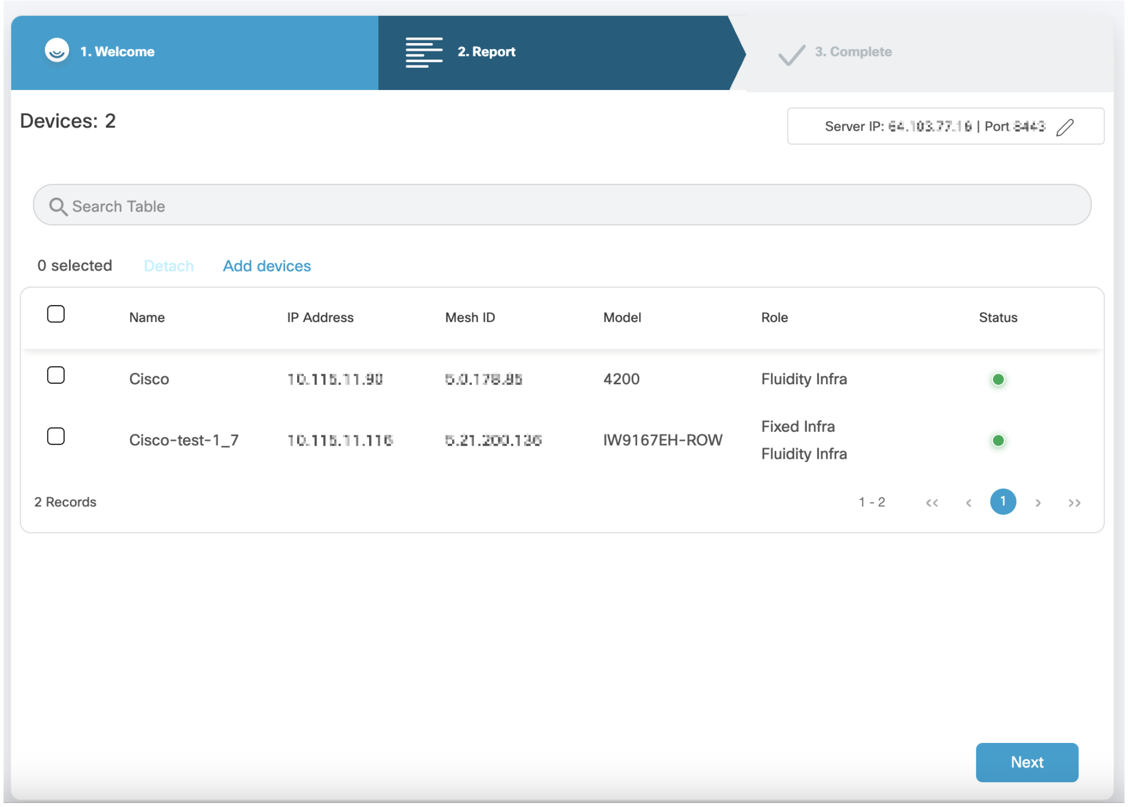
These devices have been added successfully 2/2

203.0.113.27	5.23.174.24	IW9167EH-B	Demo_ME
203.0.113.28	5.23.174.112	IW9167EH-B	Demo_MP

If you're still having issues please contact support_fm@cisco.com

Step 8 Click **Close**.

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



Devices: 2

Server IP: 64.103.77.16 | Port 8443

0 selected

□	Name	IP Address	Mesh ID	Model	Role	Status
□	Cisco	10.115.11.90	5.0.178.85	4200	Fluidity Infra	●
□	Cisco-test-1_7	10.115.11.116	5.21.200.136	IW9167EH-ROW	Fixed Infra Fluidity Infra	●

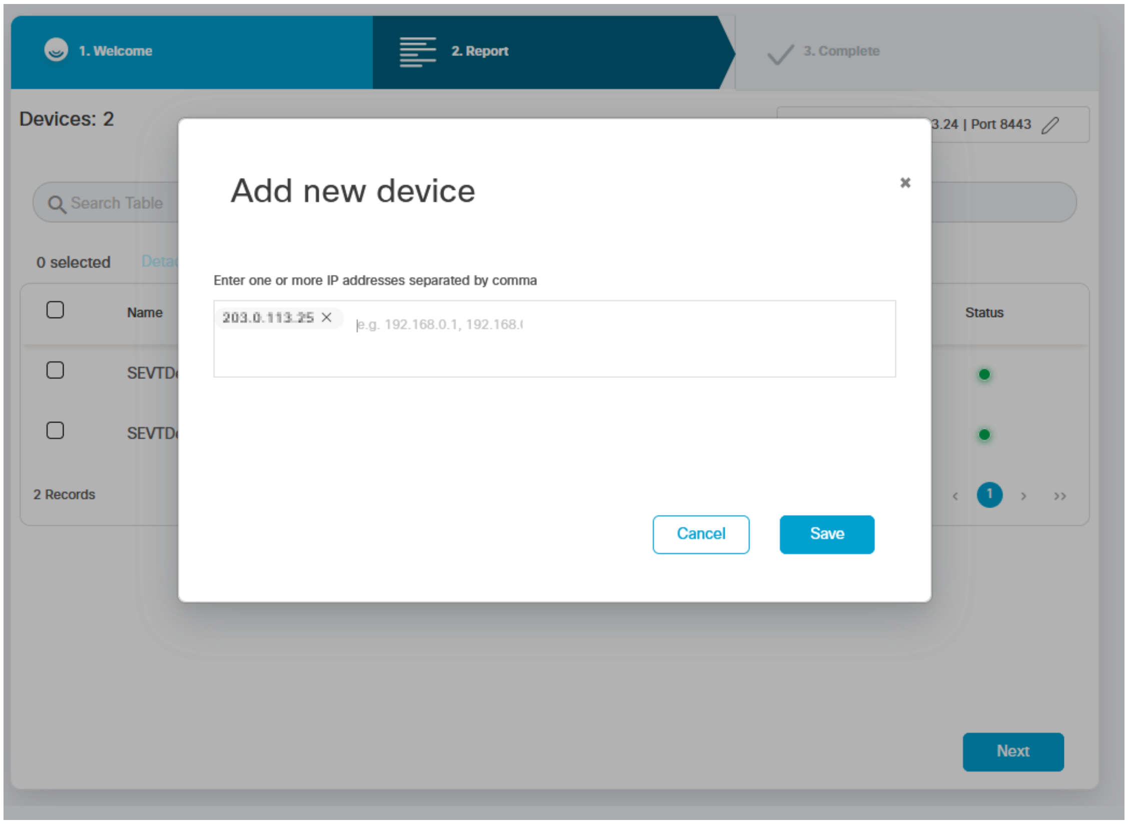
2 Records

1 - 2 ‹‹ ‹ 1 › ››

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.



Add new device

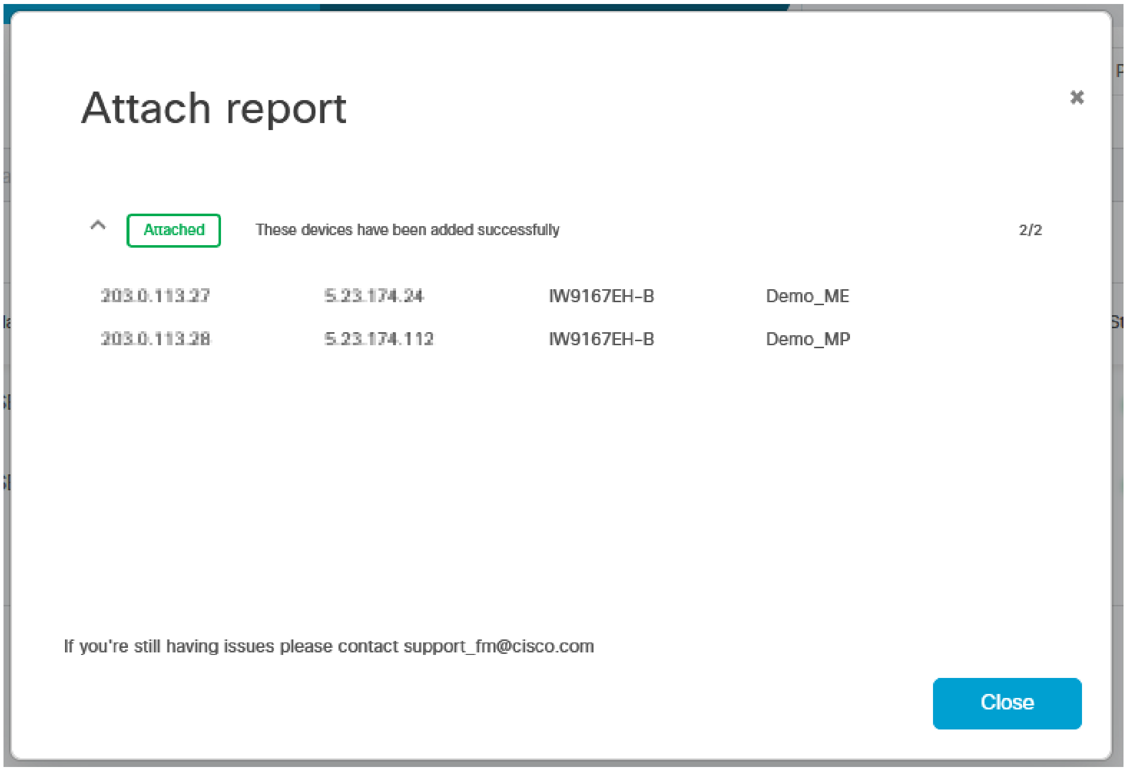
Enter one or more IP addresses separated by comma

203.0.113.25 × e.g. 192.168.0.1, 192.168.(

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.



These devices have been added successfully 2/2

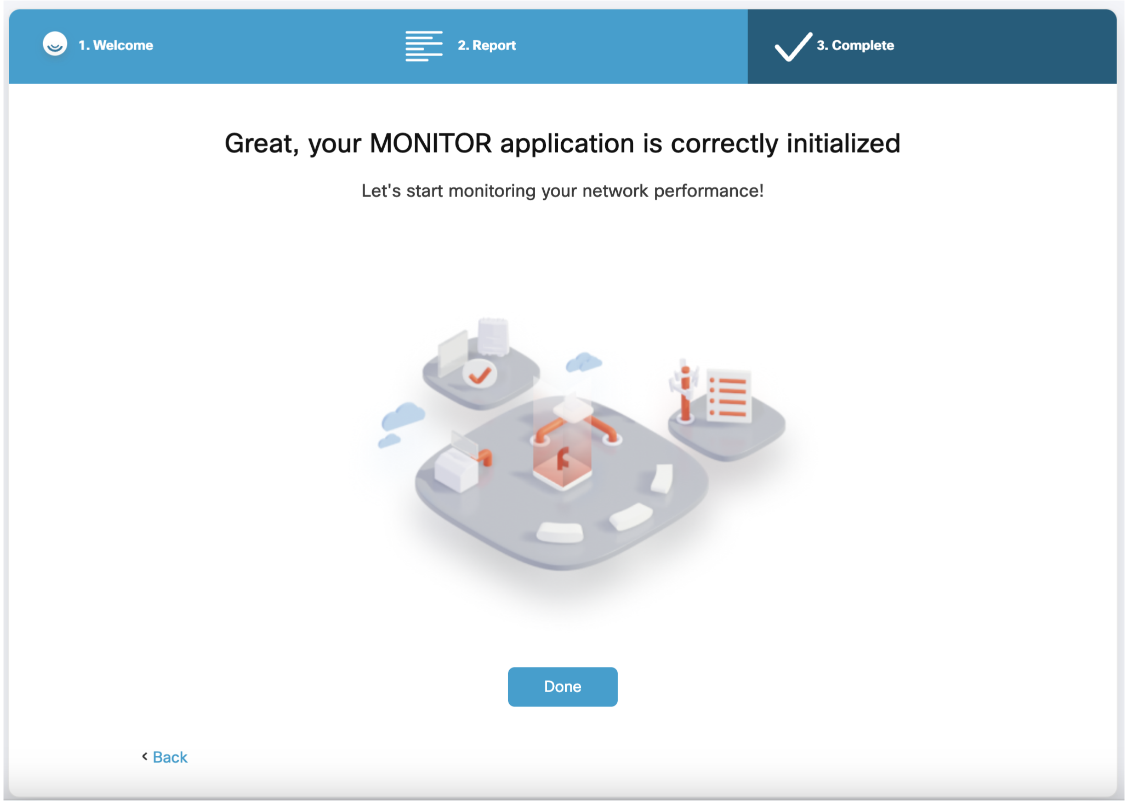
203.0.113.27	5.23.174.24	IW9167EH-B	Demo_ME
203.0.113.28	5.23.174.112	IW9167EH-B	Demo_MP

If you're still having issues please contact support_fm@cisco.com

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:

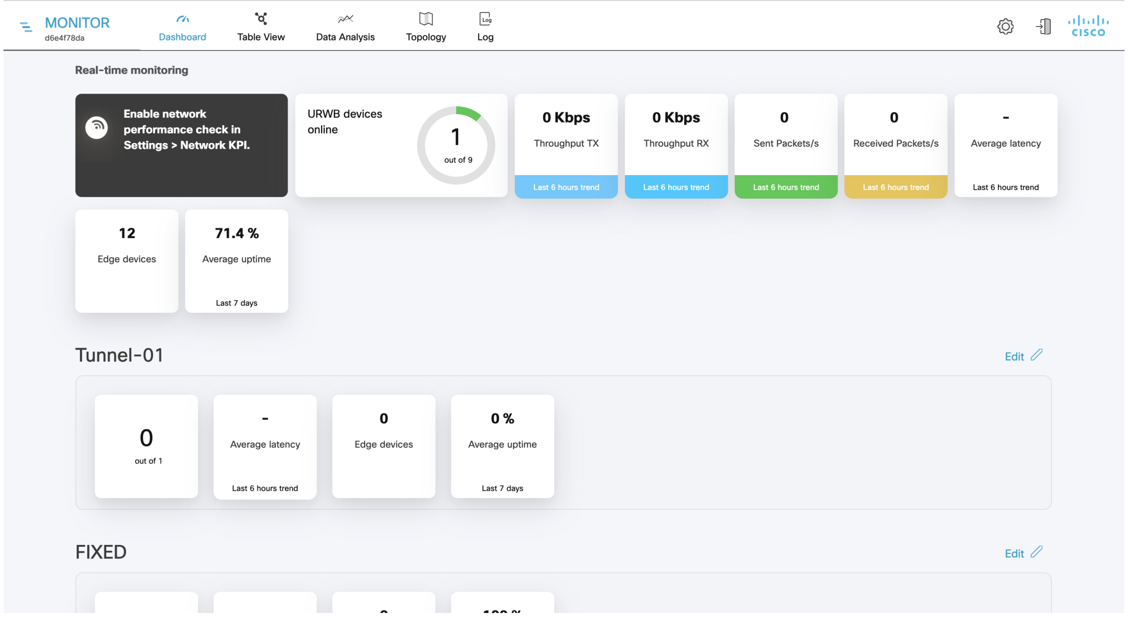


Great, your MONITOR application is correctly initialized

Let's start monitoring your network performance!

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

The IW Monitor dashboard appears:



Enable network performance check in Settings > Network KPI.

CHAPTER 4

Adding Devices to the IW Monitor

Adding Devices to the IW Monitor

Procedure

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.

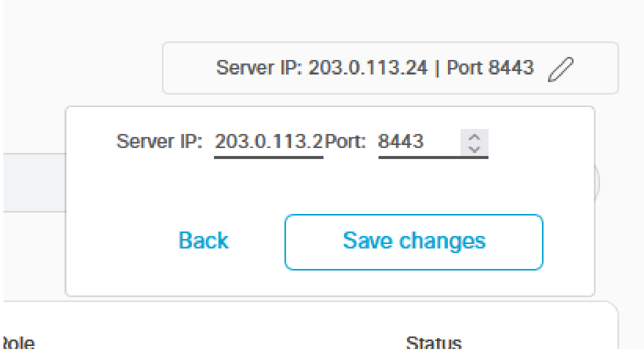
Step 4 If needed, add the server IP address in the **Server IP** field.

