Converged Public Transportation - Mass Transit

Implementation Guide (CVD)

October 2023

Cisco Validated Design

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED "AS IS." ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY 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 BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Introduction 4

Cisco IR1800 managed by IoT OD 5

CAPWAP mode for IoT OD IR1800 Wi-Fi 25

Cisco IR1800 managed by SD-WAN Manager 25

WAN Failover Operation 26

CURWB Backhaul Managed with IoT OD 29

C9800 WLC Configuration for IR1800 Wi-Fi in CAPWAP Mode with Captive Portal 42

Configure WLAN 42
WLAN General 43
WLAN Security 44
Configure Profiles 47
Configure Tags 50
Verify 52

Secure Equipment Access to Onboard Equipment 53

IOx Applications 61

Example Vehicle CANBUS Data Application 61

Bus Services 64

Automatic Passenger Counting with DILAX 65
Emissions Monitoring with SensorComm Wi-NOx 67
Video Surveillance with AXIS and Milestone 70
Voice Communication with InstantConnect 75

Additional Resources 77

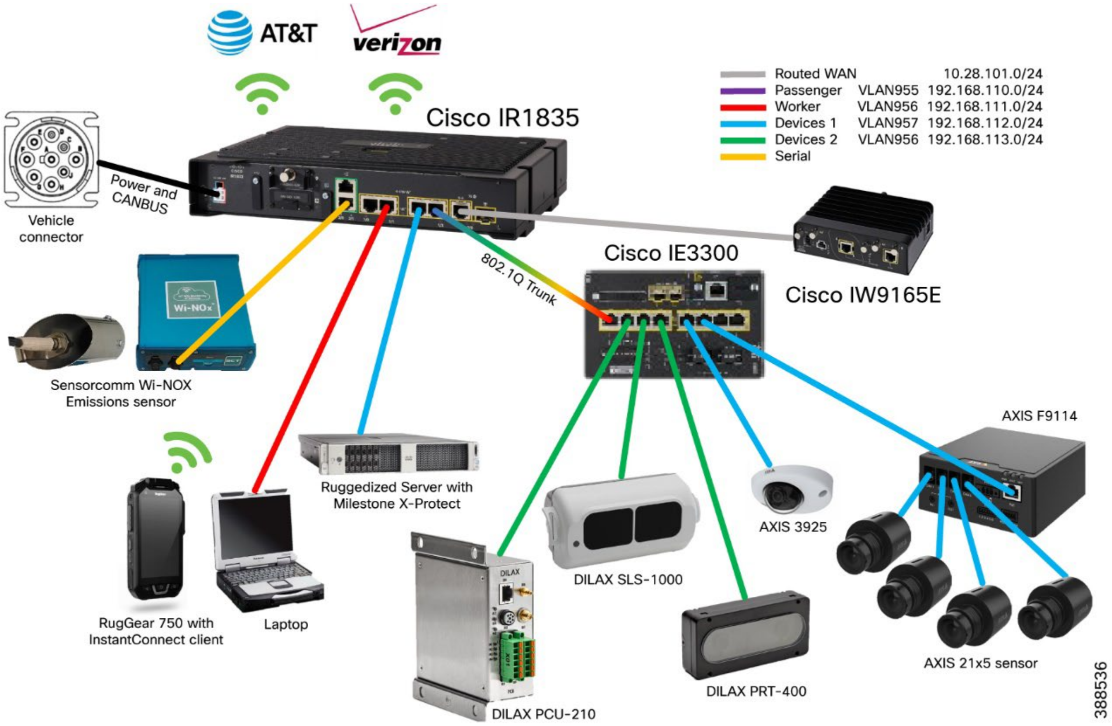
Cisco References 77
Third-party References 77

Introduction

The configurations in this implementation guide are based on the topology shown below. The IR1835 router and subtended IE3300 switch are used to connect the various devices on the bus. Some sections, like the example vehicle CANBUS IOX application, and the third-party bus services components are only covered at a high level to show what is possible in a Mass Transit deployment, not to document specific configuration steps.

Multiple VLANs are used to provide segmentation between different devices connected behind the IR1800 router as depicted in the color-coded key in the diagram that follows.

Figure 1. IR1835 Mass Transit Equipment Physical Topology


AT&T
verizon
Routed WAN 10.28.101.0/24
Passenger VLAN955 192.168.110.0/24
Worker VLAN956 192.168.111.0/24
Devices 1 VLAN957 192.168.112.0/24
Devices 2 VLAN956 192.168.113.0/24
Serial
Cisco IR1835
Power and CANBUS
Vehicle connector
802.1Q Trunk
Cisco IE3300
Cisco IW9165E
Sensorcomm Wi-NOX Emissions sensor
Ruggedized Server with Milestone X-Protect
AXIS F9114
AXIS 3925
DILAX SLS-1000
RugGear 750 with InstantConnect client
Laptop
DILAX PRT-400
AXIS 21x5 sensor
DILAX PCU-210
388536

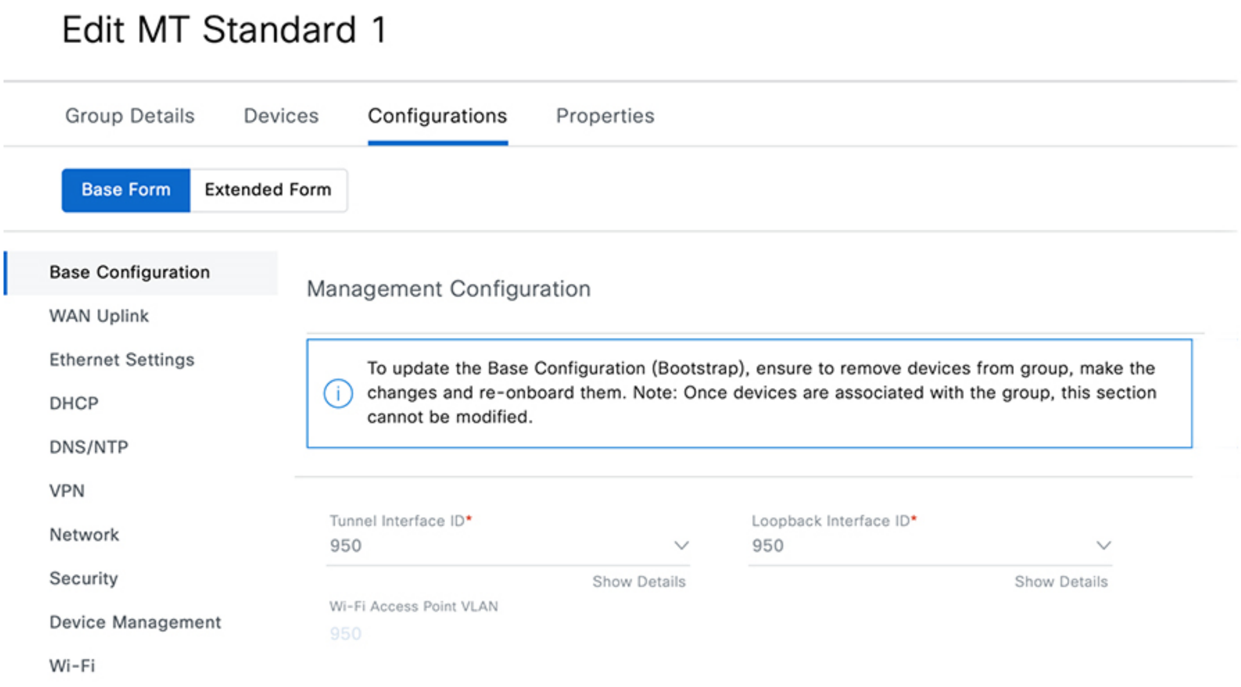
Cisco IR1800 managed by IoT OD

This section documents the configuration for the IR1835 router, managed by IoT Operations Dashboard, using an eCVD Standard Template. The screenshots show the configuration of the various features available in the eCVD template. Some features needed to support the mass transit solution were added as CLI configuration on top of the graphical based eCVD template.

This section shows two different options for configuring the Wi-Fi access point module on the IR1835 with IoT OD – first as a WGB with Hotspot functionality, and secondly as a CAPWAP access point managed by a C9800 wireless LAN controller.

In the **Base Configuration** section, the interface numbering options are left as default. If the default values conflict with the desired interface naming scheme, they can be changed.

Figure 2. Cisco IR1800 managed by IoT OD – eCVD Template – Base Configuration



To update the Base Configuration (Bootstrap), ensure to remove devices from group, make the changes and re-onboard them. Note: Once devices are associated with the group, this section cannot be modified.