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



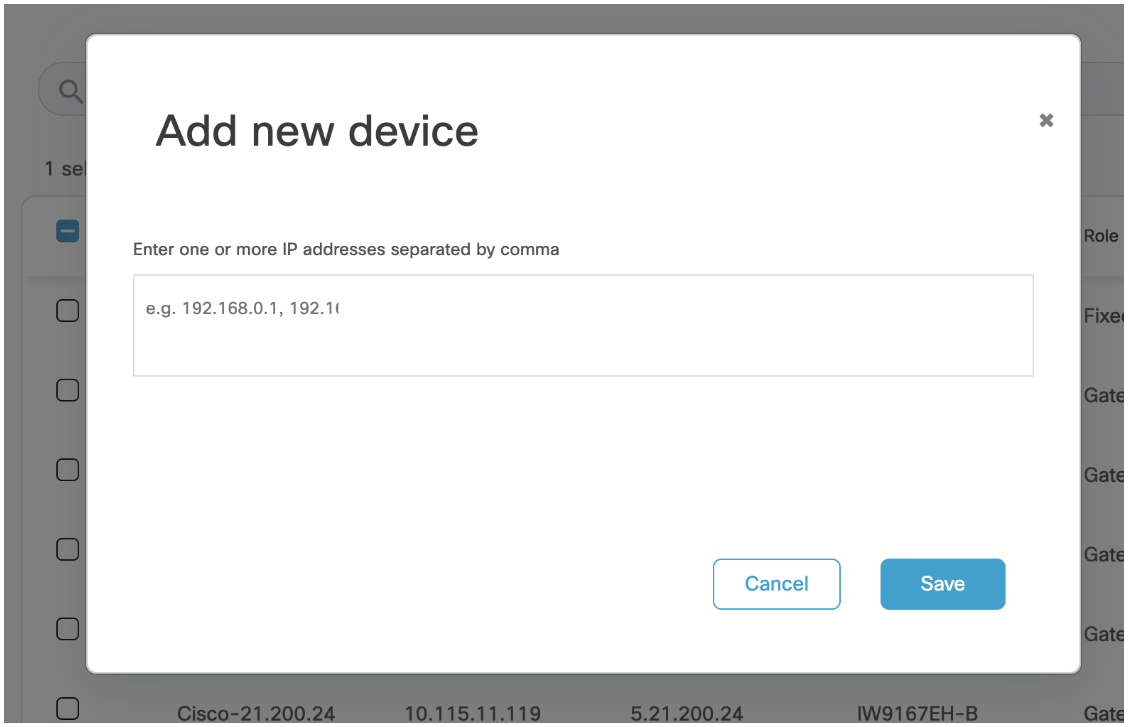
Server IP: 203.0.113.24 | Port 8443

Server IP: 203.0.113.2 Port: 8443

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.



Add new device

Enter one or more IP addresses separated by comma

e.g. 192.168.0.1, 192.1(

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

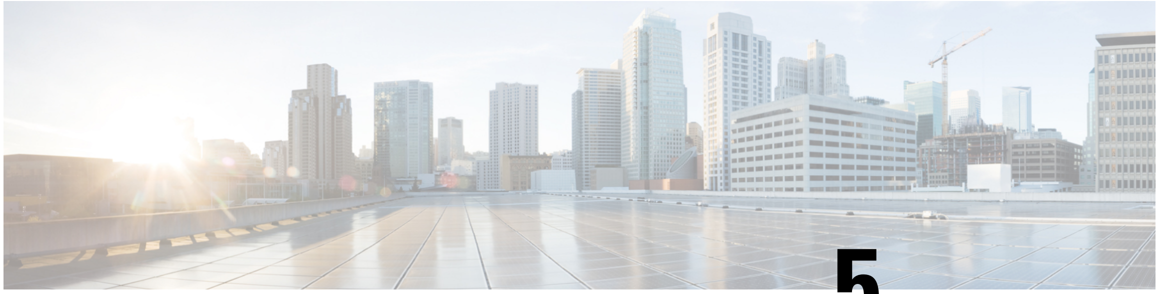
Note

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.



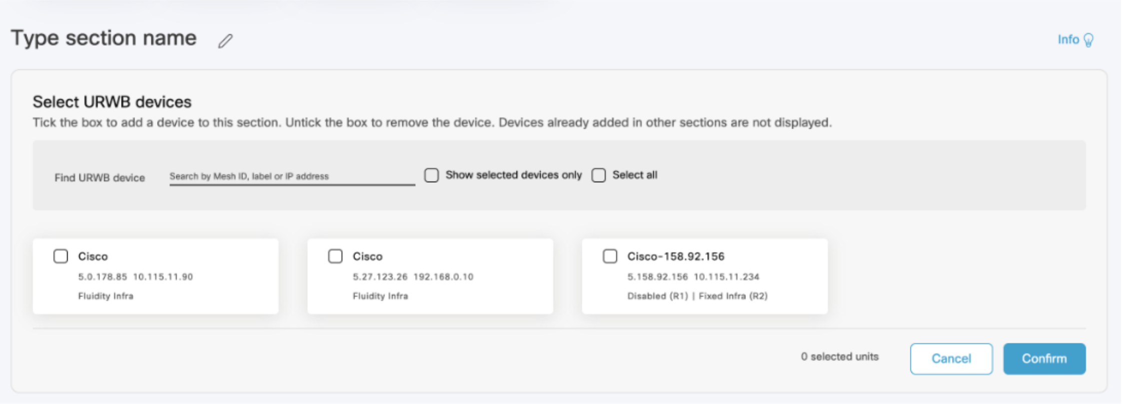
CHAPTER 5

Managing Sections

Create a new Section

Procedure

Step 1 Click **+ ADD SECTION**.



Type section name ✎ Info

Select URWB devices

Tick the box to add a device to this section. Untick the box to remove the device. Devices already added in other sections are not displayed.

Find URWB device: Search by Mesh ID, label or IP address □ Show selected devices only □ Select all

□ Cisco
5.0.178.85 10.115.11.90
Fluidity Infra

□ Cisco
5.27.123.26 192.168.0.10
Fluidity Infra

□ Cisco-158.92.156
5.158.92.156 10.115.11.234
Disabled (R1) | Fixed Infra (R2)

0 selected units

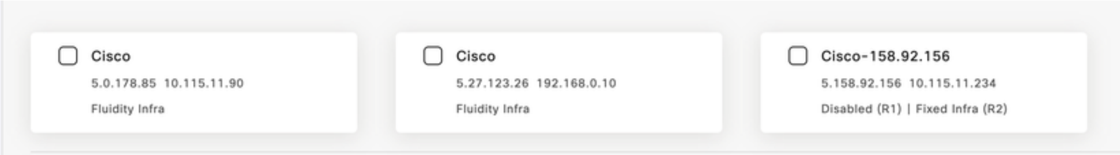
Step 2 Click ✎ edit icon and enter a name for the new section.

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

Step 4 Select the devices to be added 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.



□ Cisco
5.0.178.85 10.115.11.90
Fluidity Infra

□ Cisco
5.27.123.26 192.168.0.10
Fluidity Infra

□ Cisco-158.92.156
5.158.92.156 10.115.11.234
Disabled (R1) | Fixed Infra (R2)

Step 5 Click **Confirm**.

The selected devices are added to the new section.

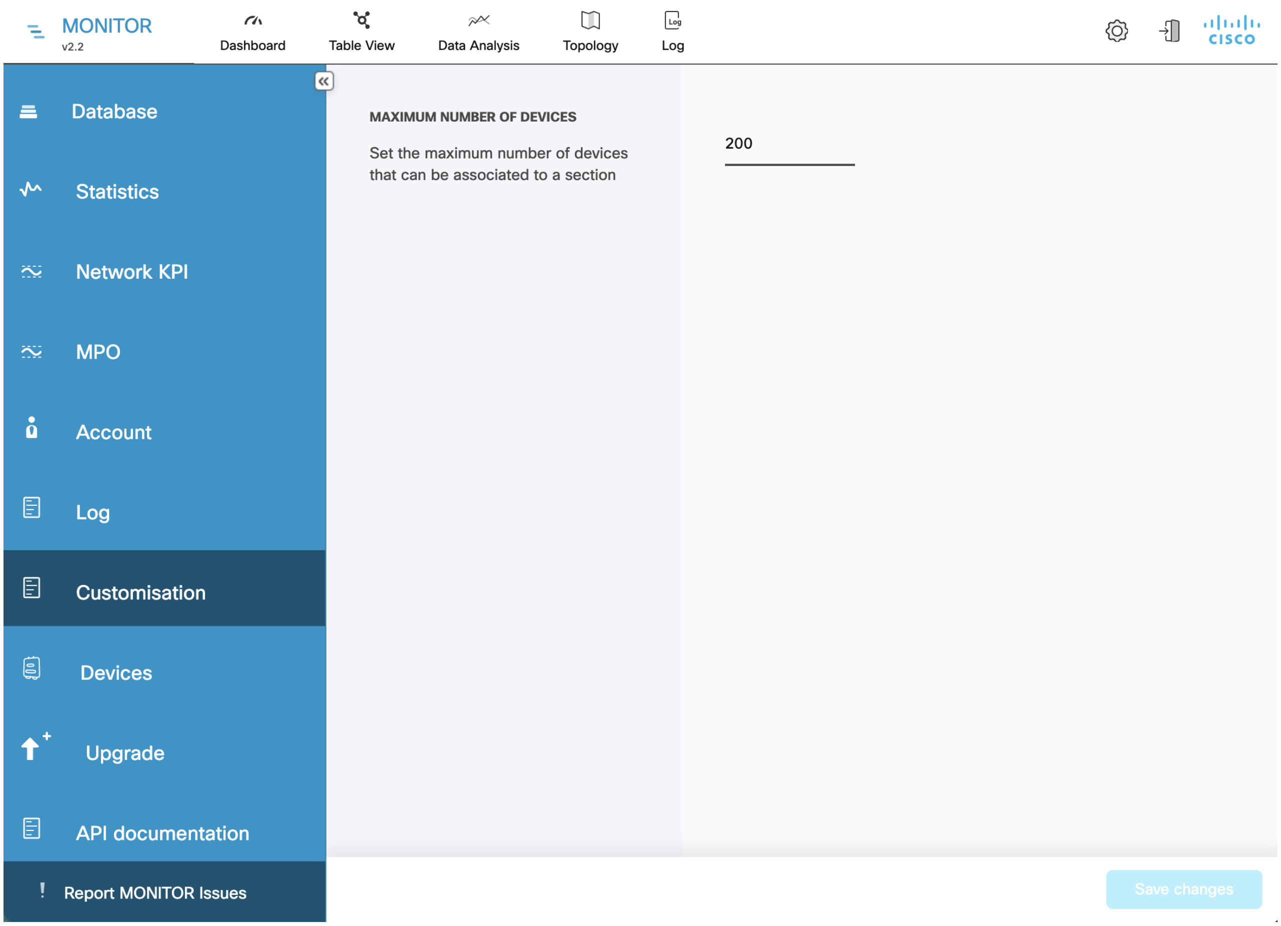
Set maximum number of devices

You can set the maximum number of devices that can be included in a section. The default value for each section is 200 devices.

Procedure

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

Step 2 Set the **Maximum number of devices** for the section.



MAXIMUM NUMBER OF DEVICES

Set the maximum number of devices that can be associated to a section

200

Step 3 Click **Save changes**.

Editing a Section

Procedure

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

Procedure

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

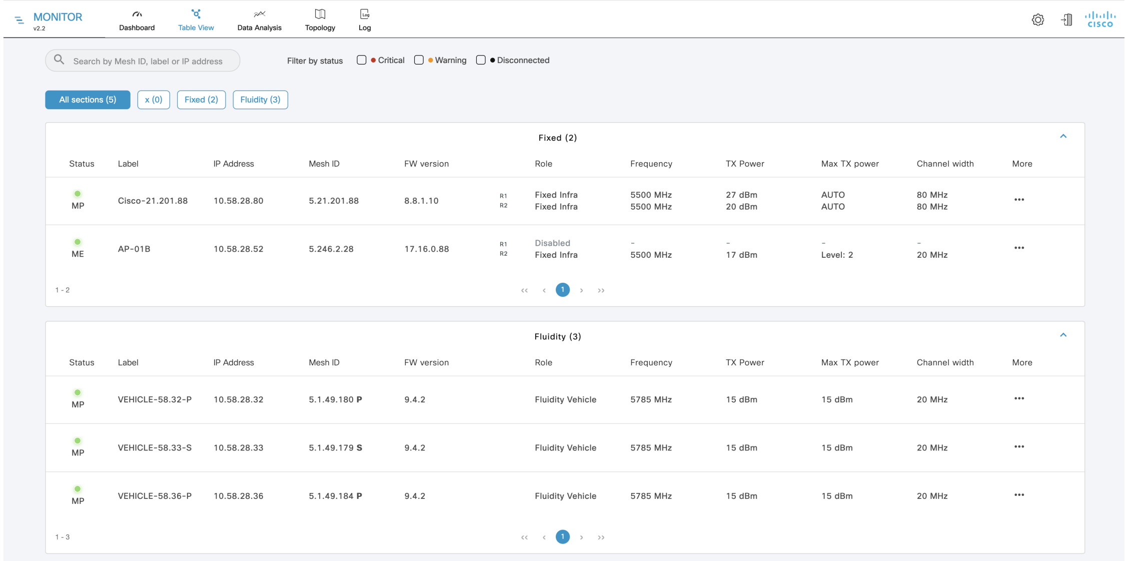
Managing Devices

Editing the Device Configuration Parameters using Configurator Interface

Procedure

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

A new screen as below appears:



Fixed (2)

Status	Label	IP Address	Mesh ID	FW version		Role	Frequency	TX Power	Max TX power	Channel width	More
● MP	Cisco-21.201.88	10.58.28.80	5.21.201.88	8.8.1.10	R1 R2	Fixed Infra Fixed Infra	5500 MHz 5500 MHz	27 dBm 20 dBm	AUTO AUTO	80 MHz 80 MHz	•••
● ME	AP-01B	10.58.28.52	5.246.2.28	17.16.0.88	R1 R2	Disabled Fixed Infra	- 5500 MHz	- 17 dBm	- Level: 2	- 20 MHz	•••

1 - 2

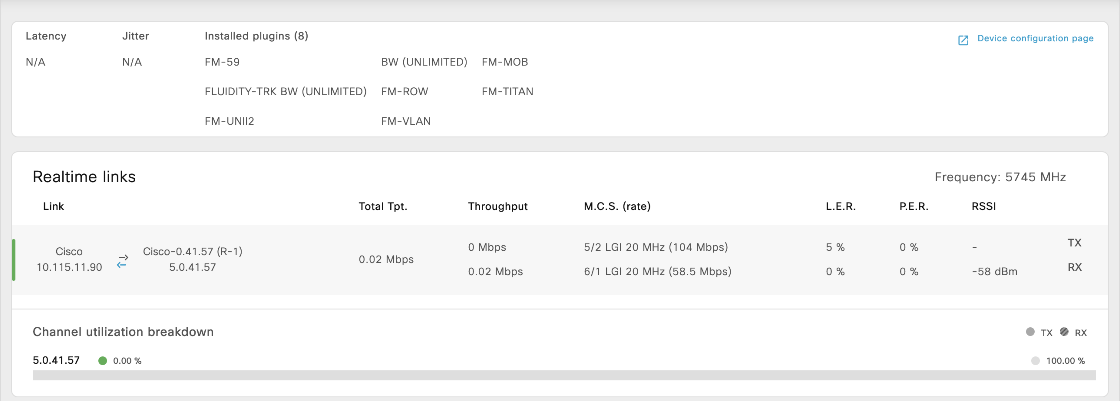
Fluidity (3)

Status	Label	IP Address	Mesh ID	FW version	Role	Frequency	TX Power	Max TX power	Channel width	More
● MP	VEHICLE-58.32-P	10.58.28.32	5.1.49.180 **P**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••
● MP	VEHICLE-58.33-S	10.58.28.33	5.1.49.179 **S**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••
● MP	VEHICLE-58.36-P	10.58.28.36	5.1.49.184 **P**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••

1 - 3

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

A detailed section appears:



Latency	Jitter	Installed plugins (8)		
N/A	N/A	FM-59	BW (UNLIMITED)	FM-MOB
		FLUIDITY-TRK BW (UNLIMITED)	FM-ROW	FM-TITAN
		FM-UNII2	FM-VLAN	

Device configuration page

Realtime links

Frequency: 5745 MHz

Link	Total Tpt.	Throughput	M.C.S. (rate)	L.E.R.	P.E.R.	RSSI	
Cisco 10.115.11.90 ⇄ Cisco-0.41.57 (R-1) 5.0.41.57	0.02 Mbps	0 Mbps	5/2 LGI 20 MHz (104 Mbps)	5 %	0 %	-	TX
		0.02 Mbps	6/1 LGI 20 MHz (58.5 Mbps)	0 %	0 %	-58 dBm	RX

Channel utilization breakdown

● TX ● RX

5.0.41.57 ● 0.00 % ● 100.00 %

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

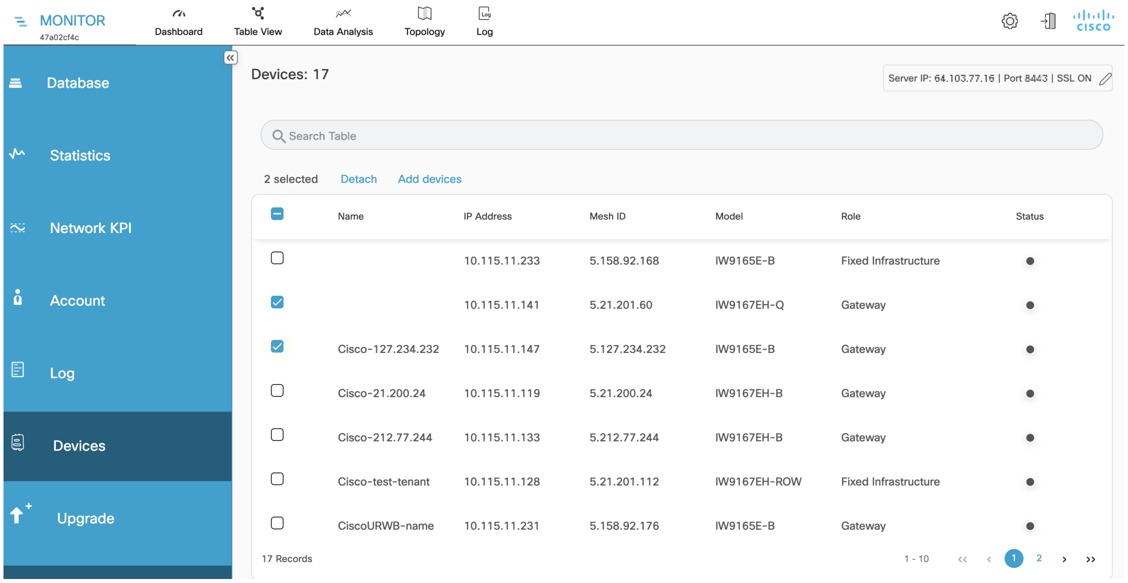
Procedure

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.



Devices: 17

Server IP: 64.103.77.16 | Port 8443 | SSL ON

Search Table

2 selected Detach Add devices

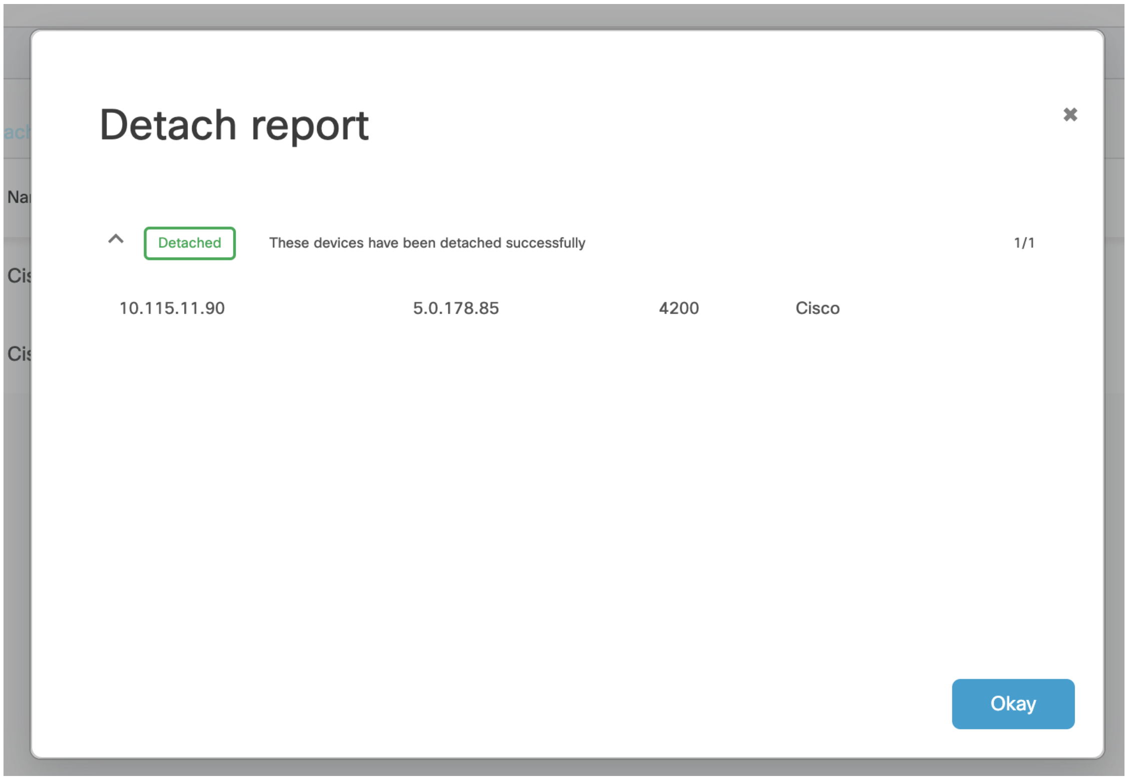
☐	Name	IP Address	Mesh ID	Model	Role	Status
☐		10.115.11.233	5.158.92.168	IW9165E-B	Fixed Infrastructure	●
☑		10.115.11.141	5.21.201.60	IW9167EH-Q	Gateway	●
☑	Cisco-127.234.232	10.115.11.147	5.127.234.232	IW9165E-B	Gateway	●
☐	Cisco-21.200.24	10.115.11.119	5.21.200.24	IW9167EH-B	Gateway	●
☐	Cisco-212.77.244	10.115.11.133	5.212.77.244	IW9167EH-B	Gateway	●
☐	Cisco-test-tenant	10.115.11.128	5.21.201.112	IW9167EH-ROW	Fixed Infrastructure	●
☐	CiscoURWB-name	10.115.11.231	5.158.92.176	IW9165E-B	Gateway	●

17 Records 1 - 10 ‹‹ ‹ 1 2 › ››

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:



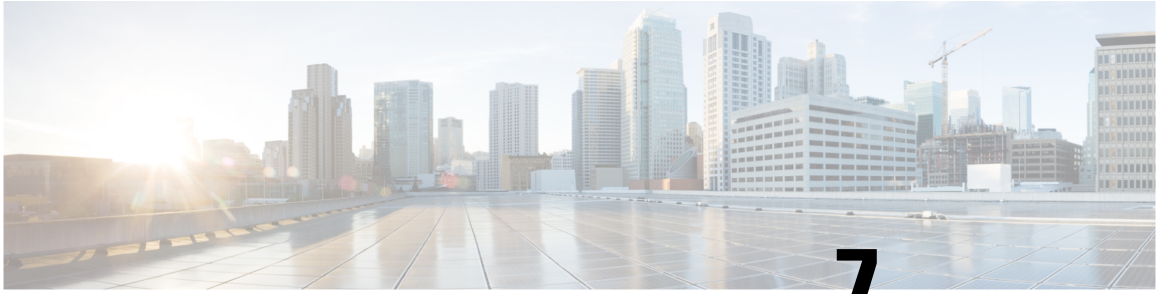
Detach report

Detached These devices have been detached successfully 1/1

10.115.11.90	5.0.178.85	4200	Cisco

Okay

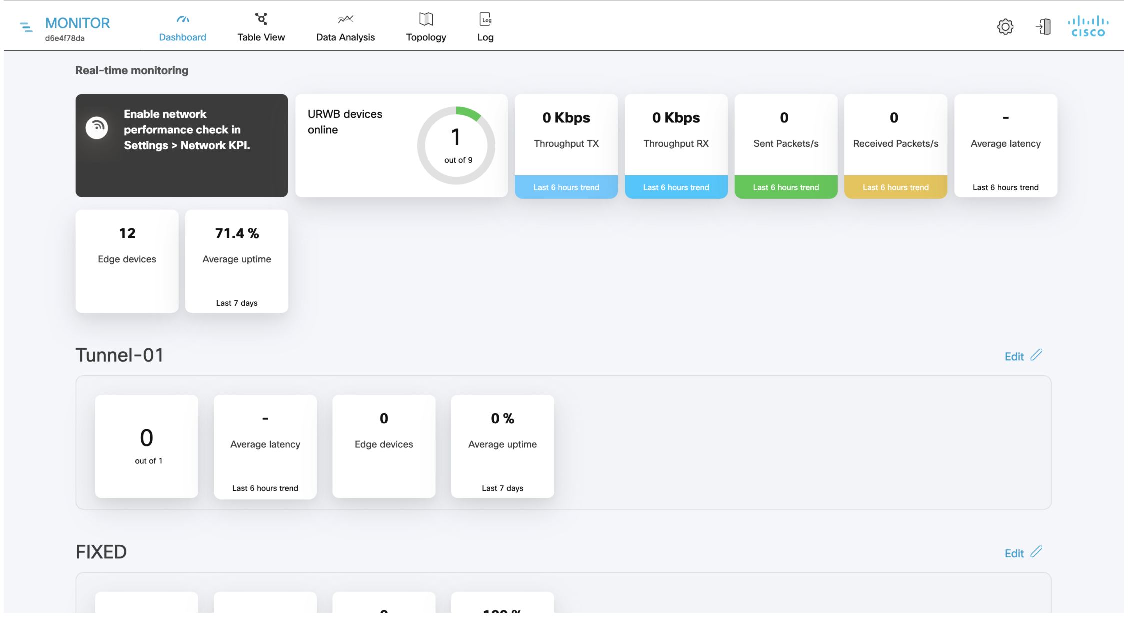
Step 5 To remove a device from the IW Monitor using the Configurator interface's detach function, see Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide.



CHAPTER 7

Monitoring Network Performance

Viewing the Network Statistics



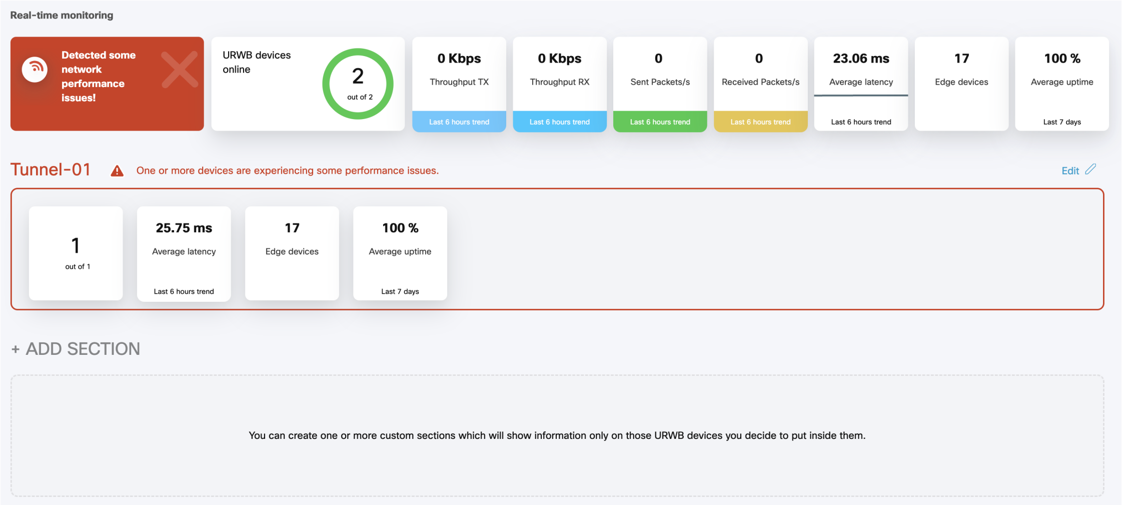
Enable network performance check in Settings > Network KPI.

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 Create a new Section, on page 23.



Real-time monitoring

Detected some network performance issues!

URWB devices online 2 out of 2

0 Kbps	0 Kbps	0	0	23.06 ms	17	100 %
Throughput TX	Throughput RX	Sent Packets/s	Received Packets/s	Average latency	Edge devices	Average uptime
Last 6 hours trend	Last 6 hours trend	Last 6 hours trend	Last 6 hours trend	Last 6 hours trend		Last 7 days

Tunnel-01 One or more devices are experiencing some performance issues. Edit

1	25.75 ms	17	100 %
out of 1	Average latency	Edge devices	Average uptime
	Last 6 hours trend		Last 7 days

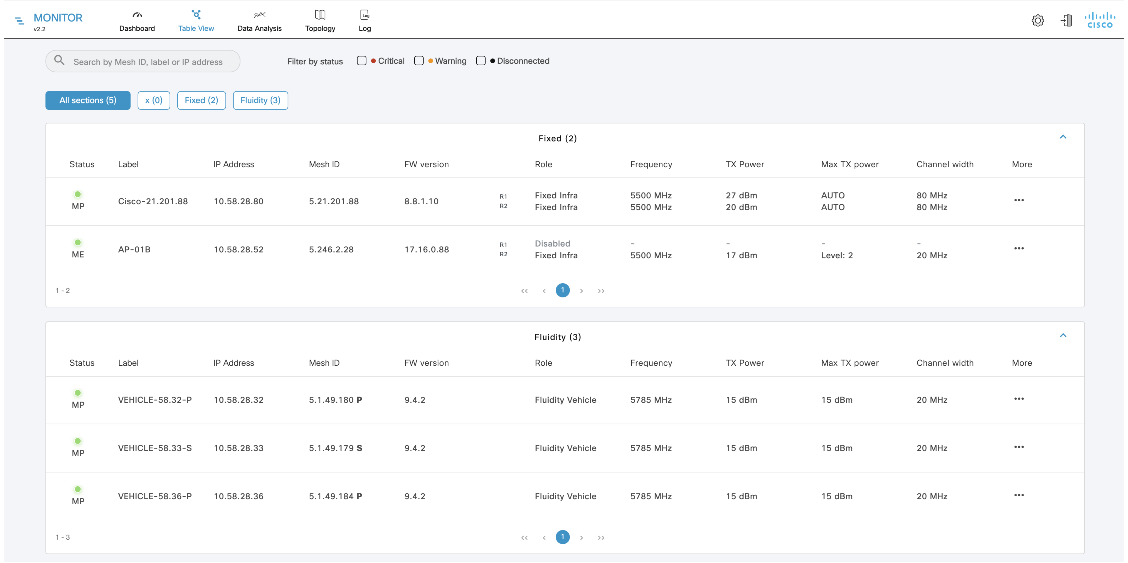
+ ADD SECTION

You can create one or more custom sections which will show information only on those URWB devices you decide to put inside them.

Viewing the Devices using Table View

Procedure

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



Fixed (2)

Status	Label	IP Address	Mesh ID	FW version		Role	Frequency	TX Power	Max TX power	Channel width	More
● MP	Cisco-21.201.88	10.58.28.80	5.21.201.88	8.8.1.10	R1 R2	Fixed Infra Fixed Infra	5500 MHz 5500 MHz	27 dBm 20 dBm	AUTO AUTO	80 MHz 80 MHz	•••
● ME	AP-01B	10.58.28.52	5.246.2.28	17.16.0.88	R1 R2	Disabled Fixed Infra	- 5500 MHz	- 17 dBm	- Level: 2	- 20 MHz	•••

1 - 2

Fluidity (3)

Status	Label	IP Address	Mesh ID	FW version	Role	Frequency	TX Power	Max TX power	Channel width	More
● MP	VEHICLE-58.32-P	10.58.28.32	5.1.49.180 **P**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••
● MP	VEHICLE-58.33-S	10.58.28.33	5.1.49.179 **S**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••
● MP	VEHICLE-58.36-P	10.58.28.36	5.1.49.184 **P**	9.4.2	Fluidity Vehicle	5785 MHz	15 dBm	15 dBm	20 MHz	•••

1 - 3

- All the devices that are not assigned to any specific sections are shown under **Uncategorized**. To add uncategorized devices to a specific section, see Create 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:

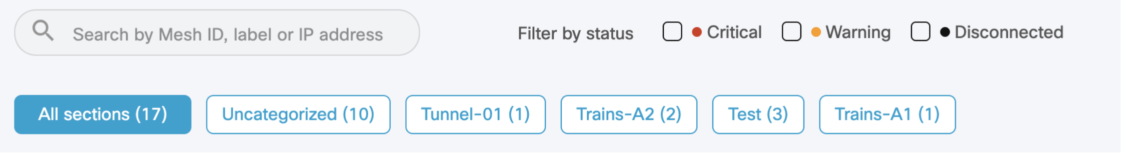
Parameter	Description
Status (icon color and designation)	Icon colors represent the following device status: • **Green**: Device is online and connected to an IW Monitor with all the performance levels in an acceptable range. • **Gray**: Device is disconnected from IW Monitor. • **Orange**: Device is 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 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.
Max TX Power	Shows the user-defined value of the radio device’s maximum transmission power level. **Note** For dual-radio devices, the **Max TX Power** parameter is shown for each radio interface.

Parameter	Description
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.