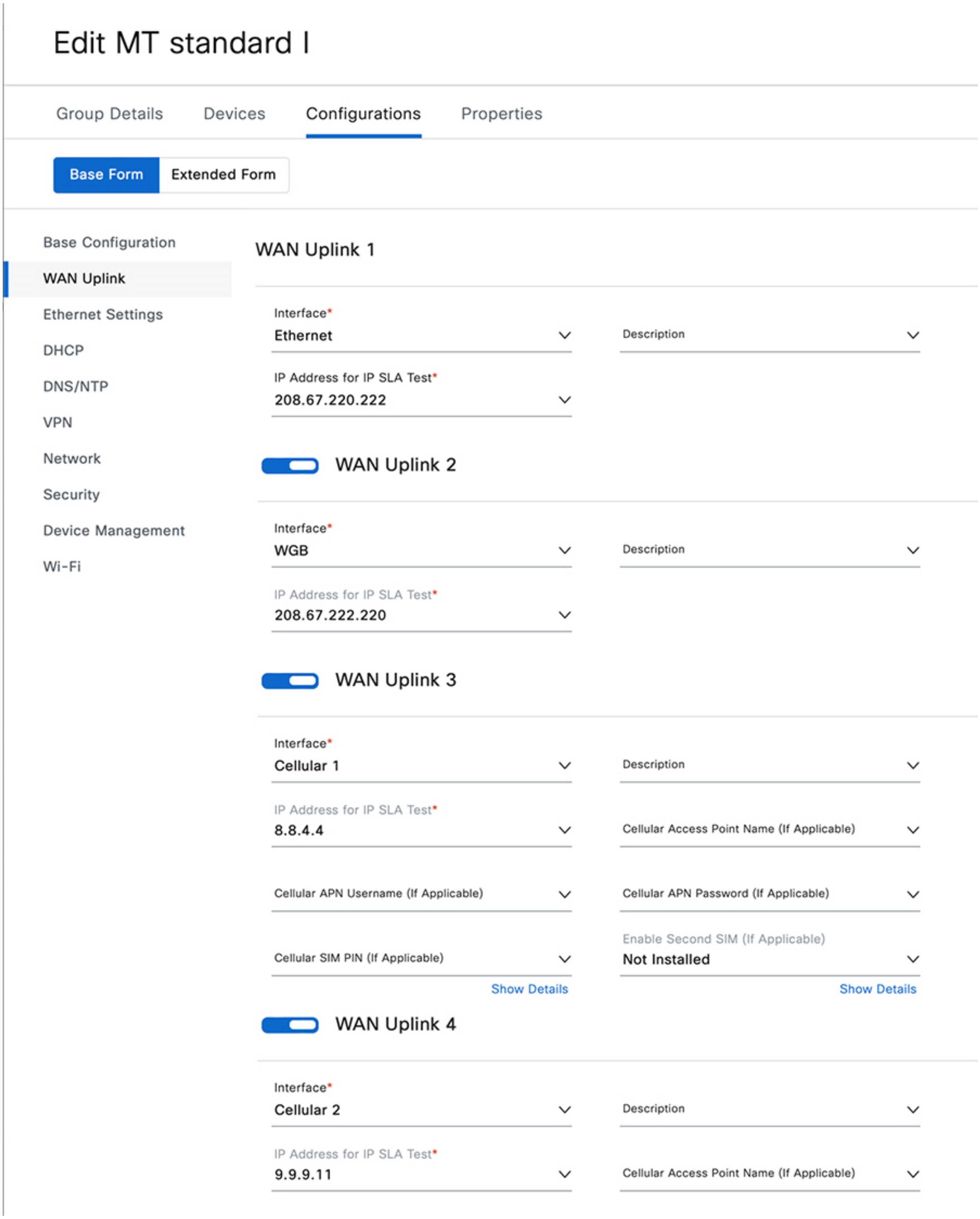
Tunnel Interface ID* 950

Loopback Interface ID* 950

Wi-Fi Access Point VLAN 950

The **WAN Uplink** section determines which interfaces are used as WAN interfaces, along with details for cellular APN, IP SLA destination, and so on. In the IR1800 for a transit vehicle, the “Ethernet” interface refers to Gigabit 0/0/0, which will be connected to the CURWB radio and get a DHCP IP address. WGB refers to the 5 GHz Wi-FI uplink from the WP-WIFI6 module, to be used when the vehicle enters the yard. Cellular 1 is the Cellular 0/4/0 interface in the first PIM slot, and Cellular 2 is the Cellular 0/5/0 interface in the second PIM slot, regardless of which specific hardware modules are used.

Figure 3. Cisco IR1800 managed by IoT OD – eCVD Template – WAN Uplink



Edit MT standard I

WAN Uplink 1

Interface*: Ethernet

Description

IP Address for IP SLA Test*: 208.67.220.222

WAN Uplink 2

Interface*: WGB

Description

IP Address for IP SLA Test*: 208.67.222.220

WAN Uplink 3

Interface*: Cellular 1

Description

IP Address for IP SLA Test*: 8.8.4.4

Cellular Access Point Name (If Applicable)

Cellular APN Username (If Applicable)

Cellular APN Password (If Applicable)

Cellular SIM PIN (If Applicable)

Enable Second SIM (If Applicable): Not Installed

WAN Uplink 4

Interface*: Cellular 2

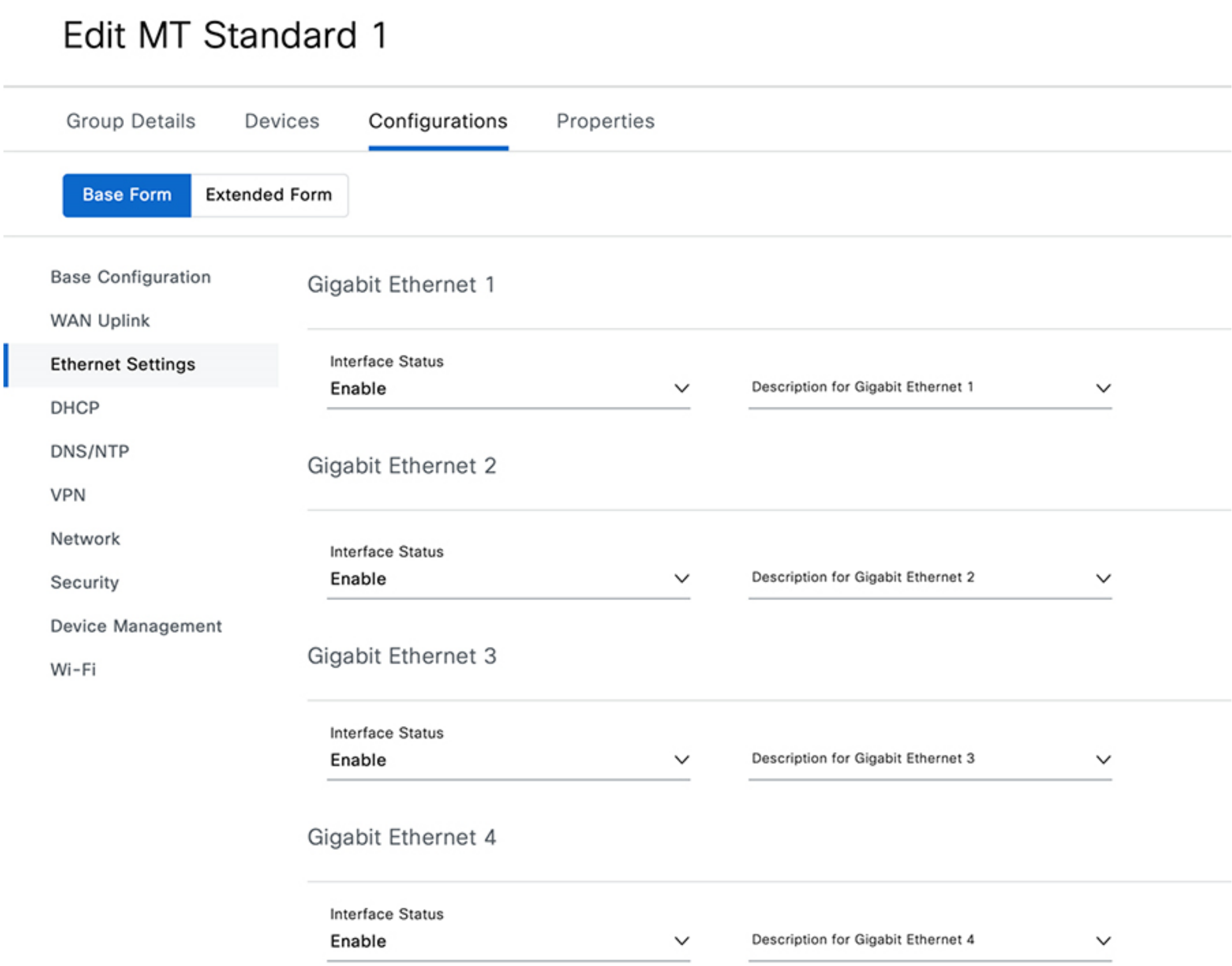
Description

IP Address for IP SLA Test*: 9.9.9.11

Cellular Access Point Name (If Applicable)

The **Ethernet Settings** section simply enables the four LAN interfaces on the IR1800, to be used to connect to downstream devices. By default, all interfaces are put in VLAN 948. Additional configuration to put the interfaces in different VLANs (for Passenger, Worker, Devices1, and so on), enable 802.1x, apply ZBFW, and more is added later in the CLI at the end of this section.

Figure 4. Cisco IR1800 managed by IoT OD – eCVD Template – Ethernet Settings



Gigabit Ethernet 1

Interface Status: Enable

Description for Gigabit Ethernet 1

Gigabit Ethernet 2

Interface Status: Enable

Description for Gigabit Ethernet 2

Gigabit Ethernet 3

Interface Status: Enable

Description for Gigabit Ethernet 3

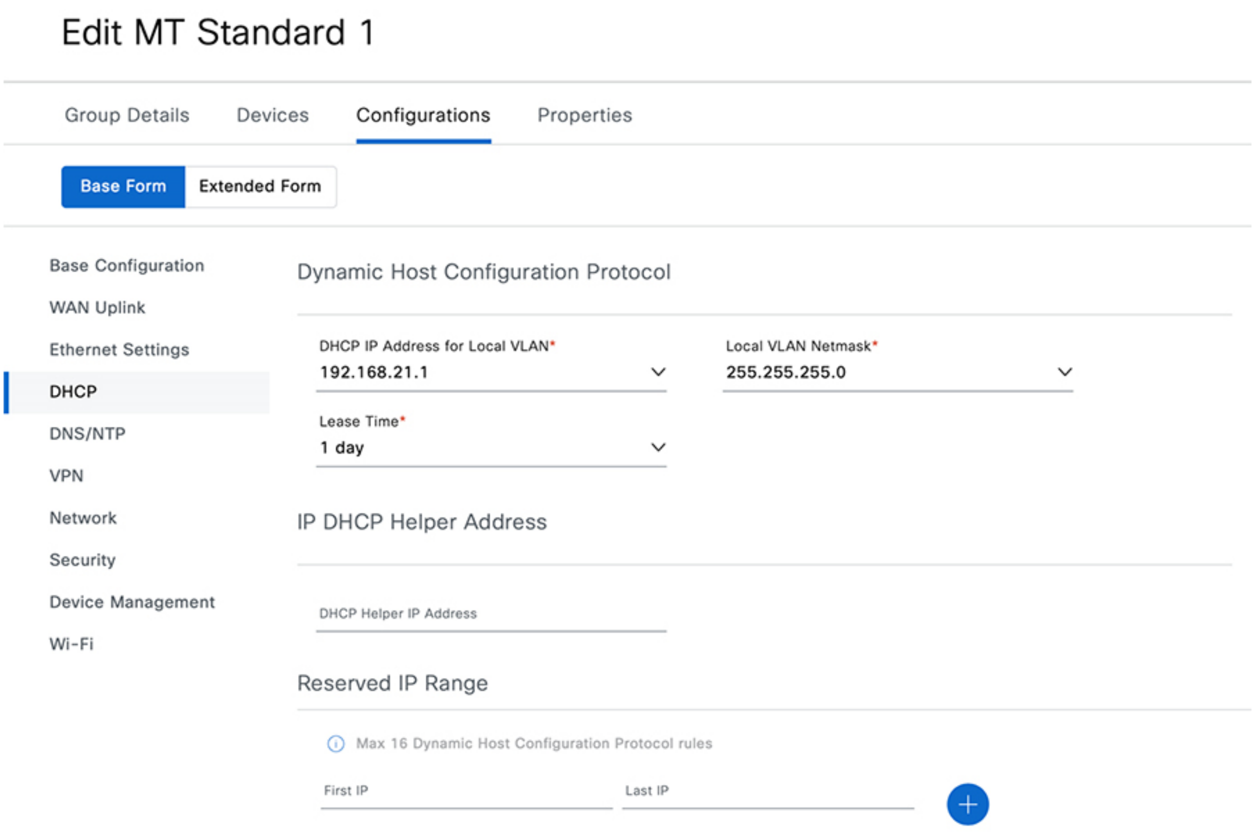
Gigabit Ethernet 4

Interface Status: Enable

Description for Gigabit Ethernet 4

The **DHCP** section is used to configure a DHCP pool for VLAN 948. DHCP Pools for the other VLANs are added automatically. The various VLANs are used to provide separation for different types of devices on the network. Refer to Figure 1 to better understand how the VLANs are used.