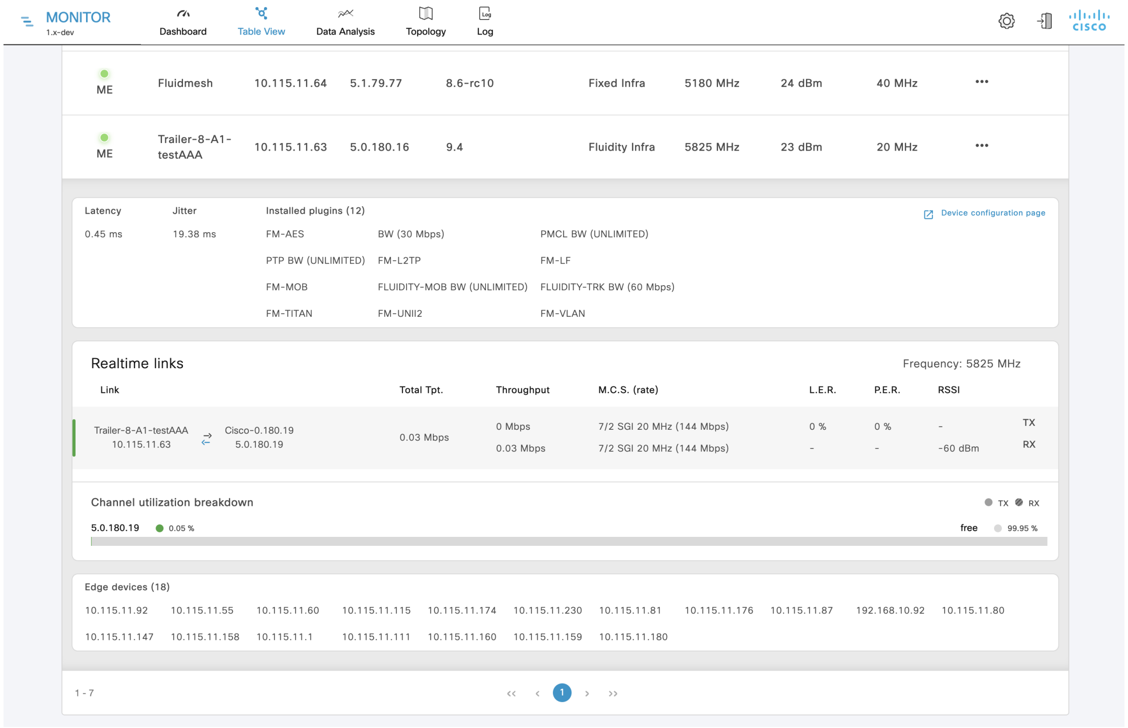


- The **Critical** filter allows you to view the list of devices for which the thresholds are beyond the upper threshold limit.
- The **Warning** filter allows you to view the list of devices for which the thresholds are between the upper and lower threshold limits.
- The **Disconnected** filter allows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

Viewing the Uplink and Downlink Information for a Device

Procedure

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



● ME	Fluidmesh	10.115.11.64	5.1.79.77	8.6-rc10	Fixed Infra	5180 MHz	24 dBm	40 MHz	•••
● ME	Trailer-8-A1-testAAA	10.115.11.63	5.0.180.16	9.4	Fluidity Infra	5825 MHz	23 dBm	20 MHz	•••

Latency	Jitter	Installed plugins (12)		
0.45 ms	19.38 ms	FM-AES	BW (30 Mbps)	PMCL BW (UNLIMITED)
		PTP BW (UNLIMITED)	FM-L2TP	FM-LF
		FM-MOB	FLUIDITY-MOB BW (UNLIMITED)	FLUIDITY-TRK BW (60 Mbps)
		FM-TITAN	FM-UNII2	FM-VLAN

Device configuration page

Realtime links

Frequency: 5825 MHz

Link		Total Tpt.	Throughput	M.C.S. (rate)	L.E.R.	P.E.R.	RSSI	
Trailer-8-A1-testAAA 10.115.11.63	Cisco-0.180.19 5.0.180.19	0.03 Mbps	0 Mbps	7/2 SGI 20 MHz (144 Mbps)	0 %	0 %	-	TX
			0.03 Mbps	7/2 SGI 20 MHz (144 Mbps)	-	-	-60 dBm	RX

Channel utilization breakdown

● TX ● RX

5.0.180.19 ● 0.05 %

free ● 99.95 %

Edge devices (18)

10.115.11.92	10.115.11.55	10.115.11.60	10.115.11.115	10.115.11.174	10.115.11.230	10.115.11.81	10.115.11.176	10.115.11.87	192.168.10.92	10.115.11.80
10.115.11.147	10.115.11.158	10.115.11.1	10.115.11.111	10.115.11.160	10.115.11.159	10.115.11.180				

1 - 7

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.

Parameter	Description
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.
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.

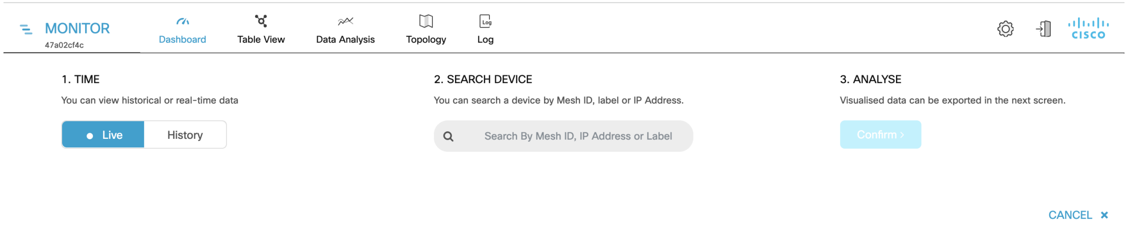
Viewing Device Statistics in Real Time

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.

Procedure

Step 1 Click **Data Analysis**.

A new screen extends as shown below:



MONITOR 47a02cf4c | Dashboard | Table View | Data Analysis | Topology | Log

1. TIME
You can view historical or real-time data
● Live | History

2. SEARCH DEVICE
You can search a device by Mesh ID, label or IP Address.
Search By Mesh ID, IP Address or Label

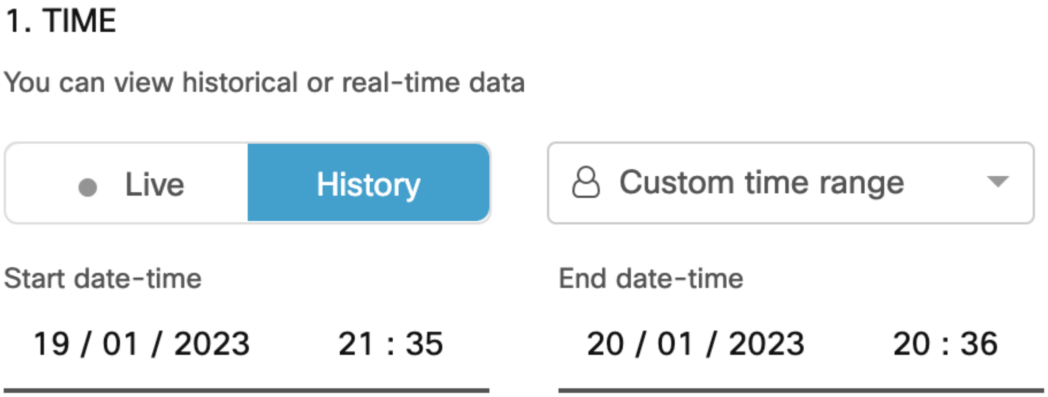
3. ANALYSE
Visualised data can be exported in the next screen.
Confirm ›

CANCEL ×

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.



1. TIME

You can view historical or real-time data

● Live | History

Custom time range

Start date-time
19 / 01 / 2023 21 : 35

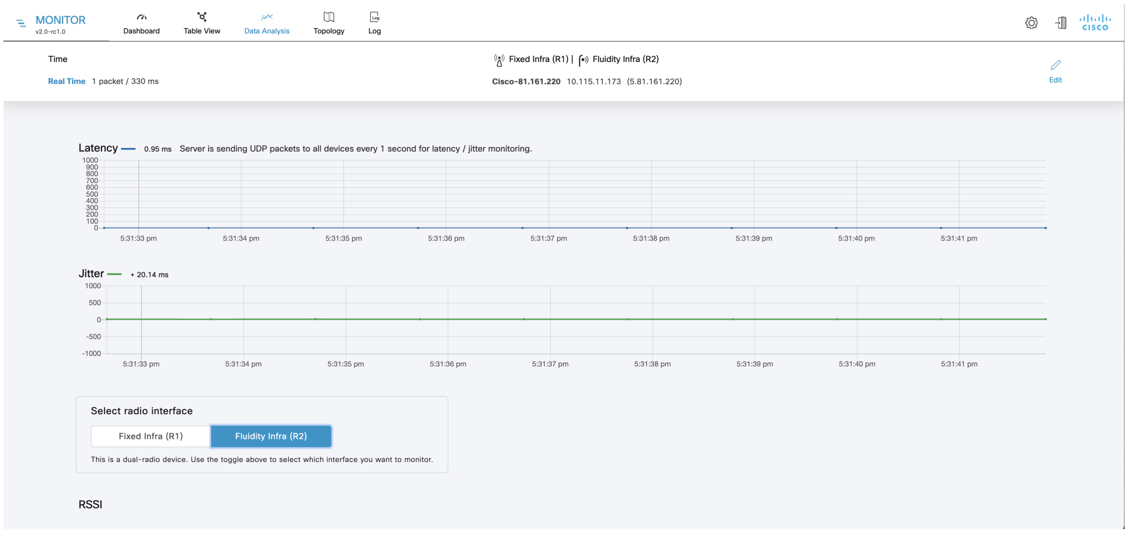
End date-time
20 / 01 / 2023 20 : 36

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**.



Time

Real Time 1 packet / 330 ms

Fixed Infra (R1) | Fluidity Infra (R2)

Cisco-81.161.220 10.115.11.173 (5.81.161.220)

Latency 0.95 ms Server is sending UDP packets to all devices every 1 second for latency / jitter monitoring.

Jitter + 20.14 ms

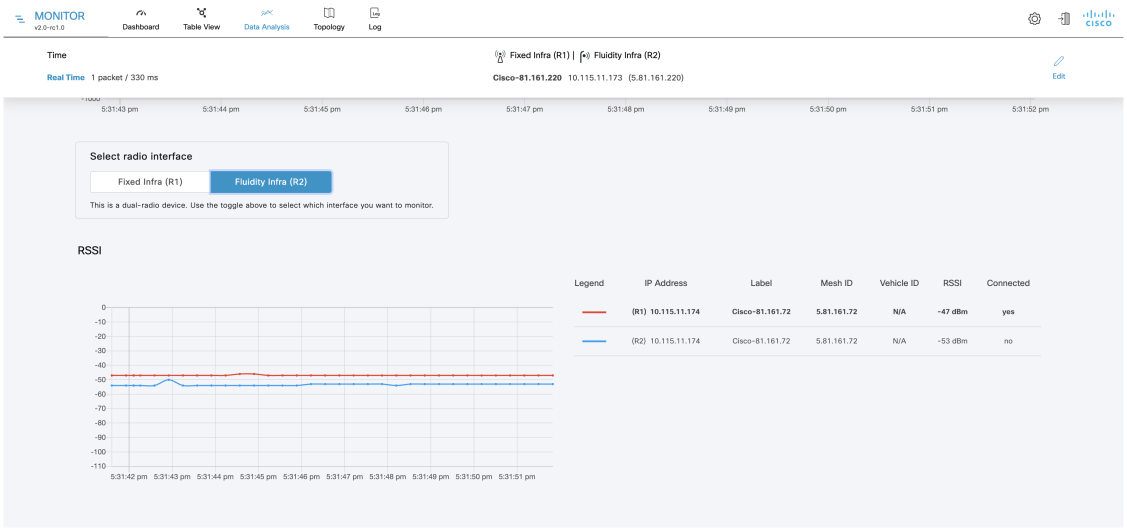
Select radio interface

This is a dual-radio device. Use the toggle above to select which interface you want to monitor.

RSSI

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:



Time

Real Time 1 packet / 330 ms

Fixed Infra (R1) | Fluidity Infra (R2)

Cisco-81.161.220 10.115.11.173 (5.81.161.220)

Select radio interface

This is a dual-radio device. Use the toggle above to select which interface you want to monitor.

RSSI

Legend	IP Address	Label	Mesh ID	Vehicle ID	RSSI	Connected
🟥	**(R1) 10.115.11.174**	**Cisco-81.161.72**	**5.81.161.72**	**N/A**	**-47 dBm**	**yes**
🟦	(R2) 10.115.11.174	Cisco-81.161.72	5.81.161.72	N/A	-53 dBm	no

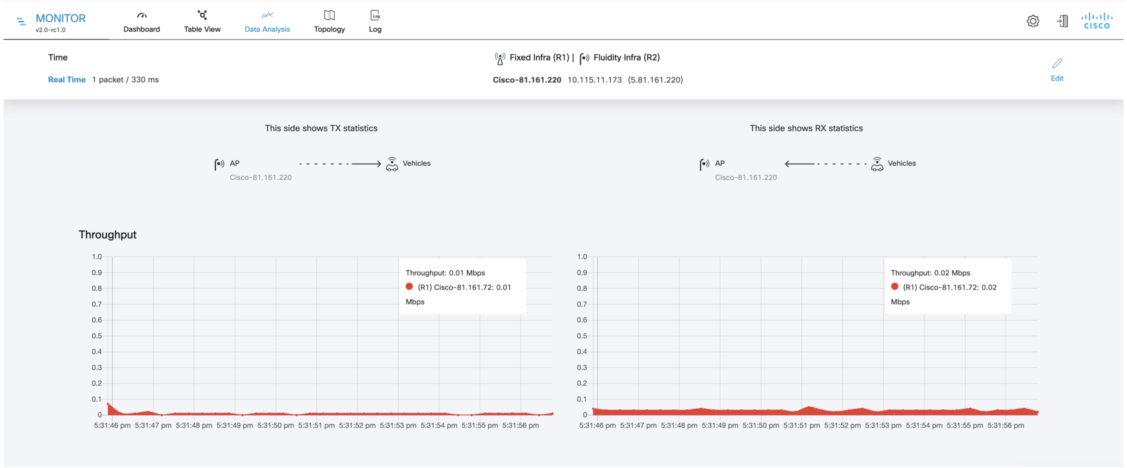
- The upper left corner of the graph shows whether the device currently accepts handoff requests.
- If the chosen device is currently connected to a Fluidity-enabled (vehicle-mounted) radio unit, a thick, dashed black line is superimposed over the Fluidity device's RSSI line. This line is the RSSI envelope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

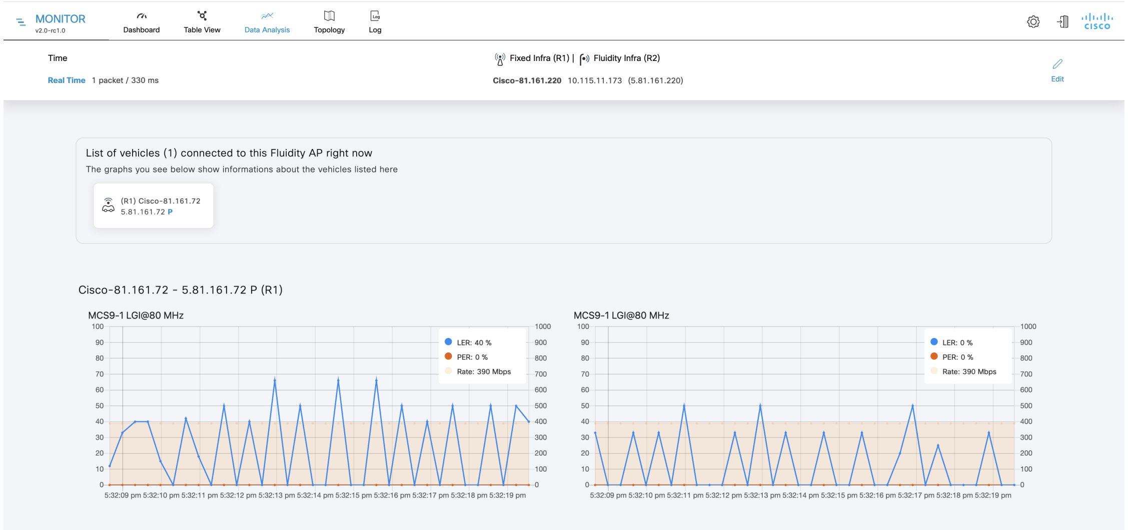
b. The Throughput graphs show the throughput statistics as a function of Mbps/time. The throughput is shown for the selected device and the device to which the chosen device is currently connected.

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).


MONITOR
v2.0-rc1.0
Dashboard
Table View
Data Analysis
Topology
Log
cisco
Time
Real Time 1 packet / 330 ms
Fixed Infra (R1) | Fluidity Infra (R2)
Cisco-81.161.220 10.115.11.173 (5.81.161.220)
Edit
This side shows TX statistics
AP
Cisco-81.161.220
Vehicles
This side shows RX statistics
AP
Cisco-81.161.220
Vehicles
Throughput
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Throughput: 0.01 Mbps
(R1) Cisco-81.161.72: 0.01 Mbps
Throughput: 0.02 Mbps
(R1) Cisco-81.161.72: 0.02 Mbps
5:31:46 pm 5:31:47 pm 5:31:48 pm 5:31:49 pm 5:31:50 pm 5:31:51 pm 5:31:52 pm 5:31:53 pm 5:31:54 pm 5:31:55 pm 5:31:56 pm

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.

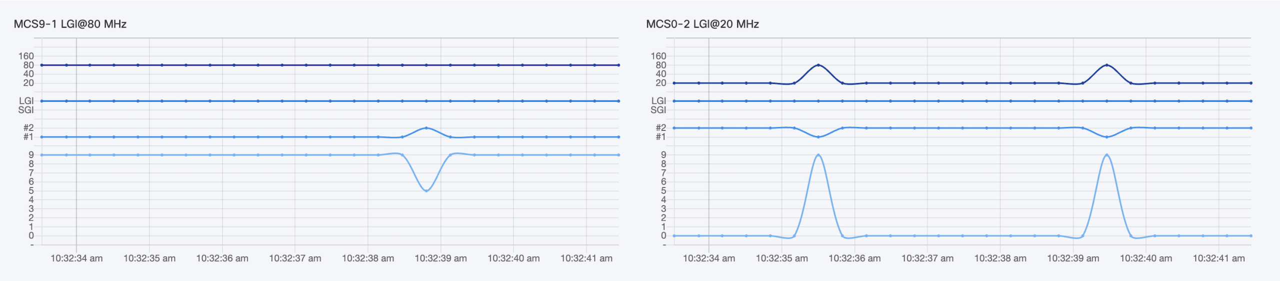
Note
The left graph shows uplink statistics (data flow from the current device), while the right graph shows downlink statistics (data flow to the current device).


MONITOR
v2.0-rc1.0
Dashboard
Table View
Data Analysis
Topology
Log
cisco
Time
Real Time 1 packet / 330 ms
Fixed Infra (R1) | Fluidity Infra (R2)
Cisco-81.161.220 10.115.11.173 (5.81.161.220)
Edit
List of vehicles (1) connected to this Fluidity AP right now
The graphs you see below show informations about the vehicles listed here
(R1) Cisco-81.161.72
5.81.161.72 P
Cisco-81.161.72 - 5.81.161.72 P (R1)
MCS9-1 LGI@80 MHz
MCS9-1 LGI@80 MHz
100
90
80
70
60
50
40
30
20
10
0
1000
900
800
700
600
500
400
300
200
100
0
LER: 40 %
PER: 0 %
Rate: 390 Mbps
LER: 0 %
PER: 0 %
Rate: 390 Mbps
5:32:09 pm 5:32:10 pm 5:32:11 pm 5:32:12 pm 5:32:13 pm 5:32:14 pm 5:32:15 pm 5:32:16 pm 5:32:17 pm 5:32:18 pm 5:32:19 pm

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.

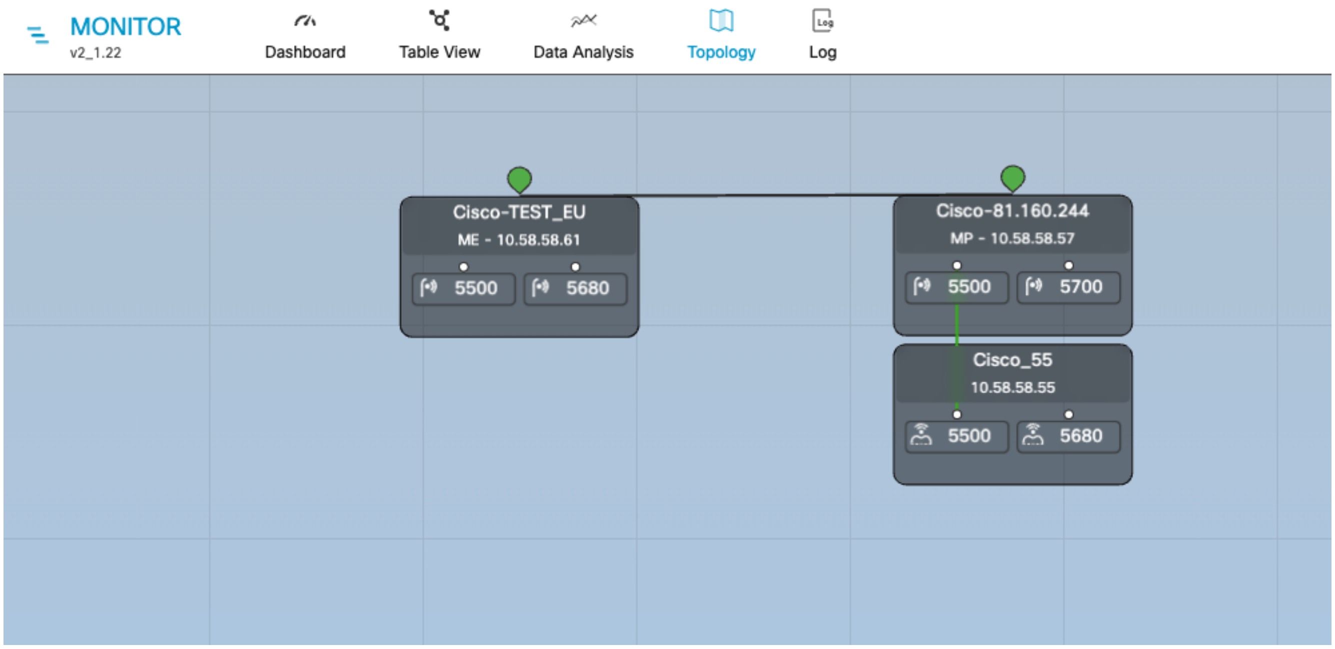
Step 5 Click **Edit** to view the statistical view for another device.

Viewing the Devices from Topology

Procedure

Step 1 Click Topology **Topology**.

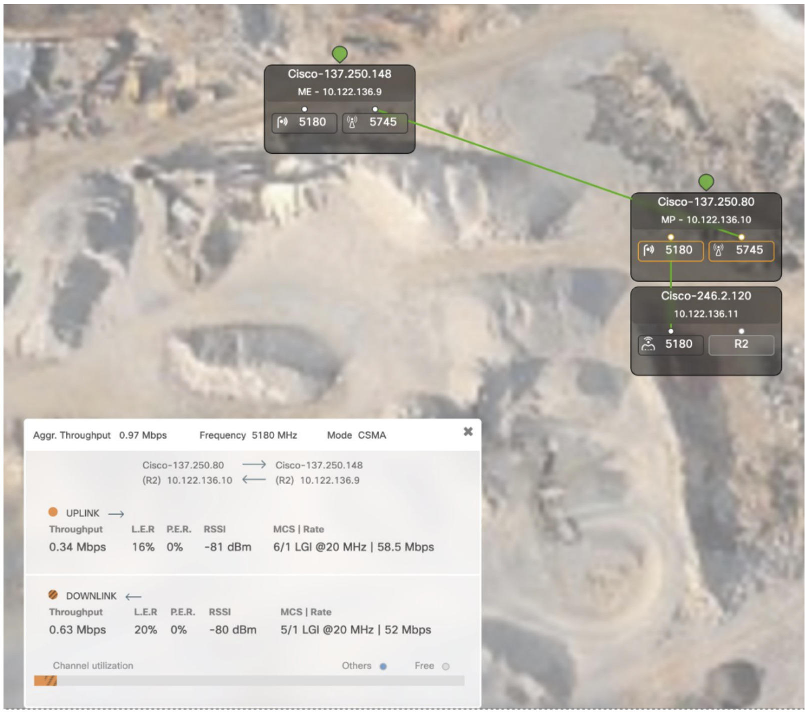
A new screen appears with topology.



Step 2 Click on the device for more details.

Step 3 Click on the wireless link or a mobile unit.

A new screen appears as shown.



Aggr. Throughput 0.97 Mbps   Frequency 5180 MHz   Mode CSMA

Cisco-137.250.80 ⟶ Cisco-137.250.148
(R2) 10.122.136.10 ⟵ (R2) 10.122.136.9

UPLINK ⟶

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.34 Mbps	16%	0%	-81 dBm	6/1 LGI @20 MHz | 58.5 Mbps

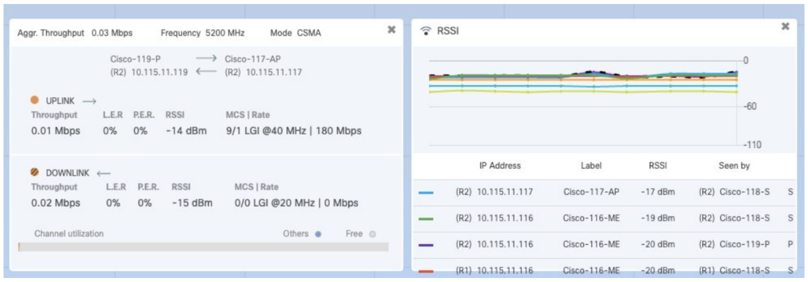
DOWNLINK ⟵

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.63 Mbps	20%	0%	-80 dBm	5/1 LGI @20 MHz | 52 Mbps

Channel utilization   Others ●   Free ○

Step 4 Click on the Fluidity Vehicle Unit.

A new screen appears as shown.



Aggr. Throughput 0.03 Mbps   Frequency 5200 MHz   Mode CSMA

Cisco-119-P ⟶ Cisco-117-AP
(R2) 10.115.11.119 ⟵ (R2) 10.115.11.117

UPLINK ⟶

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.01 Mbps	0%	0%	-14 dBm	9/1 LGI @40 MHz | 180 Mbps

DOWNLINK ⟵

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.02 Mbps	0%	0%	-15 dBm	0/0 LGI @20 MHz | 0 Mbps

Channel utilization   Others ●   Free ○

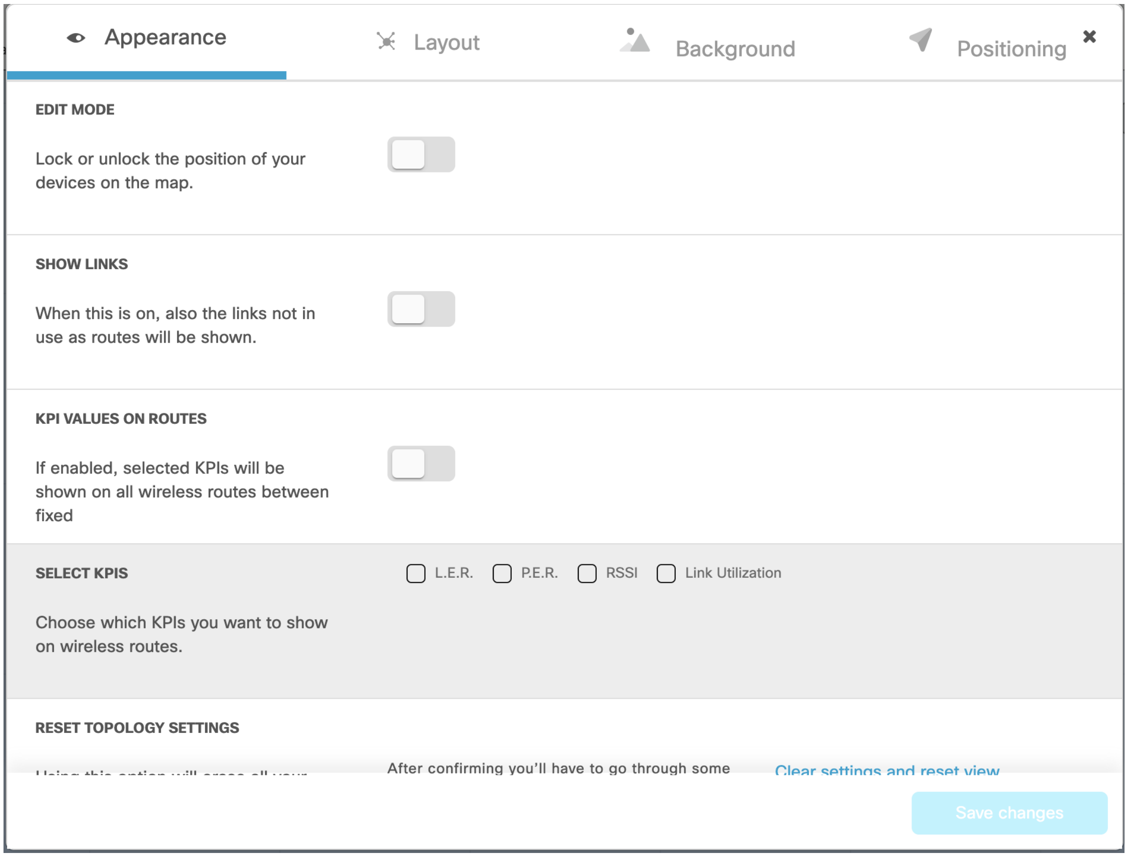
	IP Address	Label	RSSI	Seen by	
—	(R2) 10.115.11.117	Cisco-117-AP	-17 dBm	(R2) Cisco-118-S	S
—	(R2) 10.115.11.116	Cisco-116-ME	-19 dBm	(R2) Cisco-118-S	S
—	(R2) 10.115.11.116	Cisco-116-ME	-20 dBm	(R2) Cisco-119-P	P
—	(R1) 10.115.11.116	Cisco-116-ME	-20 dBm	(R1) Cisco-118-S	S

Step 5 Click on **Web page** and it redirects to the respective web interface of the device.

Step 6 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.



EDIT MODE

Lock or unlock the position of your devices on the map.

SHOW LINKS

When this is on, also the links not in use as routes will be shown.

KPI VALUES ON ROUTES

If enabled, selected KPIs will be shown on all wireless routes between fixed

SELECT KPIS

□ L.E.R. □ P.E.R. □ RSSI □ Link Utilization

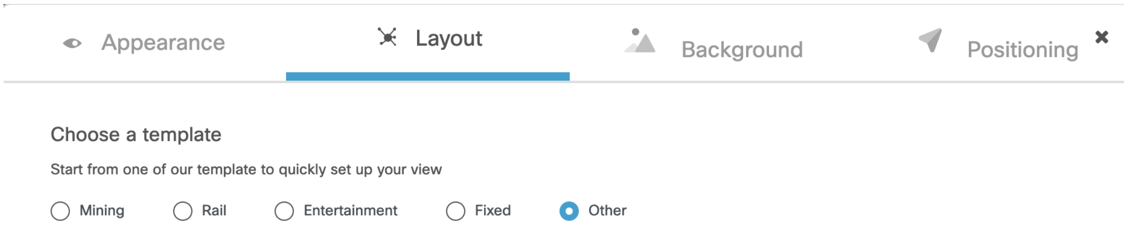
Choose which KPIs you want to show on wireless routes.

RESET TOPOLOGY SETTINGS

Using this option will erase all your

After confirming you'll have to go through some

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

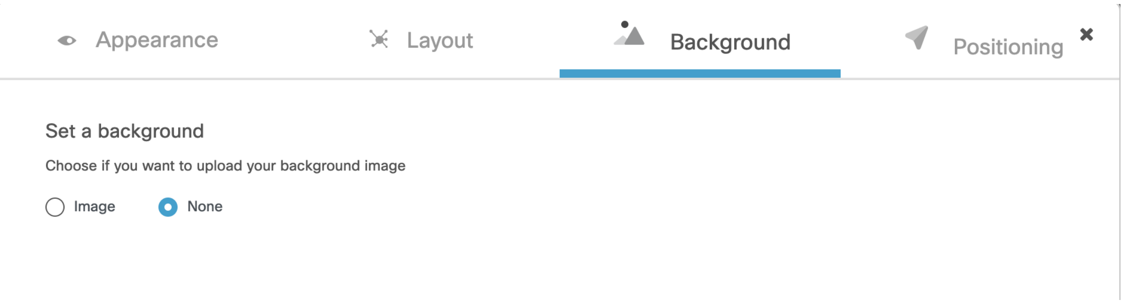


Choose a template

Start from one of our template to quickly set up your view

○ Mining ○ Rail ○ Entertainment ○ Fixed ● Other

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



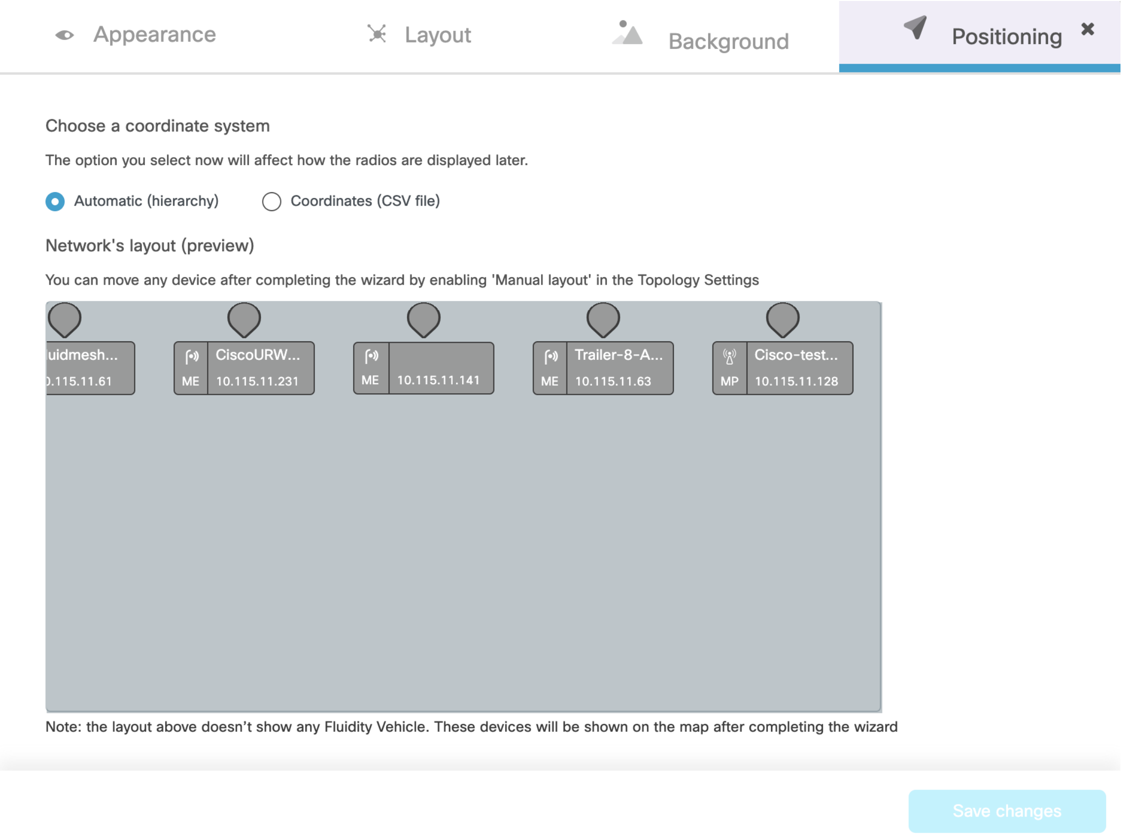
Set a background

Choose if you want to upload your background image

○ Image ● None

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.



Choose a coordinate system

The option you select now will affect how the radios are displayed later.