Figure 5. Cisco IR1800 managed by IoT OD – eCVD Template – DHCP



Edit MT Standard 1

Dynamic Host Configuration Protocol

DHCP IP Address for Local VLAN*: 192.168.21.1

Local VLAN Netmask*: 255.255.255.0

Lease Time*: 1 day

IP DHCP Helper Address

DHCP Helper IP Address

Reserved IP Range

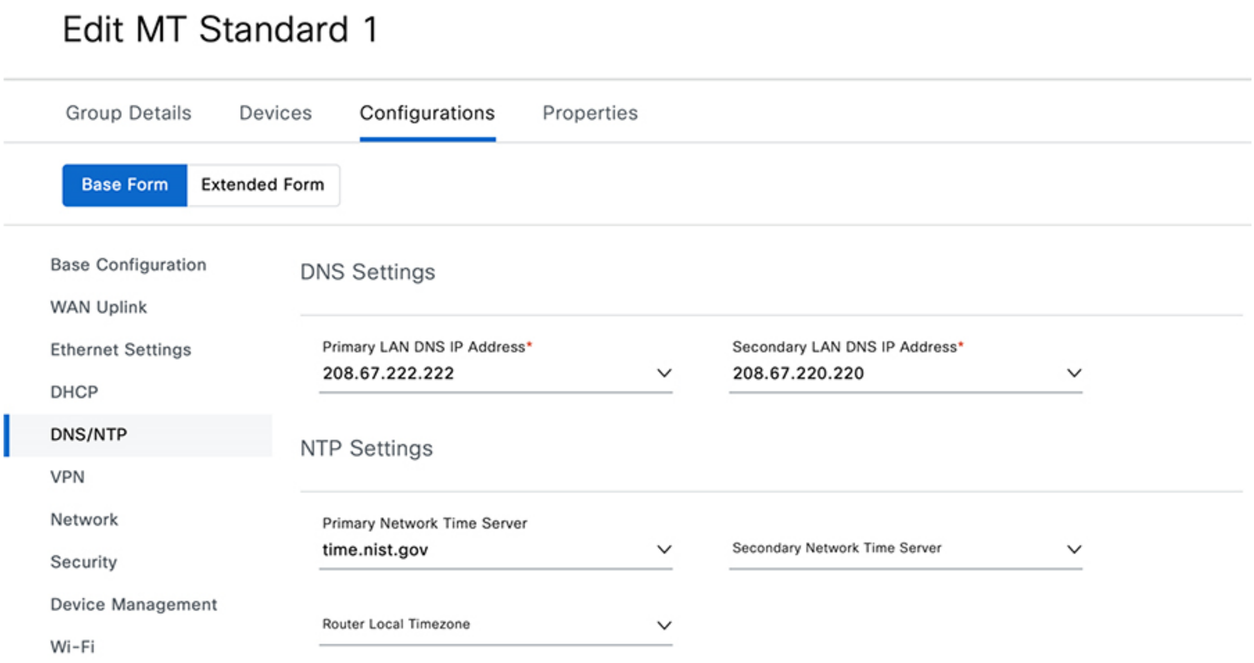
Max 16 Dynamic Host Configuration Protocol rules

First IP

Last IP

The **DNS / NTP** section can be left as default unless specific configuration is required.

Figure 6. Cisco IR1800 managed by IoT OD – eCVD Template – DNS/NTP



Edit MT Standard 1

DNS Settings

Primary LAN DNS IP Address*: 208.67.222.222

Secondary LAN DNS IP Address*: 208.67.220.220

NTP Settings

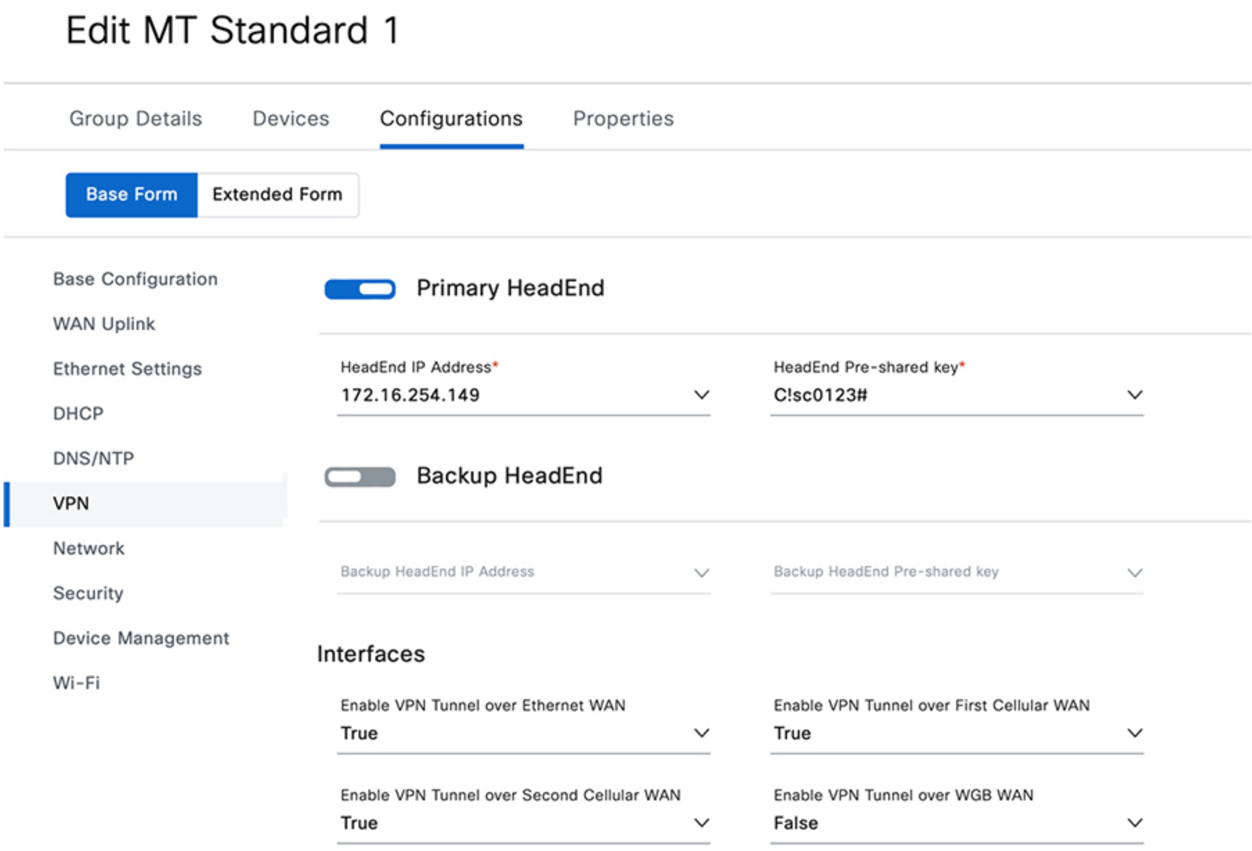
Primary Network Time Server: time.nist.gov

Secondary Network Time Server

Router Local Timezone

The **VPN** section creates the FlexVPN tunnel (Tunnel 949) to the enterprise headend, based on PSK authentication. In this example, the tunnel is enabled for the CURWB and Cellular interfaces, but not the WGB interface. Depending on the existing enterprise routing and security policies, it may be desirable to disable the VPN over CURWB as well, or potentially if the Cellular interface is using a private APN with direct connectivity to the enterprise.

Figure 7. Cisco IR1800 managed by IoT OD – eCVD Template – VPN



Edit MT Standard 1

Primary HeadEnd

HeadEnd IP Address*: 172.16.254.149

HeadEnd Pre-shared key*: C!sc0123#

Backup HeadEnd

Backup HeadEnd IP Address

Backup HeadEnd Pre-shared key

Interfaces

Enable VPN Tunnel over Ethernet WAN: True

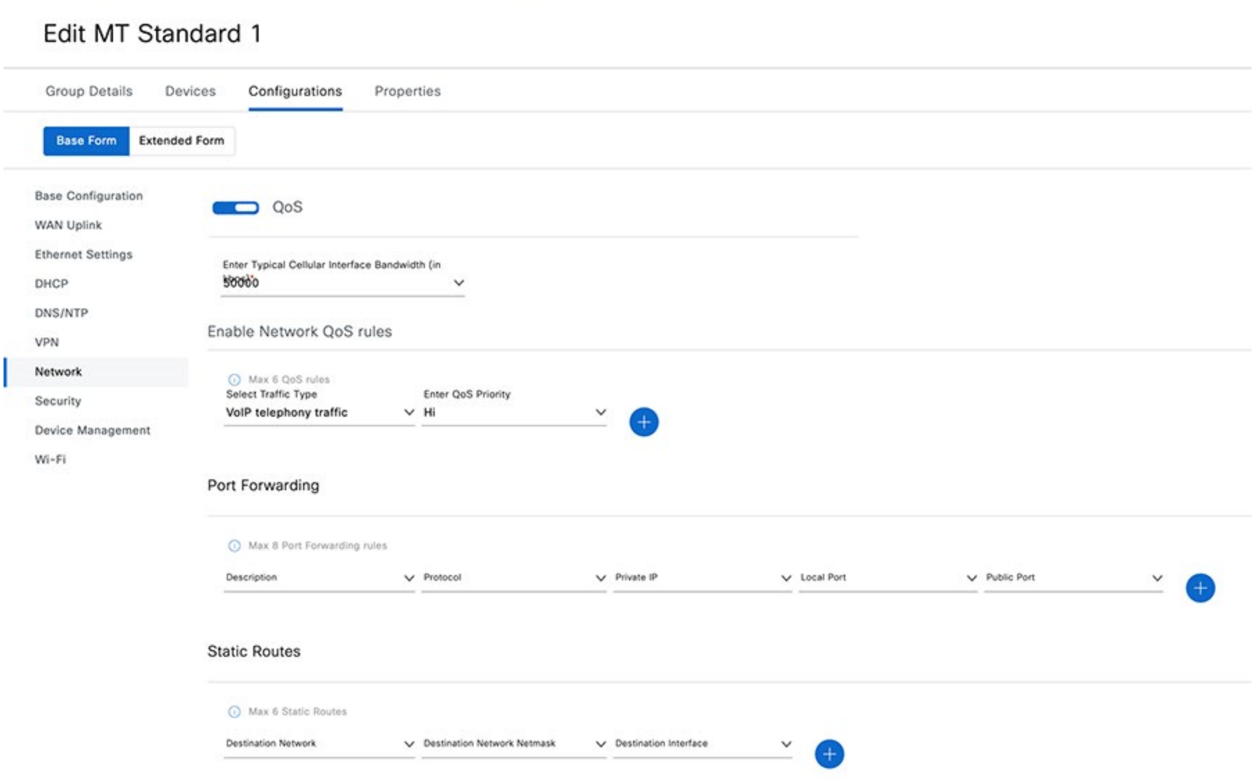
Enable VPN Tunnel over First Cellular WAN: True

Enable VPN Tunnel over Second Cellular WAN: True

Enable VPN Tunnel over WGB WAN: False

In the **Network** section, a QoS policy can be enabled based on various traffic classes.