● Automatic (hierarchy) ○ Coordinates (CSV file)

Network's layout (preview)

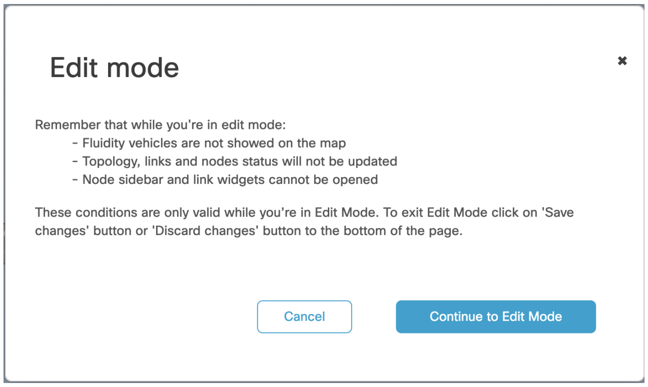
You can move any device after completing the wizard by enabling 'Manual layout' in the Topology Settings

Note: the layout above doesn't show any Fluidity Vehicle. These devices will be shown on the map after completing the wizard

Step 7 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**.



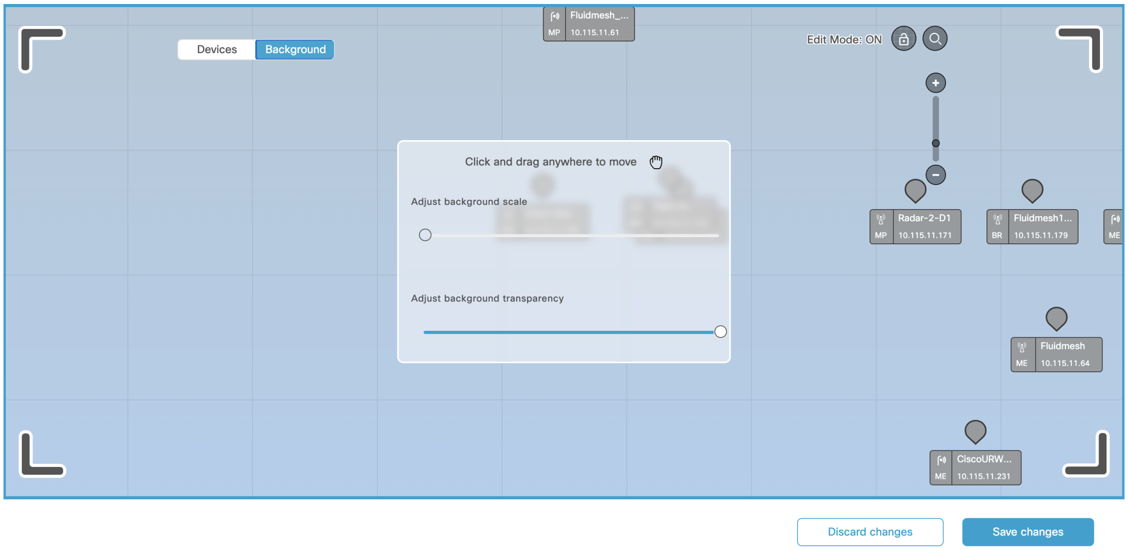
Edit mode

Remember that while you're in edit mode:
- Fluidity vehicles are not showed on the map
- Topology, links and nodes status will not be updated
- Node sidebar and link widgets cannot be opened

These conditions are only valid while you're in Edit Mode. To exit Edit Mode click on 'Save changes' button or 'Discard changes' button to the bottom of the page.

- 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 8 Click 🔍 **Zoom** to zoom in/out the topology view.

Step 9 Enable MPO.

a) Click **Settings** icon at the top right corner of the screen.

b) Select **MPO** > **Enable MPO Processing.**

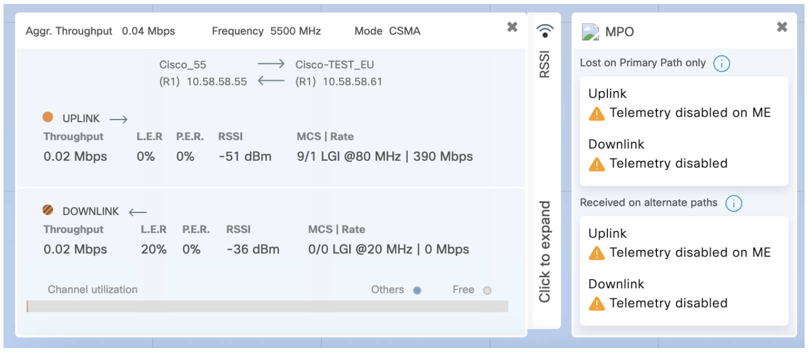
c) Select **Time Window** and granularity. For example, 1minute to 59 minutes and 1hour to 24hours.

d) Click **Save Changes.**

Step 10 Enable MPO telemetry on both Mesh Ends and Fluidity. See the Software Configuration Guide to use the CLI commands.

Step 11 Click Fluidity Vehicle Unit in the topology.

If the MPO telemetry is not enabled, you see warning messages.



Aggr. Throughput 0.04 Mbps Frequency 5500 MHz Mode CSMA

Cisco_55 (R1) 10.58.58.55 ⟶ ⟵ Cisco-TEST_EU (R1) 10.58.58.61

UPLINK ⟶

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.02 Mbps	0%	0%	-51 dBm	9/1 LGI @80 MHz | 390 Mbps

DOWNLINK ⟵

Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
0.02 Mbps	20%	0%	-36 dBm	0/0 LGI @20 MHz | 0 Mbps

MPO

Lost on Primary Path only

Uplink
⚠ Telemetry disabled on ME

Downlink
⚠ Telemetry disabled

Received on alternate paths

Uplink
⚠ Telemetry disabled on ME

Downlink
⚠ Telemetry disabled

If MPO telemetry is enabled, you should see the following metrics:

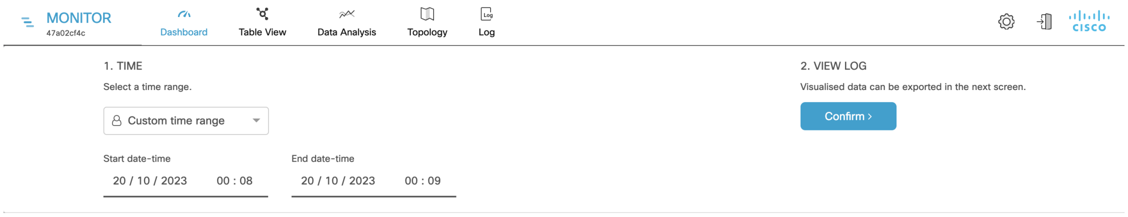
Metrics	Description
Lost on Primary Path only	This metrics provides details about number of packets lost, or received out-of-order on the primary MPO path only, over the total number of packets sent on the primary path.
Received on alternate paths	This metrics provides details about the number of packets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

Filtering and Viewing Network Events

Procedure

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

A new screen extends as shown below:



1. TIME

Select a time range.

Custom time range

Start date-time 20 / 10 / 2023 00 : 08

End date-time 20 / 10 / 2023 00 : 09

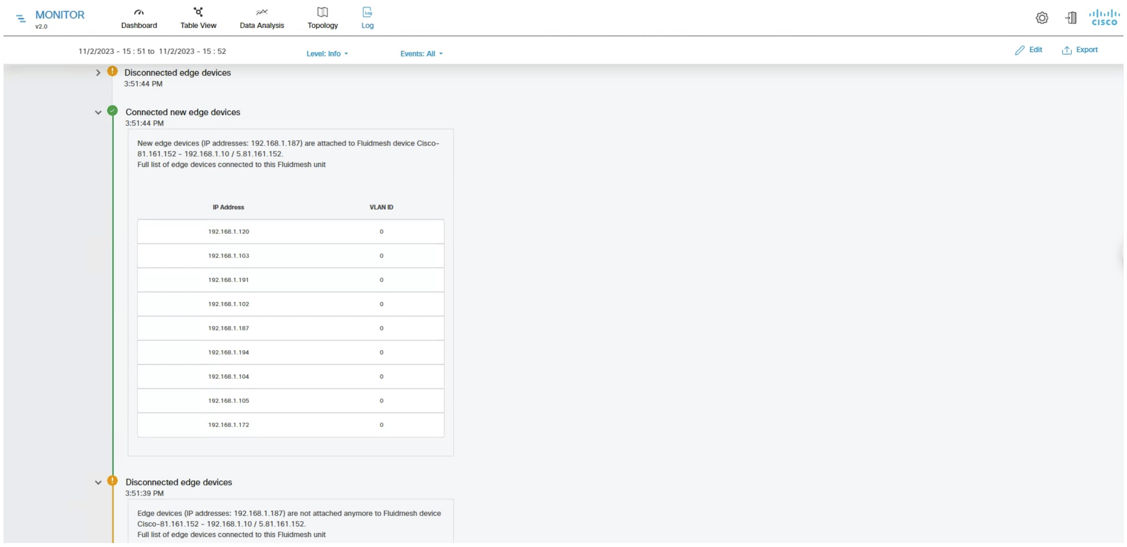
2. VIEW LOG

Visualised data can be exported in the next screen.

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.



11/2/2023 - 15 : 51 to 11/2/2023 - 15 : 52

Level: Info

Events: All

Disconnected edge devices
3:51:44 PM

Connected new edge devices
3:51:44 PM

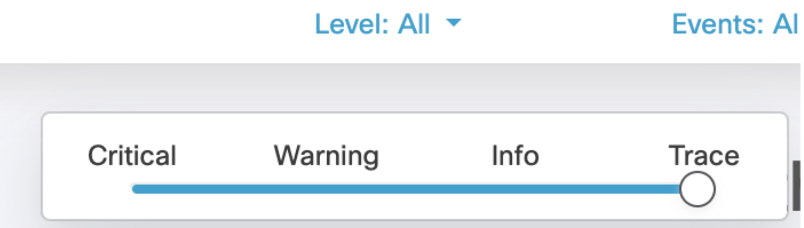
New edge devices (IP addresses: 192.168.1.187) are attached to Fluidmesh device Cisco-81.161.152 - 192.168.1.10 / 5.81.161.152.
Full list of edge devices connected to this Fluidmesh unit

IP Address	VLAN ID
192.168.1.120	0
192.168.1.103	0
192.168.1.191	0
192.168.1.102	0
192.168.1.187	0
192.168.1.194	0
192.168.1.104	0
192.168.1.105	0
192.168.1.172	0

Disconnected edge devices
3:51:39 PM

Edge devices (IP addresses: 192.168.1.187) are not attached anymore to Fluidmesh device Cisco-81.161.152 - 192.168.1.10 / 5.81.161.152.
Full list of edge devices connected to this Fluidmesh unit

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.

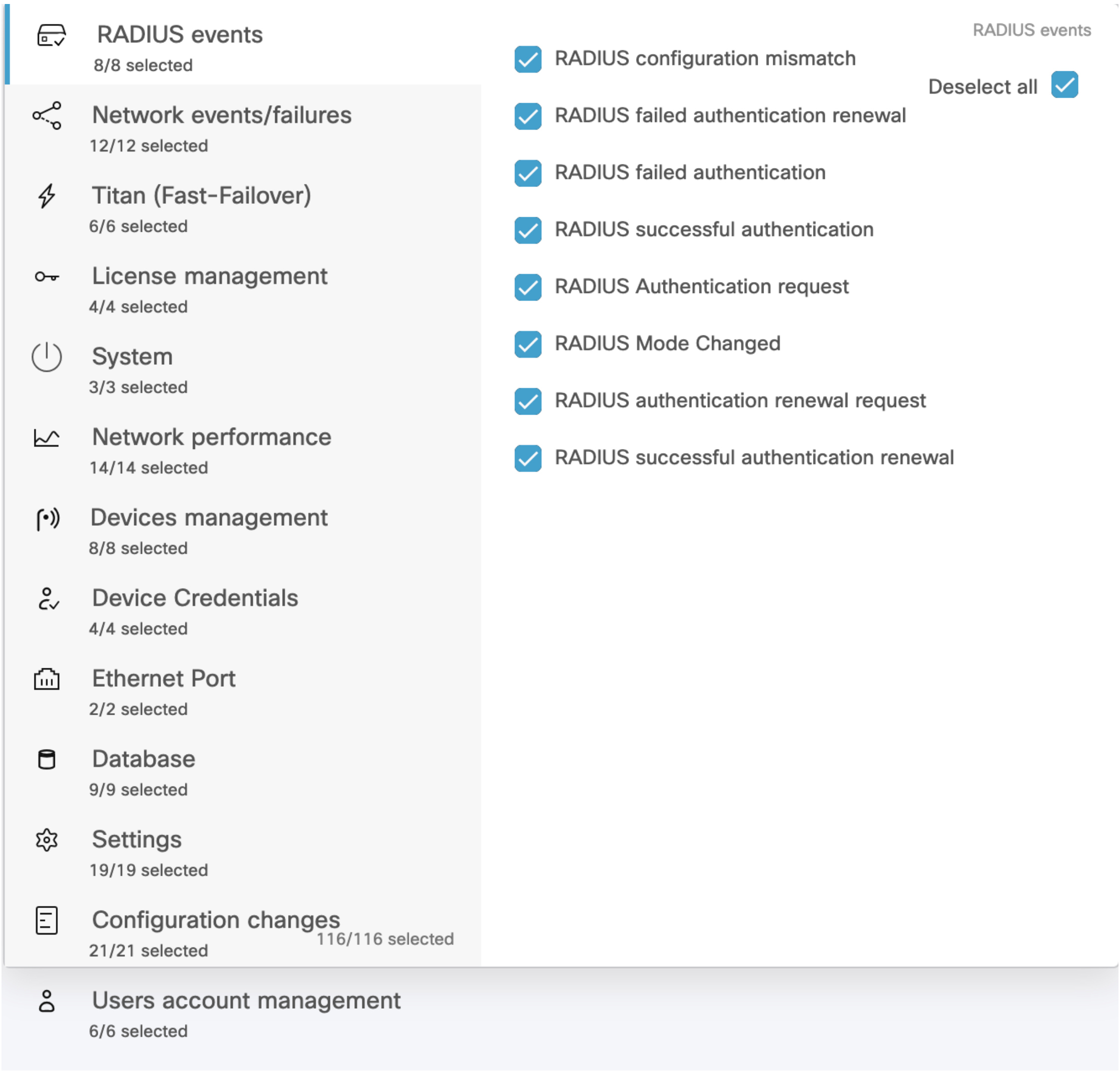
b) In the pop-up, click the relevant category from left pane, and select the check-boxes for the required network event.

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**.



RADIUS events
8/8 selected

Network events/failures
12/12 selected

Titan (Fast-Failover)
6/6 selected

License management
4/4 selected

System
3/3 selected

Network performance
14/14 selected

Devices management
8/8 selected

Device Credentials
4/4 selected

Ethernet Port
2/2 selected

Database
9/9 selected

Settings
19/19 selected

Configuration changes
21/21 selected

116/116 selected

Users account management
6/6 selected

RADIUS events

Deselect all ☑

☑ RADIUS configuration mismatch
☑ RADIUS failed authentication renewal
☑ RADIUS failed authentication
☑ RADIUS successful authentication
☑ RADIUS Authentication request
☑ RADIUS Mode Changed
☑ RADIUS authentication renewal request
☑ RADIUS successful authentication renewal

Exporting a Network Event Log as a CSV File

Procedure

Step 1 Request the log of network events as mentioned in Filtering and Viewing Network Events, on page 47.

Step 2 Click .

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

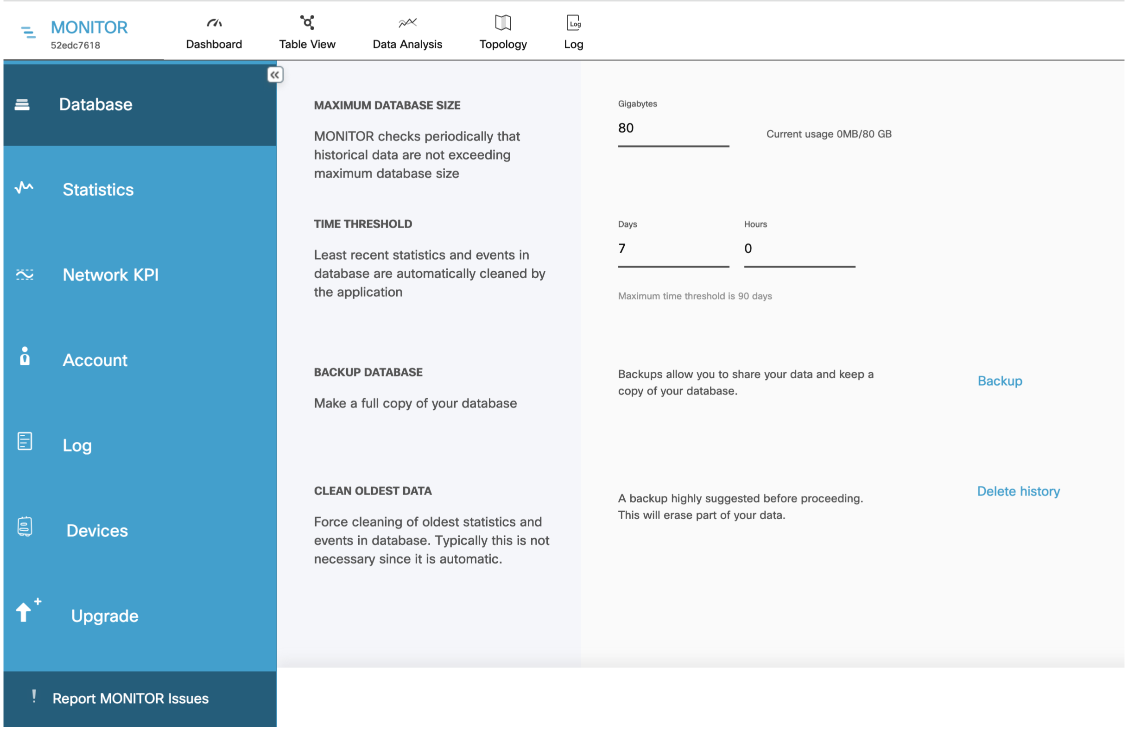
Configuring IW Monitor Database Settings

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

Procedure

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

The database settings page is shown.



MAXIMUM DATABASE SIZE

MONITOR checks periodically that historical data are not exceeding maximum database size

Gigabytes: 80

Current usage 0MB/80 GB

TIME THRESHOLD

Least recent statistics and events in database are automatically cleaned by the application

Days: 7

Hours: 0

Maximum time threshold is 90 days

BACKUP DATABASE

Make a full copy of your database

Backups allow you to share your data and keep a copy of your database.

CLEAN OLDEST DATA

Force cleaning of oldest statistics and events in database. Typically this is not necessary since it is automatic.

A backup highly suggested before proceeding. This will erase part of your data.

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.

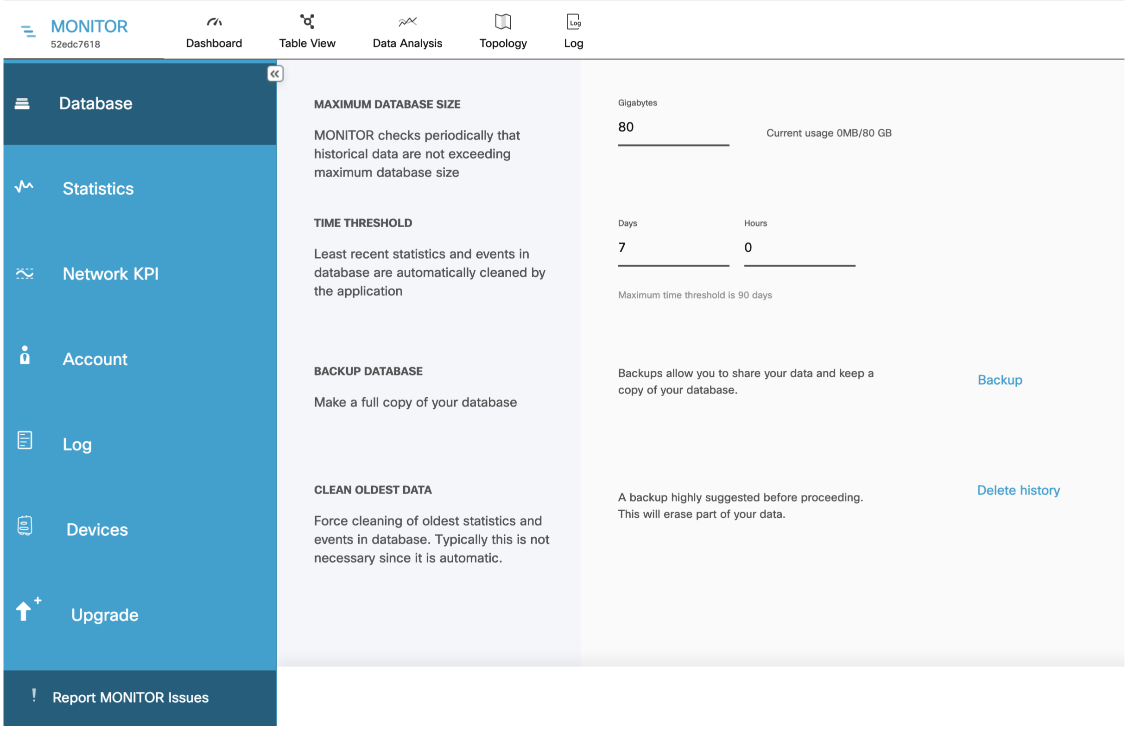
Note
The minimum amount of time-related network-statistics data that can be stored before overwrite is one hour, and the maximum amount of time-related data that can be stored before overwrite is 90 days.

Backing up the IW Monitor Statistics Database

Procedure

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

The database settings page is shown.



MAXIMUM DATABASE SIZE

MONITOR checks periodically that historical data are not exceeding maximum database size

Gigabytes: 80

Current usage 0MB/80 GB

TIME THRESHOLD

Least recent statistics and events in database are automatically cleaned by the application

Days: 7

Hours: 0

Maximum time threshold is 90 days

BACKUP DATABASE

Make a full copy of your database

Backups allow you to share your data and keep a copy of your database.

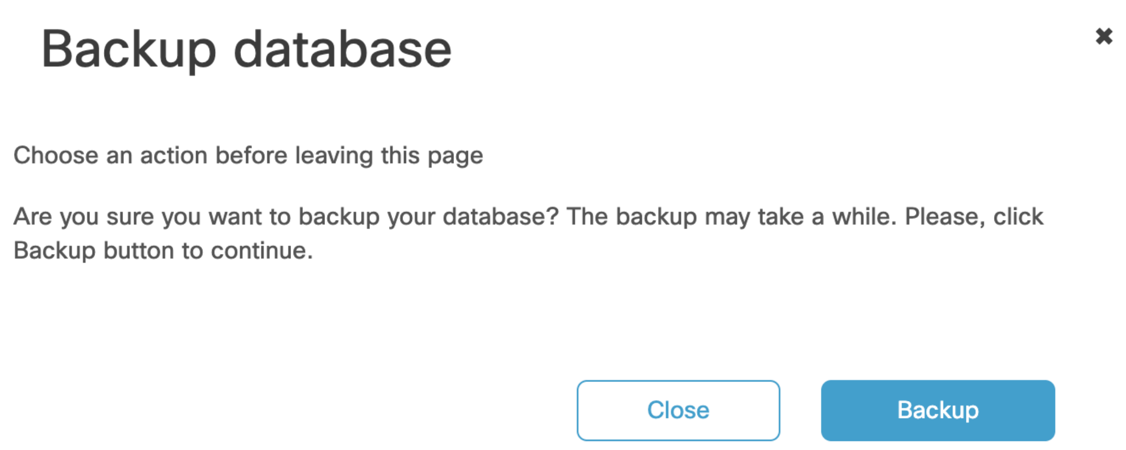
CLEAN OLDEST DATA

Force cleaning of oldest statistics and events in database. Typically this is not necessary since it is automatic.

A backup highly suggested before proceeding. This will erase part of your data.

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

A confirmation pop-up appears.



Backup database

Choose an action before leaving this page

Are you sure you want to backup your database? The backup may take a while. Please, click Backup button to continue.

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

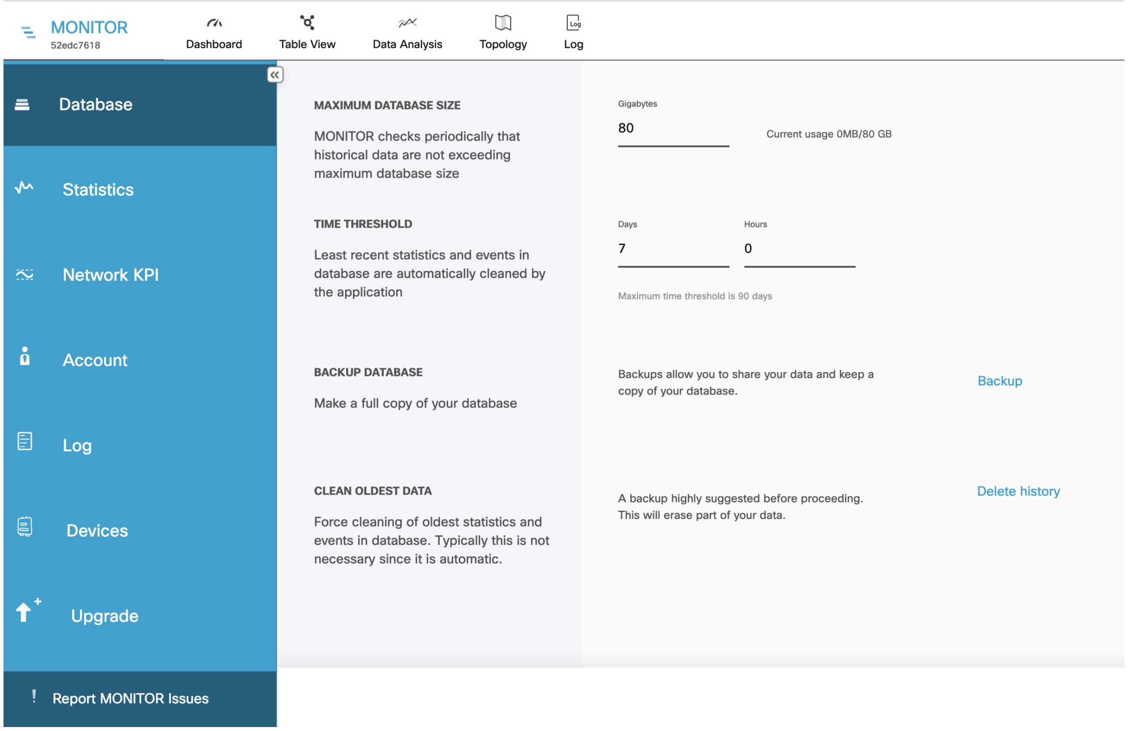
You can manually delete the oldest statistics and event data in the IW Monitor database if you feel that excessive amounts of network statistics data are being written to the hard disk in short periods of time.

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 53.

Procedure

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

The database settings page is shown.



MAXIMUM DATABASE SIZE

MONITOR checks periodically that historical data are not exceeding maximum database size

Gigabytes: 80

Current usage 0MB/80 GB

TIME THRESHOLD

Least recent statistics and events in database are automatically cleaned by the application

Days: 7

Hours: 0

Maximum time threshold is 90 days

BACKUP DATABASE

Make a full copy of your database

Backups allow you to share your data and keep a copy of your database.

Backup

CLEAN OLDEST DATA

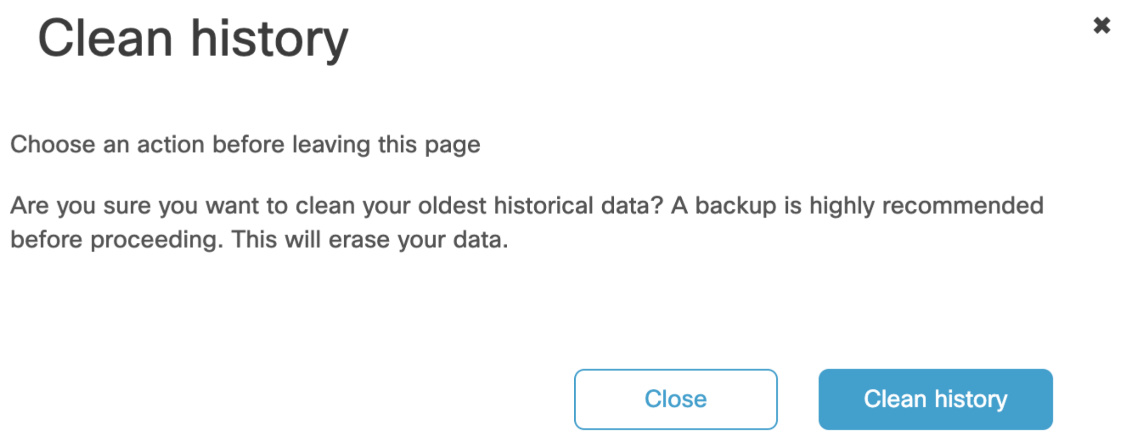
Force cleaning of oldest statistics and events in database. Typically this is not necessary since it is automatic.

A backup highly suggested before proceeding. This will erase part of your data.

Delete history

Step 2 Click **Delete history**.

A confirmation pop-up appears.


Clean history

Choose an action before leaving this page

Are you sure you want to clean your oldest historical data? A backup is highly recommended before proceeding. This will erase your data.

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

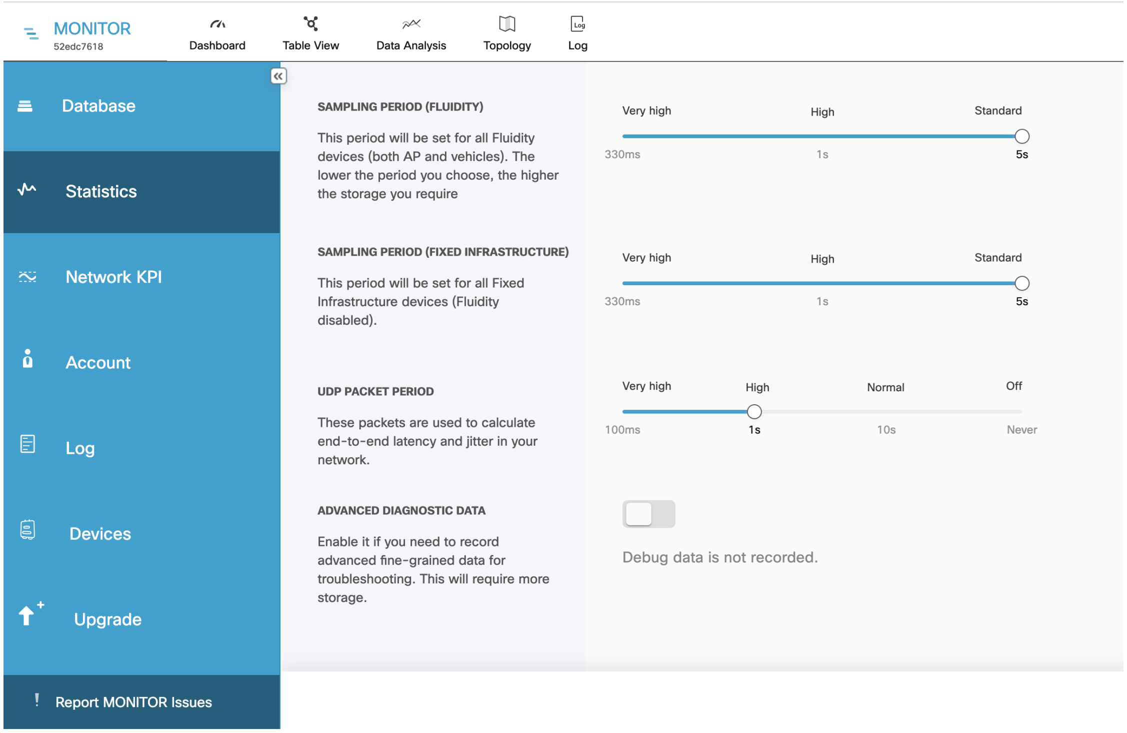
Procedure

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.



SAMPLING PERIOD (FLUIDITY)

This period will be set for all Fluidity devices (both AP and vehicles). The lower the period you choose, the higher the storage you require

SAMPLING PERIOD (FIXED INFRASTRUCTURE)

This period will be set for all Fixed Infrastructure devices (Fluidity disabled).

UDP PACKET PERIOD

These packets are used to calculate end-to-end latency and jitter in your network.

ADVANCED DIAGNOSTIC DATA

Enable it if you need to record advanced fine-grained data for troubleshooting. This will require more storage.

Debug data is not recorded.

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)

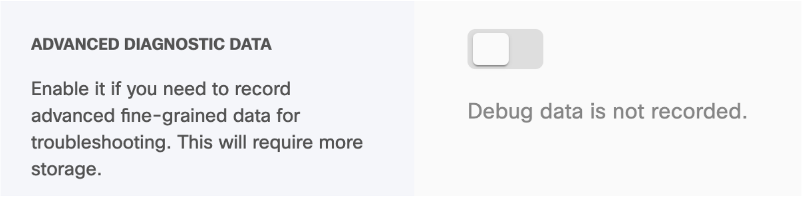
Note

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.



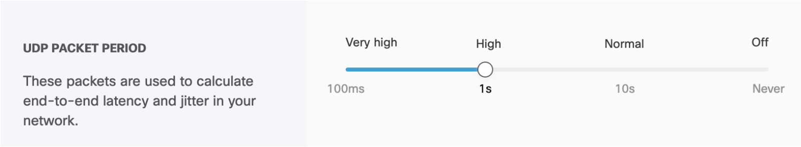
ADVANCED DIAGNOSTIC DATA

Enable it if you need to record advanced fine-grained data for troubleshooting. This will require more storage.

Debug data is not recorded.

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.



UDP PACKET PERIOD

These packets are used to calculate end-to-end latency and jitter in your network.

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

Procedure

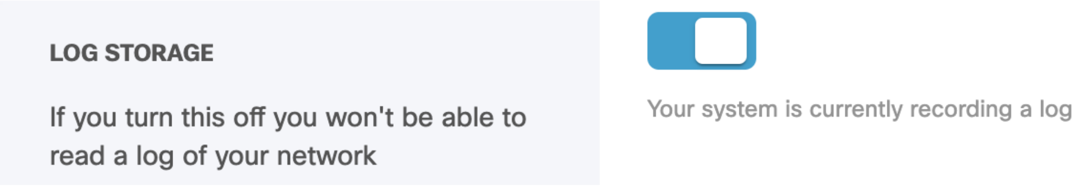
Step 1 Click ⚙ **Settings** in the top right corner.