Figure 8. Cisco IR1800 managed by IoT OD – eCVD Template – Network



QoS

Enter Typical Cellular Interface Bandwidth (in kbps): 50000

Enable Network QoS rules

Max 6 QoS rules

Select Traffic Type: VoIP telephony traffic

Enter QoS Priority: Hi

Port Forwarding

Max 8 Port Forwarding rules

Description | Protocol | Private IP | Local Port | Public Port

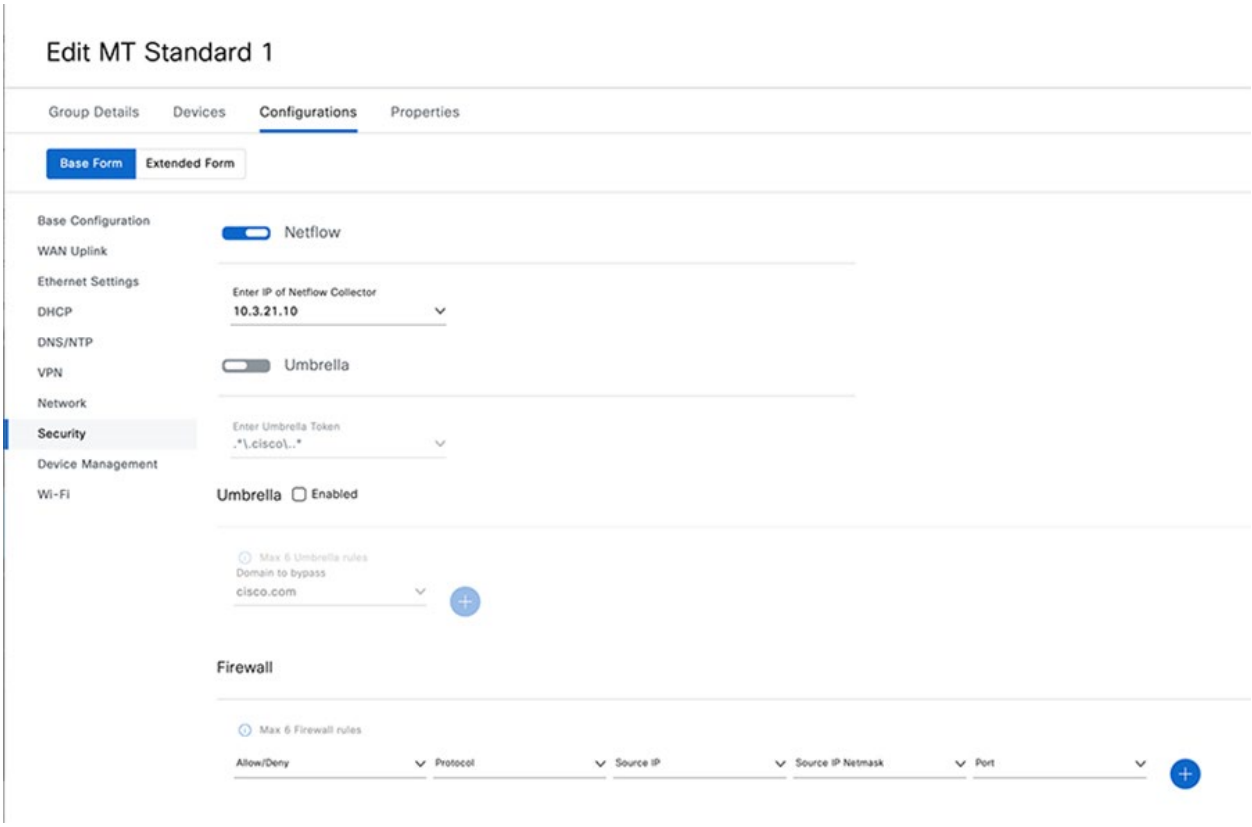
Static Routes

Max 6 Static Routes

Destination Network | Destination Network Netmask | Destination Interface

In the **Security** section, a NetFlow collector can be configured to receive exports, and basic Umbrella functionality can be enabled. Simple firewall rules can be added. An example of a ZBFW for the multiple VLANs is included in the CLI at the end of this section.

Figure 9. Cisco IR1800 managed by IoT OD – eCVD Template – Security



Netflow

Enter IP of Netflow Collector
10.3.21.10

Umbrella

Enter Umbrella Token
.*\.cisco\..*

Umbrella ☐ Enabled

Max 6 Umbrella rules
Domain to bypass
cisco.com

Firewall

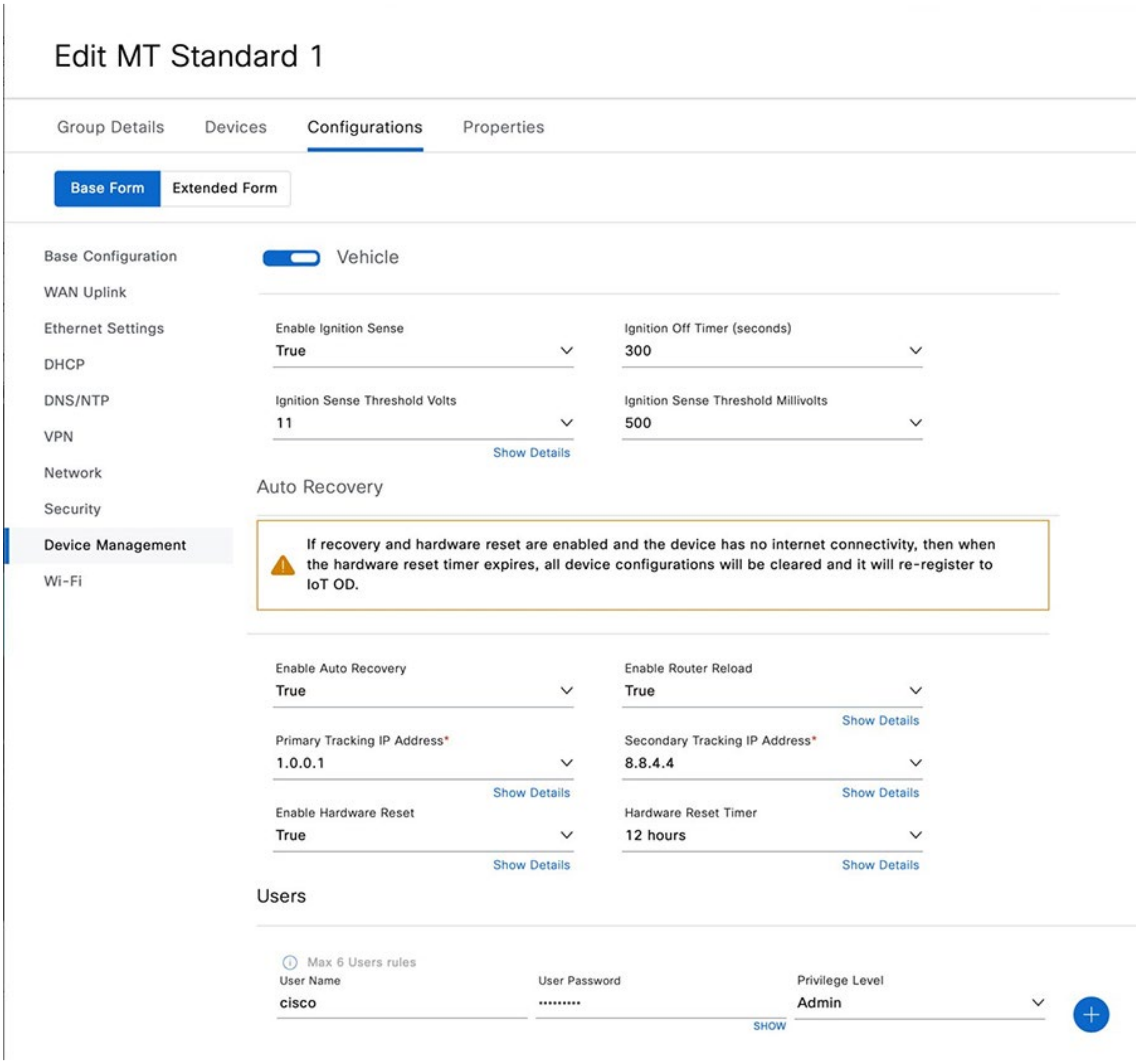
Max 6 Firewall rules

Allow/Deny | Protocol | Source IP | Source IP Netmask | Port

In the **Device Management** section, ignition sense is enabled to automatically power down the router five minutes after the vehicle is turned off. This works by configuring the router to monitor the input voltage on the power supply to the router, which should be connected to the vehicle's battery and alternator. When the vehicle is running, the alternator will be charging the battery at a slightly higher voltage than the battery will have at rest, when the vehicle is turned off. This input voltage is used to infer ignition status of the vehicle. In the example below, the voltage threshold is set to 13.2 volts. If the voltage exceeds this – the vehicle is presumed to be running and the router will power up (if previously off) or continue to stay powered up. If the detected voltage drops below this value for the configured time of 300 seconds, the router will power itself down, thus preventing it from draining the vehicle battery unnecessarily.

Auto recovery is also enabled to allow the router to attempt to recover from misconfiguration and other issues, to help prevent sending a technician to troubleshoot a device that is down.

Figure 10. Cisco IR1800 managed by IoT OD – eCVD Template – Device Management



Edit MT Standard 1

Vehicle

Enable Ignition Sense: True

Ignition Off Timer (seconds): 300

Ignition Sense Threshold Volts: 11

Ignition Sense Threshold Millivolts: 500

Auto Recovery

If recovery and hardware reset are enabled and the device has no internet connectivity, then when the hardware reset timer expires, all device configurations will be cleared and it will re-register to IoT OD.