A new settings page is shown.

Step 2 Click Log.

The log settings page is shown.

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

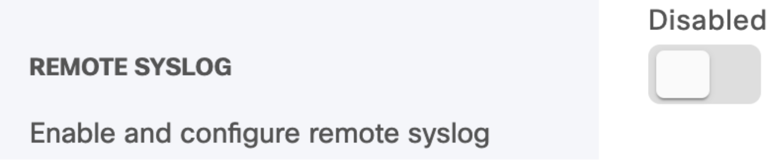


LOG STORAGE

If you turn this off you won't be able to read a log of your network

Your system is currently recording a log

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



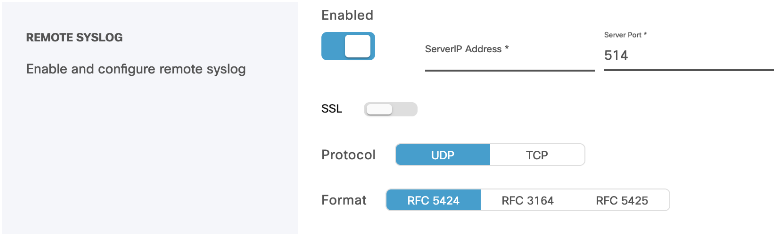
REMOTE SYSLOG

Enable and configure remote syslog

Disabled

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.



REMOTE SYSLOG

Enable and configure remote syslog

Enabled: on

ServerIP Address *

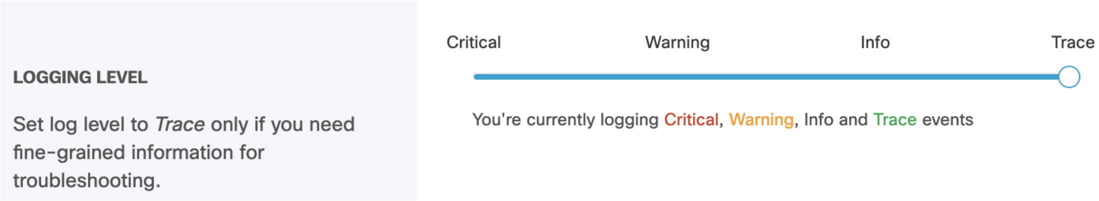
Server Port *: 514

SSL: off

Protocol: UDP (selected), TCP

Format: RFC 5424 (selected), RFC 3164, RFC 5425

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



LOGGING LEVEL

Set log level to *Trace* only if you need fine-grained information for troubleshooting.

You're currently logging Critical, Warning, Info and Trace events

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**.

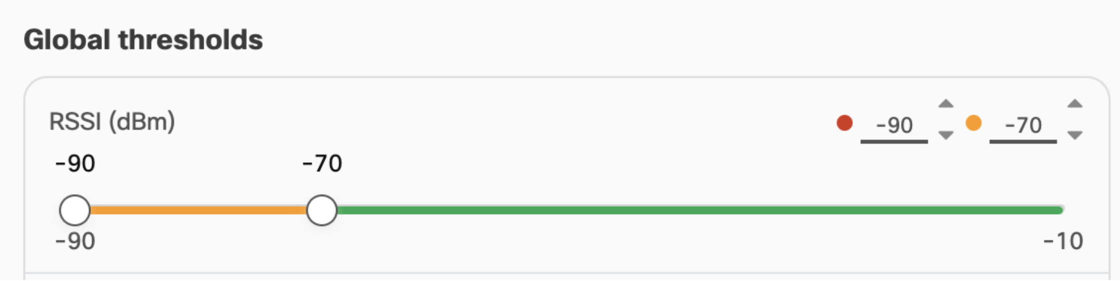
Setting Performance Thresholds

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 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.



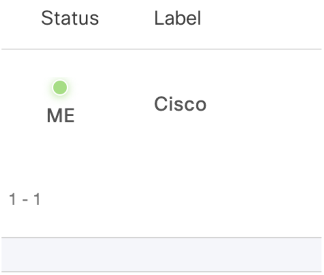
Global thresholds

RSSI (dBm) ● -90 ● -70

-90 -70

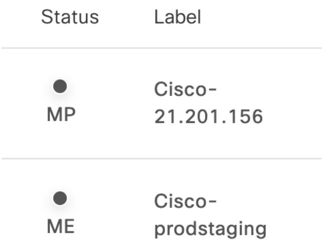
-90 -10

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.



Status	Label
● ME	Cisco

1 - 1



Status	Label
● MP	Cisco- 21.201.156
● ME	Cisco- prodstaging

Setting Performance Thresholds for Each Section

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

Procedure

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

A new settings page is shown.

Step 2 Click Network KPI.

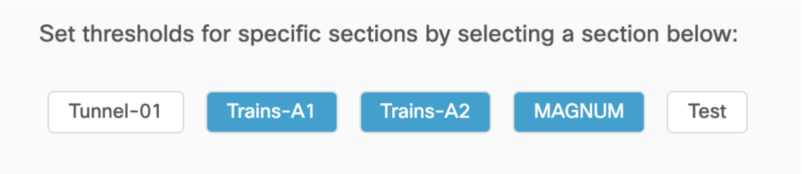
The network KPI settings page is shown.

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 Create a new Section, on page 23.

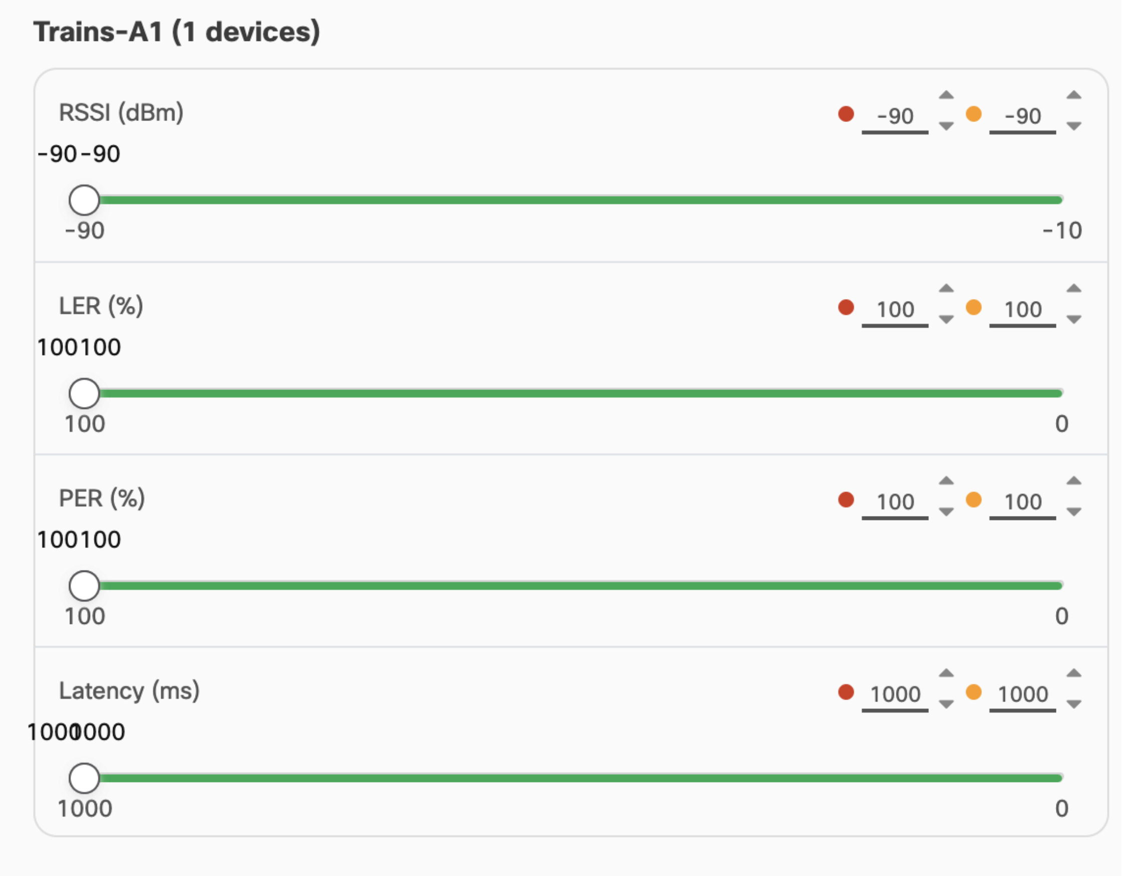
Step 5 If the network is partitioned, tabs are created for each network section under **Global Thresholds** sliders as shown below:



Set thresholds for specific sections by selecting a section 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 61.



Trains-A1 (1 devices)

RSSI (dBm) ● -90 ● -90
-90-90
-90 -10

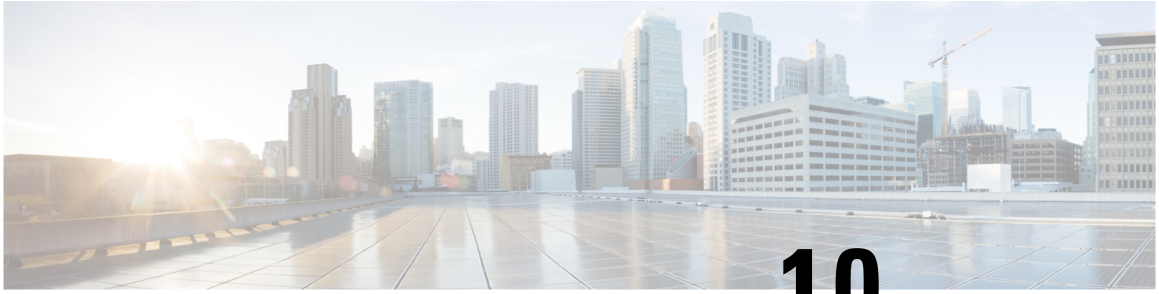
LER (%) ● 100 ● 100
100100
100 0

PER (%) ● 100 ● 100
100100
100 0

Latency (ms) ● 1000 ● 1000
10001000
1000 0

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

Procedure

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

Procedure

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) Select the user specific role in the **Role** dropdown field, either **Admin** or **Viewmode**.

- Admin: The user can perform all operations available in IW-MONITOR.
- Viewmode: The user has read-only access to IW-MONITOR.

  Viewmode users do not have access to these operations:

  - Create, edit, or delete sections
  - Save time range in Data Analysis - History
  - Update positions of the nodes in topology
  - Update topology settings
  - Update MONITOR settings
  - Invite other users
  - Upgrade MONITOR
  - Attach new devices to MONITOR
  - Detach devices from MONITOR

Note
The first user registered to IW-MONITOR through the wizard is assigned the Admin role only.

e) 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.

f) Click 👁 (eye icon) to view the generated password for the new user.
g) 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 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**.

Reset a password for another user

Reset a user’s password in case of security concerns or if the user forgets their password.

Before you begin

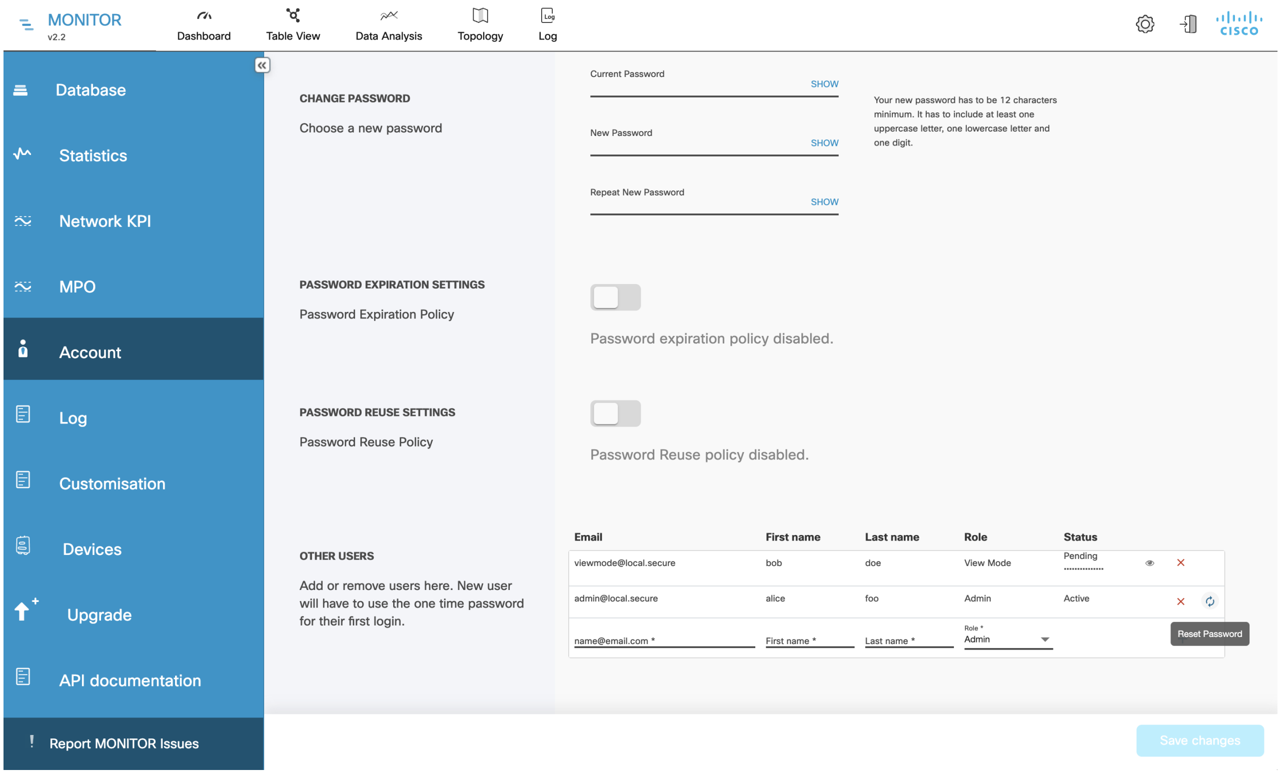
- Only Admin users can reset passwords for other users.

Procedure

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

Step 2 In the **Other Users** table, select the user whose password you want to reset.

Step 3 If the user does not have a temporary password, "reset" icon appears automatically, click on it.



CHANGE PASSWORD

Choose a new password

Current Password

New Password

Repeat New Password

Your new password has to be 12 characters minimum. It has to include at least one uppercase letter, one lowercase letter and one digit.

PASSWORD EXPIRATION SETTINGS

Password Expiration Policy

Password expiration policy disabled.

PASSWORD REUSE SETTINGS

Password Reuse Policy

Password Reuse policy disabled.

OTHER USERS

Add or remove users here. New user will have to use the one time password for their first login.

Email	First name	Last name	Role	Status
viewmode@local.secure	bob	doe	View Mode	Pending ••••••••••••••
admin@local.secure	alice	foo	Admin	Active
name@email.com *	First name *	Last name *	Role * Admin	

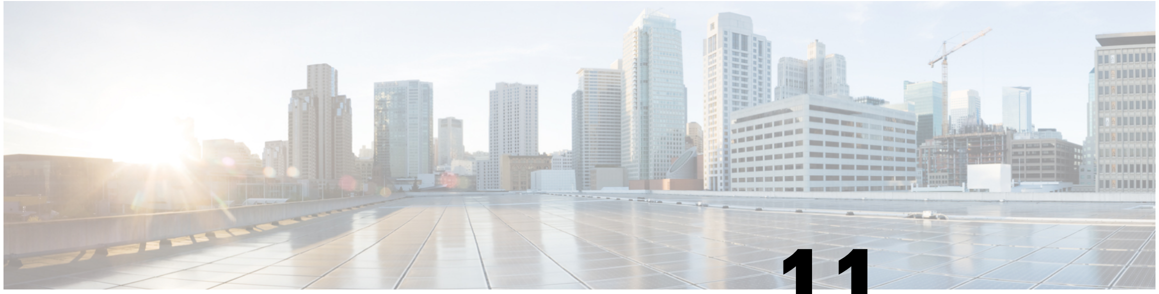
Step 4 Click **Confirm** to proceed.

The system generates a temporary secure password for the user.

Step 5 Provide the temporary password to the user.

Note
The temporary password does not expire.

Step 6 When the user logs in with the temporary password, they will be required to set a new password.



CHAPTER 11

Updating IW Monitor

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.

Procedure

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.

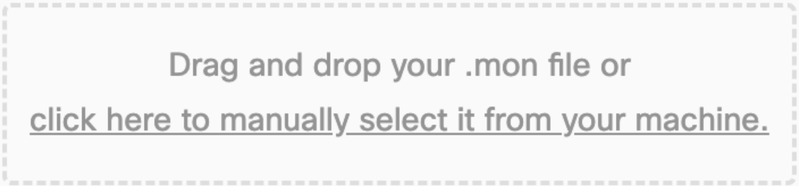
Step 3 Click ⚙ **Settings** in the top right corner.

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.



Drag and drop your .mon file or

click here to manually select it from your machine.

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

Uninstalling IW Monitor

Uninstalling 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.

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.