Enable Auto Recovery: True

Enable Router Reload: True

Primary Tracking IP Address*: 1.0.0.1

Secondary Tracking IP Address*: 8.8.4.4

Enable Hardware Reset: True

Hardware Reset Timer: 12 hours

Users

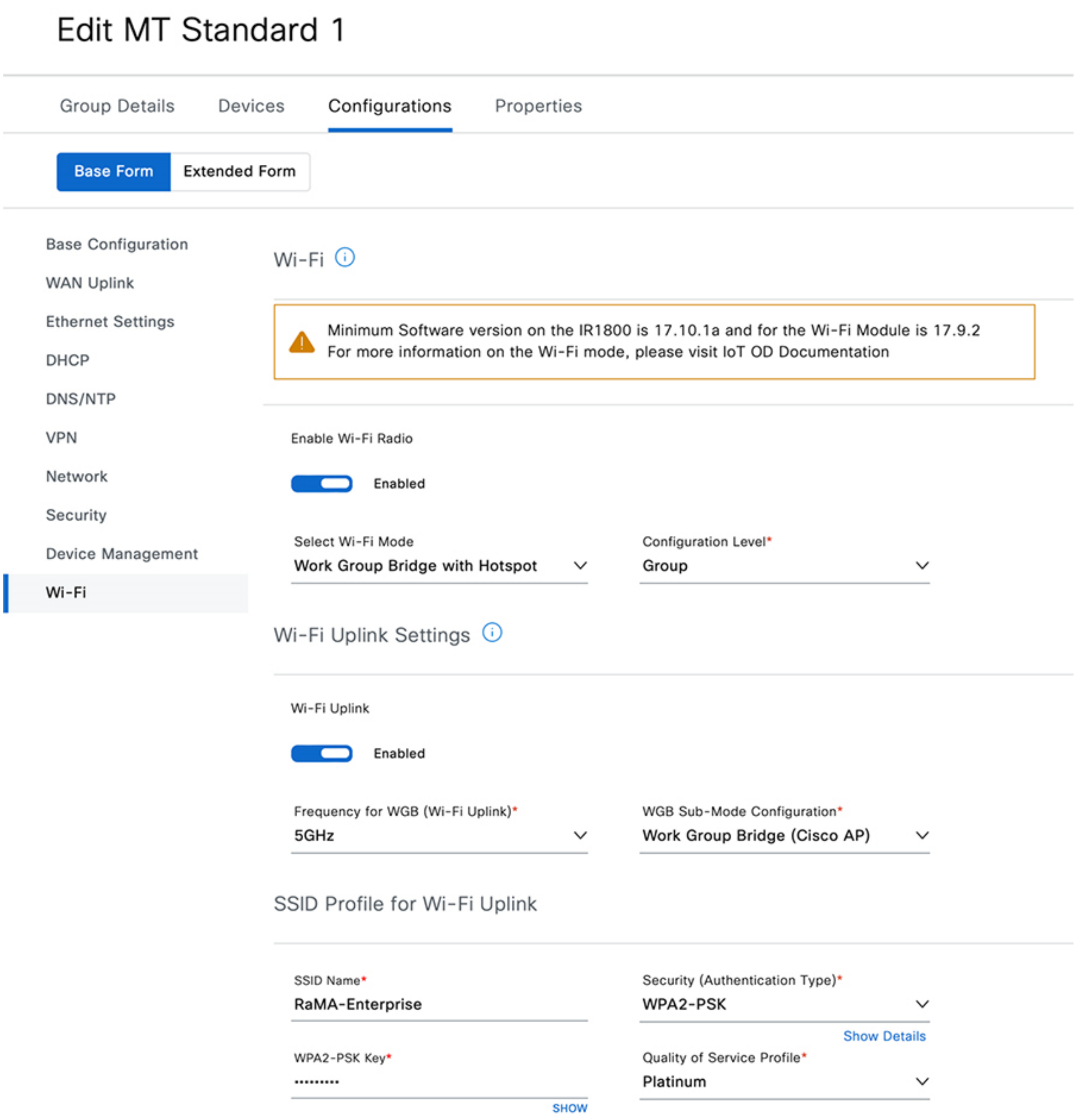
Max 6 Users rules

User Name	User Password	Privilege Level
cisco	•••••••••	Admin

In the **Wi-Fi** section the onboard access point is enabled in Workgroup Bridge with Hotspot mode. The Wi-Fi Uplink (WGB) is enabled on the 5GHz radio interface.

To have both an uplink and a hotspot, the Wi-Fi module minimum software version is 17.11 and the IR1800 minimum version is 17.10.1a. Also, the Wi-Fi module must be capable of WGB Concurrent radio, more details about this can be found in the link below, as well as steps to upgrade your module and convert it so that it has the ability for concurrent radio. If during the upgrade procedure any issues are encountered with TFTP, we recommend using HTTP to upgrade the Wi-Fi module through the CLI if there is an HTTP file server available.

Figure 11. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (WGB with Hotspot)



Edit MT Standard 1

Wi-Fi

Minimum Software version on the IR1800 is 17.10.1a and for the Wi-Fi Module is 17.9.2
For more information on the Wi-Fi mode, please visit IoT OD Documentation

Enable Wi-Fi Radio: Enabled

Select Wi-Fi Mode: Work Group Bridge with Hotspot

Configuration Level*: Group

Wi-Fi Uplink Settings

Wi-Fi Uplink: Enabled

Frequency for WGB (Wi-Fi Uplink)*: 5GHz

WGB Sub-Mode Configuration*: Work Group Bridge (Cisco AP)

SSID Profile for Wi-Fi Uplink

SSID Name*: RaMA-Enterprise

Security (Authentication Type)*: WPA2-PSK

WPA2-PSK Key*: •••••••••

Quality of Service Profile*: Platinum

To login to the CLI of a Wi-Fi module in WGB mode past 17.9.1 the login credentials are the following:

- Username: Cisco1
- Password: GigabitEth01!
- Enable Password: AppleTree01@

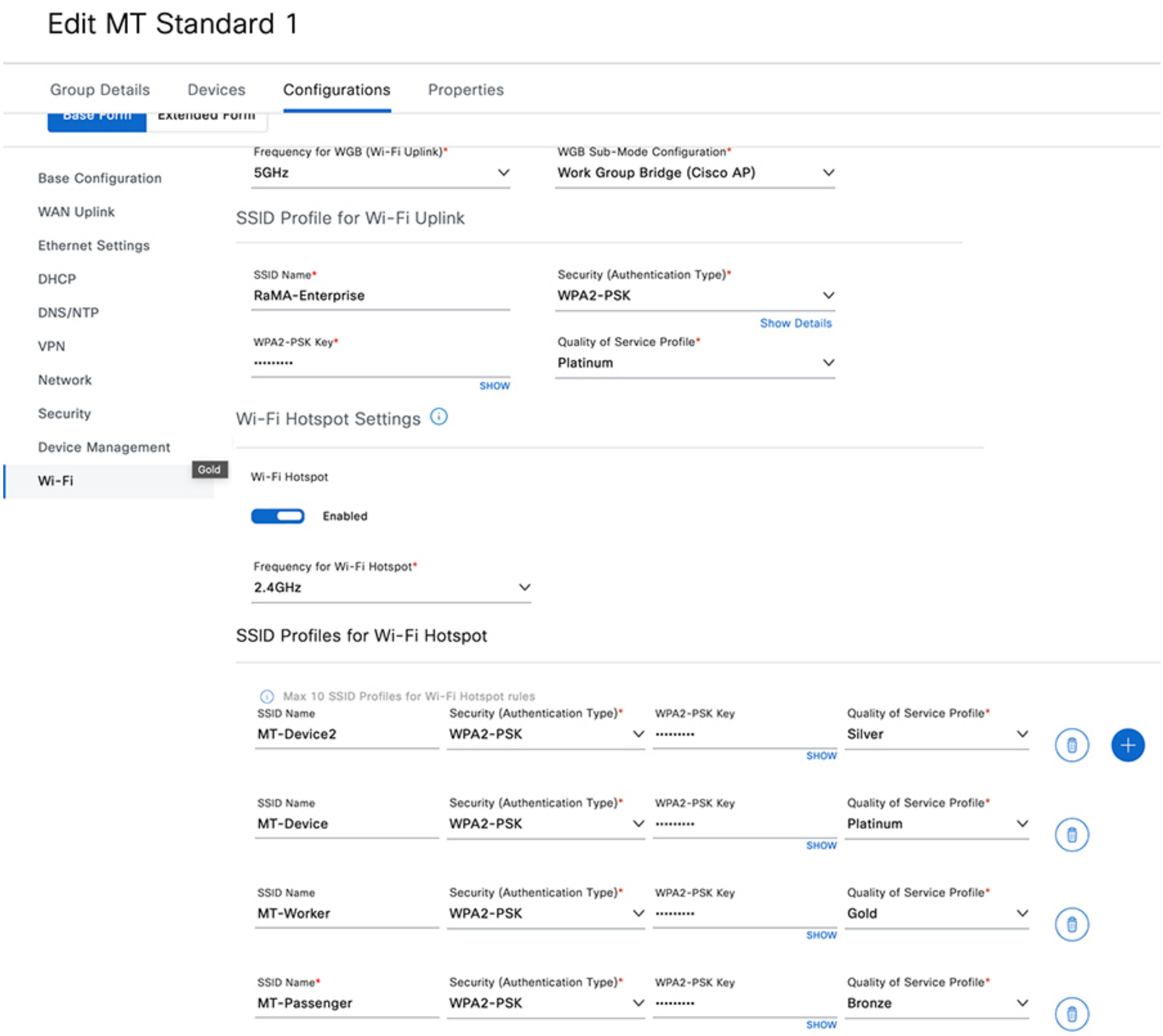
Links to the following modules are:

[Wi-Fi Module Overview]

[Wi-Fi Module Concurrent Radio]

A total of four **SSIDs** are created here for passengers, workers, and devices (two of them, for different types of devices).

Figure 12. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (WGB with Hotspot continued)



Edit MT Standard 1

Frequency for WGB (Wi-Fi Uplink)*: 5GHz

WGB Sub-Mode Configuration*: Work Group Bridge (Cisco AP)

SSID Profile for Wi-Fi Uplink

SSID Name*: RaMA-Enterprise

Security (Authentication Type)*: WPA2-PSK

WPA2-PSK Key*: ••••••••

Quality of Service Profile*: Platinum

Wi-Fi Hotspot Settings

Wi-Fi Hotspot: Enabled

Frequency for Wi-Fi Hotspot*: 2.4GHz

SSID Profiles for Wi-Fi Hotspot

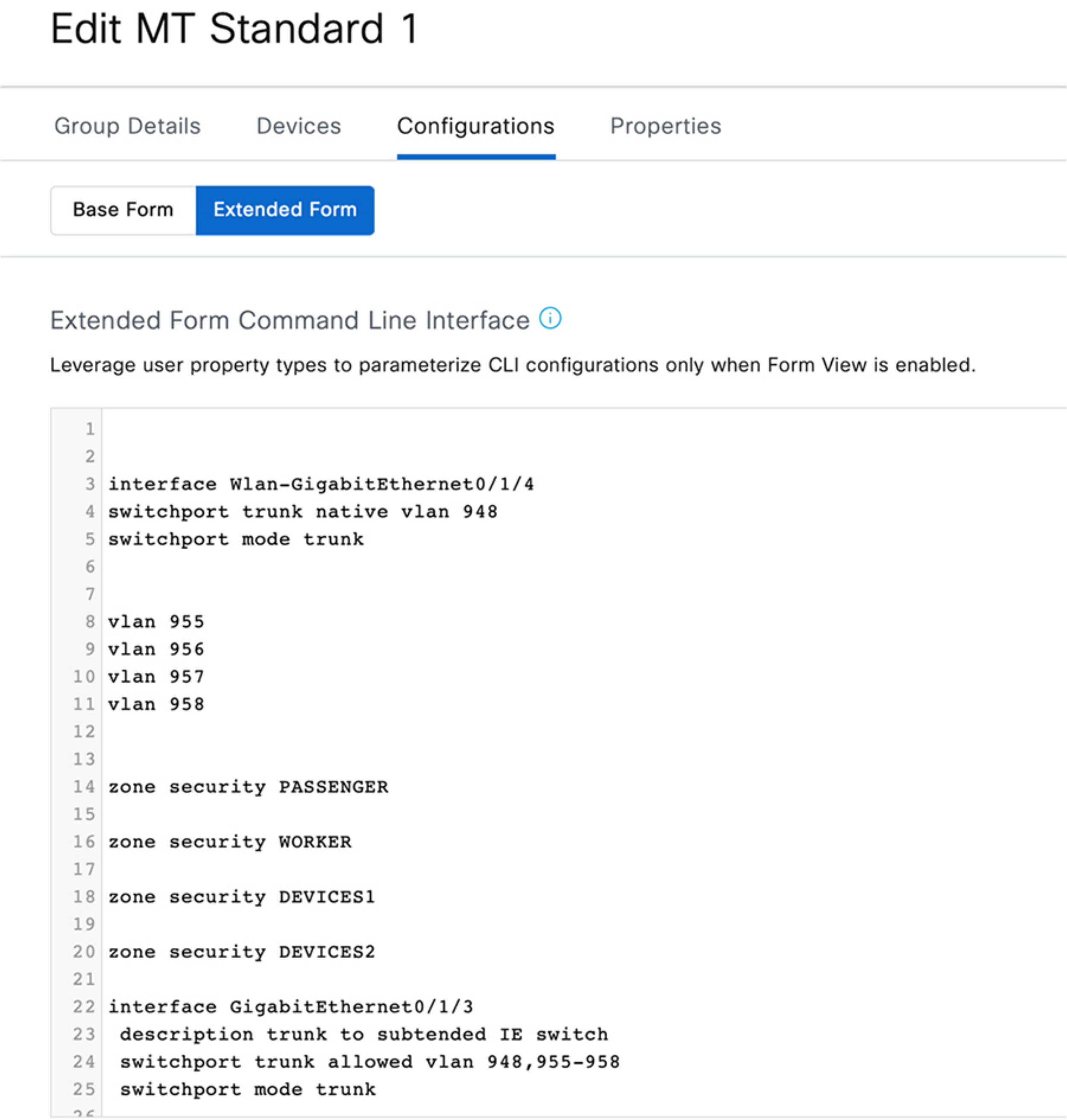
Max 10 SSID Profiles for Wi-Fi Hotspot rules

SSID Name	Security (Authentication Type)*	WPA2-PSK Key	Quality of Service Profile*
MT-Device2	WPA2-PSK	••••••••	Silver
MT-Device	WPA2-PSK	••••••••	Platinum
MT-Worker	WPA2-PSK	••••••••	Gold
MT-Passenger	WPA2-PSK	••••••••	Bronze

Each SSID will automatically create the necessary VLANs, DHCP pools, and related configuration, with the exceptions noted.

Finally, the **Extended Form** section of the configuration is used to apply additional CLI as needed, for features that are not supported in the GUI based eCVD template.

Figure 13. Cisco IR1800 managed by IoT OD – eCVD Template – Extended Form CLI



Leverage user property types to parameterize CLI configurations only when Form View is enabled.

```


interface Wlan-GigabitEthernet0/1/4
switchport trunk native vlan 948
switchport mode trunk


vlan 955
vlan 956
vlan 957
vlan 958


zone security PASSENGER

zone security WORKER

zone security DEVICES1

zone security DEVICES2

interface GigabitEthernet0/1/3
 description trunk to subtended IE switch
 switchport trunk allowed vlan 948,955-958
 switchport mode trunk
```

The internal interface connecting the router to the access point module is set as a trunk, with the default VLAN (948) set as native.

```
interface Wlan-GigabitEthernet0/1/4

switchport trunk native vlan 948

switchport mode trunk
```

Next the four VLANs for Passenger, Worker, Devices1, and Devices2 are created.

```
vlan 955
vlan 956
vlan 957
vlan 958
```

Four security zones are created, one for each VLAN.

```
zone security PASSENGER
zone security WORKER
zone security DEVICES1
zone security DEVICES2
```

One of the switch ports is configured as a trunk to connect to the subtended IE switch.

```
interface GigabitEthernet0/1/3
 description trunk to subtended IE switch
 switchport trunk allowed vlan 948,955-958
 switchport mode trunk
```

A VLAN SVI is created for the Passenger VLAN.

```
interface Vlan955
 ip address 192.168.110.1 255.255.255.0
 ip nat inside
 zone-member security PASSENGER
```

A VLAN SVI is created for the Worker VLAN.

```
interface Vlan956
 ip address 192.168.111.1 255.255.255.0
 ip nat inside
 zone-member security WORKER
```

A VLAN SVI is created for the first Devices VLAN.

```
interface Vlan957
 ip address 192.168.112.1 255.255.255.0
 ip nat inside
 zone-member security DEVICES1
```

A VLAN SVI is created for the second Devices VLAN.

```
interface Vlan958
 ip address 192.168.113.1 255.255.255.0
 ip nat inside

 zone-member security DEVICES2
```

The Zone Based Firewall uses access lists to match on the subnets for each of the four VLANs.

```
ip access-list extended PASSENGER

       permit ip 192.168.110.0 0.0.0.255 any

ip access-list extended WORKER

       permit ip 192.168.111.0 0.0.0.255 any

ip access-list extended DEVICES1

       permit ip 192.168.112.0 0.0.0.255 any

ip access-list extended DEVICES2

       permit ip 192.168.113.0 0.0.0.255 any
```

The access lists are referenced in class maps for each zone pair.

```
class-map type inspect match-all PASSENGER-TO-INTERNET-CLASS

  match access-group name PASSENGER

class-map type inspect match-all WORKER-TO-INTERNET-CLASS

  match access-group name WORKER

class-map type inspect match-all DEVICES1-TO-INTERNET-CLASS

  match access-group name DEVICES1

class-map type inspect match-all DEVICES2-TO-INTERNET-CLASS

  match access-group name DEVICES2

class-map type inspect match-all WORKER-TO-default-CLASS

  match access-group name WORKER

class-map type inspect match-all DEVICES1-TO-default-CLASS

  match access-group name DEVICES1

class-map type inspect match-all DEVICES2-TO-default-CLASS

  match access-group name DEVICES2

class-map type inspect match-all default-to-DEVICES2-CLASS

  match access-group name DEVICES2
```

Policy maps are then created to inspect each class of traffic based on the zone pairs. In this example the action is just to inspect the traffic, but depending on requirements, other actions (like drop) could be taken.

```
policy-map type inspect PASSENGER-TO-INTERNET-POLICY

  class PASSENGER-TO-INTERNET-CLASS

     inspect

   class class-default
```

```
     drop log
policy-map type inspect WORKER-TO-INTERNET-POLICY
  class WORKER-TO-INTERNET-CLASS
     inspect
   class class-default
     drop log
policy-map type inspect DEVICES1-TO-INTERNET-POLICY
  class DEVICES1-TO-INTERNET-CLASS
     inspect
   class class-default
     drop log
policy-map type inspect DEVICES2-TO-INTERNET-POLICY
  class DEVICES2-TO-INTERNET-CLASS
     inspect
   class class-default
     drop log
policy-map type inspect WORKER-TO-default-POLICY
  class WORKER-TO-default-CLASS
     inspect
   class class-default
     drop log
policy-map type inspect DEVICES1-TO-default-POLICY
  class DEVICES1-TO-default-CLASS
     inspect
   class class-default
  drop log
policy-map type inspect DEVICES2-TO-default-POLICY
  class DEVICES2-TO-default-CLASS
     inspect
   class class-default
     drop log
policy-map type inspect default-TO-DEVICES2-POLICY
  class default-TO-DEVICES2-CLASS
     inspect
   class class-default
     drop log
```

Finally, the ZBFW configuration is completed by defining the zone pairs.

```
zone-pair security PASSENGER-TO-INTERNET source PASSENGER destination INTERNET
  service-policy type inspect PASSENGER-TO-INTERNET-POLICY
zone-pair security WORKER-TO-INTERNET source WORKER destination INTERNET
  service-policy type inspect WORKER-TO-INTERNET-POLICY
zone-pair security DEVICES1-TO-INTERNET source DEVICES1 destination INTERNET
  service-policy type inspect DEVICES1-TO-INTERNET-POLICY
zone-pair security DEVICES2-TO-INTERNET source DEVICES2 destination INTERNET
  service-policy type inspect DEVICES2-TO-INTERNET-POLICY
zone-pair security WORKER-TO-default source WORKER destination default
  service-policy type inspect WORKER-TO-default-POLICY
zone-pair security DEVICES1-TO-default source DEVICES1 destination default
  service-policy type inspect DEVICES1-TO-default-POLICY
zone-pair security DEVICES2-TO-default source DEVICES2 destination default
  service-policy type inspect DEVICES2-TO-default-POLICY
zone-pair security default-TO-DEVICES2 source default destination DEVICES2
 service-policy type inspect default-TO-DEVICES2-POLICY
```

Note: The “default-TO-DEVICES2” configuration elements were added to enable SEA access from the IOX app to the devices in the 192.168.113.0/24 subnet. Similar configuration will be required if SEA needs to access other subnets.

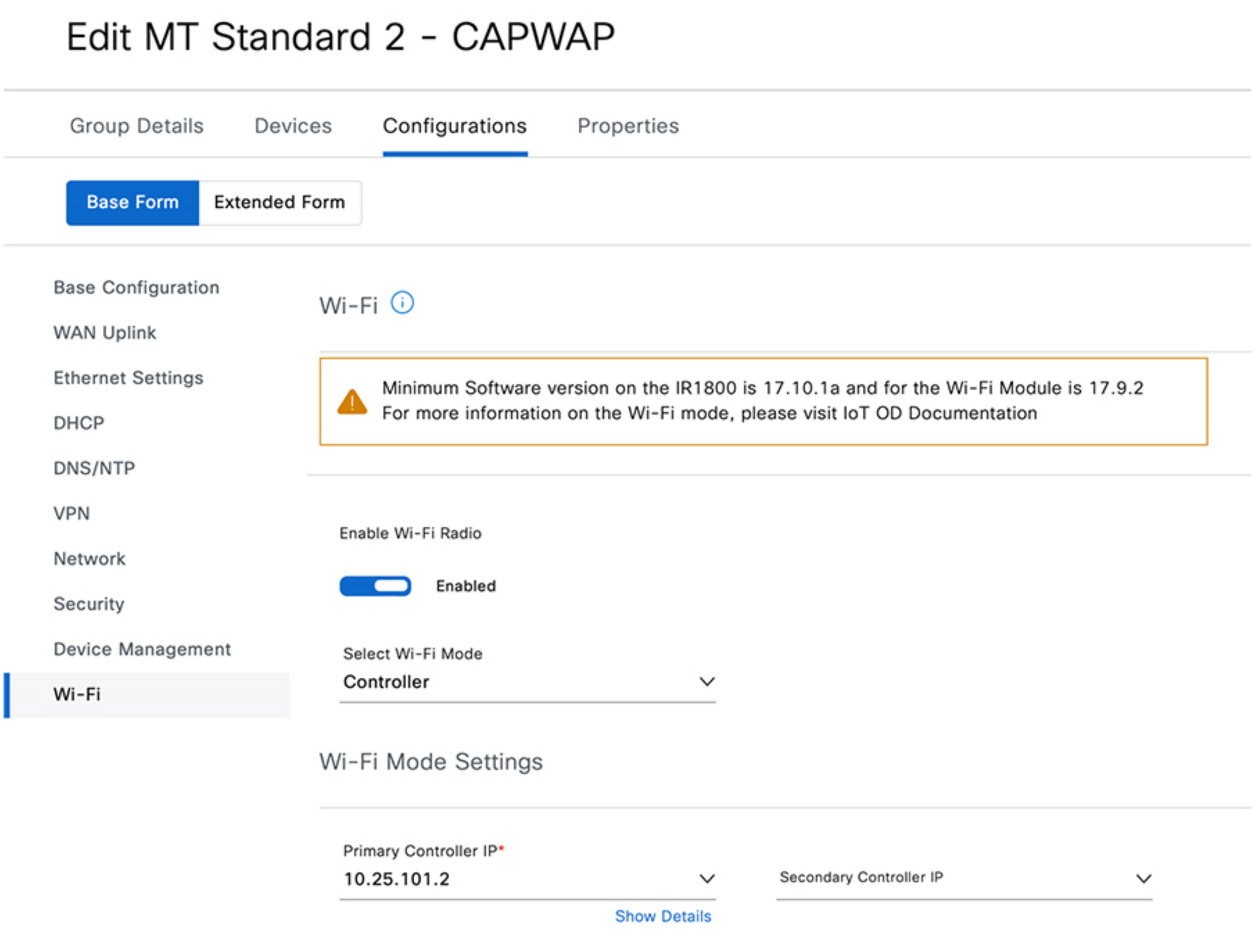
In the following section 802.1x for wired clients connected to port GigabitEthernet0/1/2 is enabled. When a device connects, it will need to be authenticated by the configured ISE server via RADIUS.

```
aaa new-model
!
!
aaa group server radius ISE-RADIUS-GROUP
 server name DatacenterISE
 ip radius source-interface Tunnel949
!
aaa authentication dot1x default group ISE-RADIUS-GROUP
aaa authorization network AUTH_LIST group ISE-RADIUS-GROUP
aaa accounting update newinfo periodic 2880
aaa accounting dot1x default start-stop group ISE-RADIUS-GROUP

!

epm logging

!

authentication mac-move permit

!

dot1x system-auth-control

!

interface GigabitEthernet0/1/2

 switchport mode access

 authentication port-control auto

 dot1x pae authenticator

!

radius-server attribute 6 on-for-login-auth

radius-server attribute 6 support-multiple

radius-server attribute 8 include-in-access-req

radius-server attribute 25 access-request include

radius-server attribute 31 mac format ietf upper-case

radius-server attribute 31 send nas-port-detail mac-only

radius-server dead-criteria time 10 tries 3

!

radius server DatacenterISE

 address ipv4 10.3.21.50 auth-port 1645 acct-port 1646

 timeout 3

 key 7 104D000A06185E5A5E57

!
```

CAPWAP mode for IoT OD IR1800 Wi-Fi

The following figure shows the alternate Wi-Fi configuration in an eCVD template in which the IR1800 access point is managed by a Cisco Catalyst 9800 Wireless LAN Controller.

Figure 14. Cisco IR1800 managed by IoT OD – eCVD Template – Wi-Fi (Controller/CAPWAP mode)



Edit MT Standard 2 - CAPWAP

Minimum Software version on the IR1800 is 17.10.1a and for the Wi-Fi Module is 17.9.2
For more information on the Wi-Fi mode, please visit IoT OD Documentation

Enable Wi-Fi Radio: Enabled

Select Wi-Fi Mode: Controller

Primary Controller IP*: 10.25.101.2

Secondary Controller IP

Cisco IR1800 managed by SD-WAN Manager

Refer to the *SD-WAN for Industrial Markets Design Guide* for detailed information on configuring the Cisco IR1835 for use in a Mass Transit scenario.

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-case-study.pdf

WAN Failover Operation

Failover between WAN interfaces is critical for mass transit buses and similar deployments where the environmental conditions are constantly changing as the vehicle moves. Reducing the failover delay is important to maintaining the best experience for connected devices and users. This interruption in connectivity must be balanced with preventing rapid flapping back-and-forth between interfaces in the case that the vehicle enters an area with poor coverage for all cellular carriers (for example).

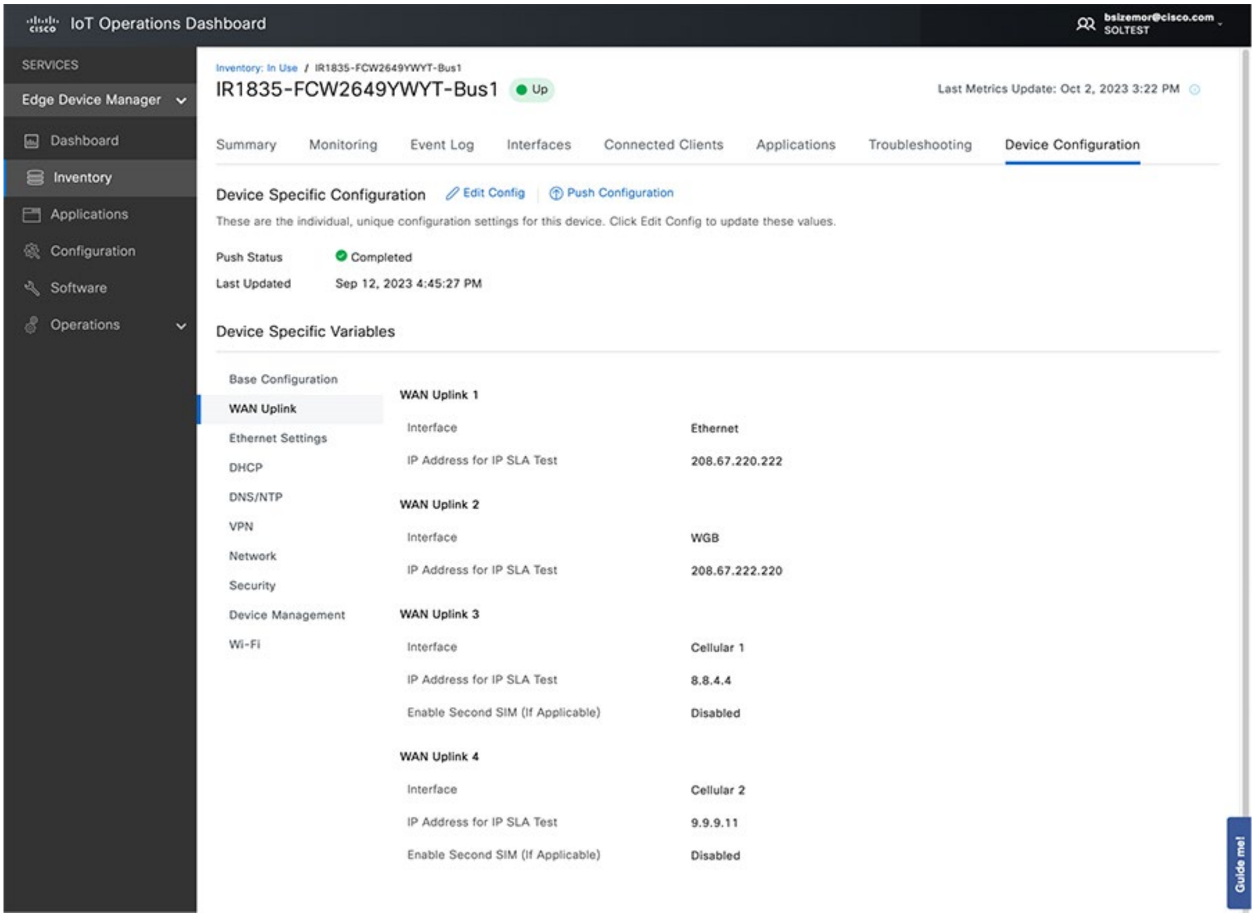
The SDWAN CVD provides details about how failovers are handled using BFD monitoring within the service VPNs, as well as other options like "last-resort-circuit" for active-standby scenarios.

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-case-study.pdf

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/m-sd-wan-iiot-fleet.pdf

This Implementation Guide focuses on how failovers are implemented using the eCVD templates in Cisco IoT Operations Dashboard.

Figure 15. IoT Operations Dashboard – WAN Interface Priorities



IR1835-FCW2649YWYT-Bus1 Up

Last Metrics Update: Oct 2, 2023 3:22 PM

Device Specific Configuration

These are the individual, unique configuration settings for this device. Click Edit Config to update these values.

Push Status: Completed

Last Updated: Sep 12, 2023 4:45:27 PM

Device Specific Variables

WAN Uplink 1

Interface	Ethernet
IP Address for IP SLA Test	208.67.220.222

WAN Uplink 2

Interface	WGB
IP Address for IP SLA Test	208.67.222.220

WAN Uplink 3

Interface	Cellular 1
IP Address for IP SLA Test	8.8.4.4
Enable Second SIM (If Applicable)	Disabled

WAN Uplink 4

Interface	Cellular 2
IP Address for IP SLA Test	9.9.9.11
Enable Second SIM (If Applicable)	Disabled

The eCVD template allows the WAN uplinks to be selected in prioritized order. Meaning that Uplink 1 will be the default route for all traffic until it is not viable, after which Uplink 2 will be the default route, and so on for Uplink 3 and 4. In the example above, the Ethernet interface (connected to an external CURWB radio) is used as uplink 1, followed by WGB as uplink 2, Cellular 0/4/0 as uplink 3, and Cellular 0/5/0 as uplink 4. The template configures the routing to only have a single default route active at any one time, therefore no load balancing is used for user traffic.

Each of the WAN interfaces is monitored with an ICMP echo based IP SLA and associated track statement. These IP SLA monitoring sessions are always active. A “delay down” statement is added to the IP SLA based track statements to prevent flapping of up/down state in the case that a single ICMP echo is missed.

```
track 12 interface Cellular0/4/0 line-protocol
track 13 interface Cellular0/5/0 line-protocol
track 40 ip sla 40 reachability
delay down 25
!
track 41 ip sla 41 reachability
delay down 25
!
track 42 ip sla 42 reachability
delay down 65
!
track 43 ip sla 43 reachability
delay down 65
!
track 237 ip sla 237 reachability
!
track 238 ip sla 238 reachability
!
track 239 interface Tunnel950 line-protocol
!
track 980 interface GigabitEthernet0/0/0 ip routing
!
track 981 interface Cellular0/4/0 ip routing
!
track 982 interface Cellular0/5/0 ip routing
!
track 983 interface Tunnel950 ip routing
!
```

The IP SLA statements are configured to ping an IP address that is reachable over the associated interface. By default in the eCVD, and as shown in this example, various public DNS server addresses are chosen as the destinations as they are assumed to be highly available and reachable over any internet connection. Different frequencies are configured by default depending on the interface type – 10 seconds for high bandwidth Ethernet uplink, and 30 seconds for Cellular. A lower frequency will potentially reduce the failover time, but at the expense of more data being sent over the interface which can be undesirable for a usage-based Cellular bill.

```
ip sla 40
icmp-echo 208.67.220.222 source-interface GigabitEthernet0/0/0
frequency 10
```

```
ip sla schedule 40 life forever start-time now
ip sla 41
icmp-echo 208.67.222.220 source-interface Vlan950
frequency 10
ip sla schedule 41 life forever start-time now
ip sla 42
icmp-echo 8.8.4.4
frequency 30
ip sla schedule 42 life forever start-time now
ip sla 43
icmp-echo 9.9.9.11
frequency 30
ip sla schedule 43 life forever start-time now
ip sla 237
icmp-echo 208.67.222.222
frequency 30
ip sla 238
icmp-echo 208.67.220.220
frequency 30
!
```

All WAN interfaces are configured to be up and connected at all times. Weighted default routes are used to prioritize one interface over another. Host routes to the IP SLA destinations are added to force the ICMP packets out a specific interface. Host routes to the IP SLA destinations out “Null0” are also added to prevent reachability to these destinations over one of the default routes, in the event the host route out the WAN interface is removed from the routing table.

```
ip route 8.8.4.4 255.255.255.255 Cellular0/4/0 track 12
ip route 9.9.9.11 255.255.255.255 Cellular0/5/0 track 13
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0 72 track 42
ip route 69.172.234.159 255.255.255.255 Cellular0/4/0 42 track 42
ip route 0.0.0.0 0.0.0.0 Cellular0/5/0 73 track 43
ip route 69.172.234.159 255.255.255.255 Cellular0/5/0 43 track 43
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0 82
ip route 0.0.0.0 0.0.0.0 Cellular0/5/0 83
ip route 8.8.4.4 255.255.255.255 Null0 3
ip route 9.9.9.11 255.255.255.255 Null0 3
ip route 44.230.145.83 255.255.255.255 Cellular0/4/0 90
ip route 44.230.145.83 255.255.255.255 Cellular0/5/0 92
ip route 208.67.220.222 255.255.255.255 Null0 3
ip route 208.67.222.220 255.255.255.255 Null0 3
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 dhcp 70
ip route 44.230.145.83 255.255.255.255 GigabitEthernet0/0/0 dhcp
ip route 208.67.220.222 255.255.255.255 GigabitEthernet0/0/0 dhcp
ip route 69.172.234.159 255.255.255.255 GigabitEthernet0/0/0 dhcp 40
ip route 0.0.0.0 0.0.0.0 Vlan950 dhcp 71
ip route 208.67.222.220 255.255.255.255 Vlan950 dhcp
```

CURWB Backhaul Managed with IoT OD

The Cisco CURWB radios, such as the IW916x series can be managed with the Industrial Wireless service in IoT Operations Dashboard. To onboard the IW radio used as an uplink for the IR1800 router, it is recommended that the initial provisioning is performed in a staging environment before installing in a vehicle.

This section summarizes the steps required to deploy an IW9167 device. For detailed steps and more information refer to the official documentation:

Cisco Catalyst IW9167 Heavy Duty Series Configuration Guides

Industrial Wireless service for IoT Operations Dashboard

1. Create a CSV file containing the serial number and MAC addresses of the IW devices that need to be onboarded into IoT OD:

```
KWC272109QD,24:16:1B:F9:2B:C0
KWC272109U3,24:16:1B:F9:2D:B8
KWC272109TY,24:16:1B:F9:2D:A4
KWC272109TK,24:16:1B:F9:2D:70
```

2. Log into **IoT Operations Dashboard**, and navigate to the **Industrial Wireless** service. From the **Inventory** page, click **Add Devices** and upload the CSV file created above.

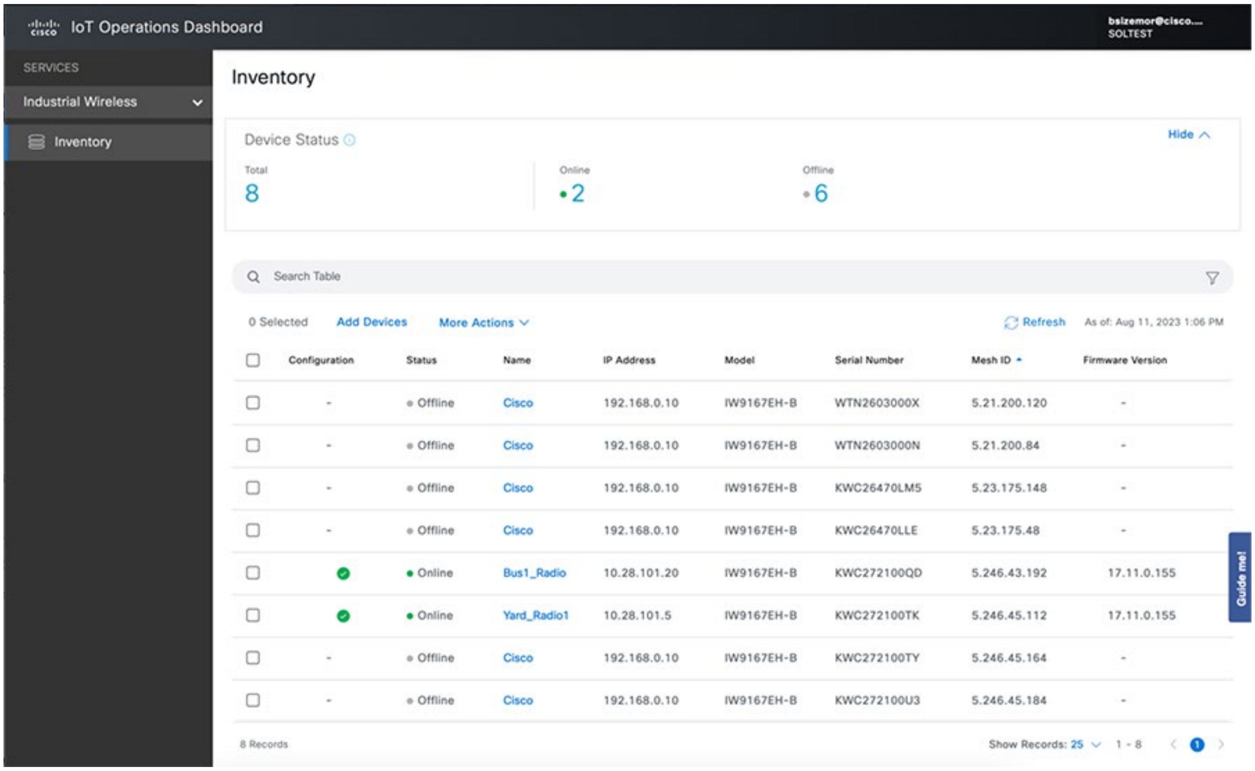
3. Either using **Configuration Groups**, or individual device configuration, setup the device as required. See detailed steps at the end of this section.

4. Next, connect the IW device to a switch that can provide a DHCP address, power over ethernet, and internet access (to IoT OD). From a computer connected to the same switch, identify the DHCP assigned address that was given to the IW access point. From the computer web browser, connect to the IW access point local GUI, or CLI and configure the device to be managed with IoT OD:

```
configure iotod-iw online
```

   The IW access point contacts the IoT OD and attempts to download the configuration parameters. The IW can now be disconnected from the staging switch and installed in the vehicle. The IW connects to the IR1800 routed Gig 0/0/0 port, with an inline power injector to provide power. The IR1800 Gig 0/0/0 interface is assigned a DHCP address, and work “out of the box” with a configuration based on an eCVD template with Ethernet WAN enabled.

Figure 16. Cisco URWB managed by IoT OD – Inventory List



Inventory

Device Status

Hide

Total	Online	Offline
8	● 2	● 6

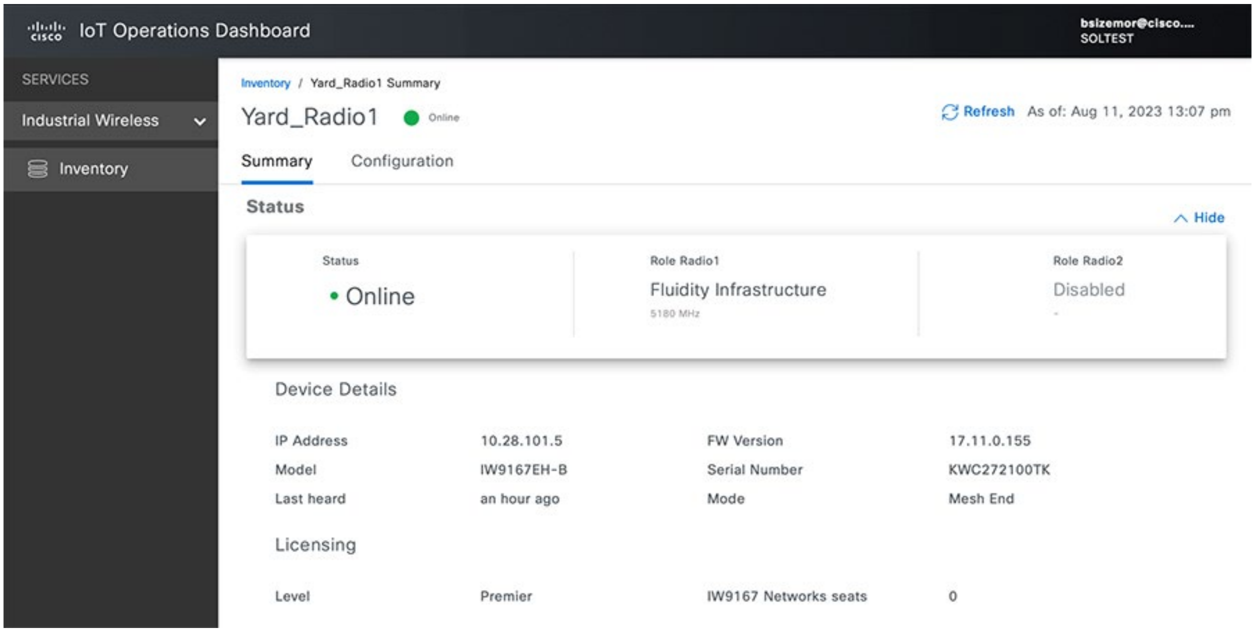
Search Table

0 Selected Add Devices More Actions Refresh As of: Aug 11, 2023 1:06 PM

□	Configuration	Status	Name	IP Address	Model	Serial Number	Mesh ID	Firmware Version
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	WTN2603000X	5.21.200.120	-
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	WTN2603000N	5.21.200.84	-
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	KWC26470LM5	5.23.175.148	-
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	KWC26470LLE	5.23.175.48	-
□	✓	● Online	Bus1_Radio	10.28.101.20	IW9167EH-B	KWC272100QD	5.246.43.192	17.11.0.155
□	✓	● Online	Yard_Radio1	10.28.101.5	IW9167EH-B	KWC272100TK	5.246.45.112	17.11.0.155
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	KWC272100TY	5.246.45.164	-
□	-	● Offline	Cisco	192.168.0.10	IW9167EH-B	KWC272100U3	5.246.45.184	-

8 Records Show Records: 25 1 - 8 1

Figure 17. Cisco URWB managed by IoT OD – Device Summary



Inventory / Yard_Radio1 Summary

Yard_Radio1 ● Online

Refresh As of: Aug 11, 2023 13:07 pm

Summary Configuration

Status

Hide

Status	Role Radio1	Role Radio2
● Online	Fluidity Infrastructure 5180 MHz	Disabled -

Device Details

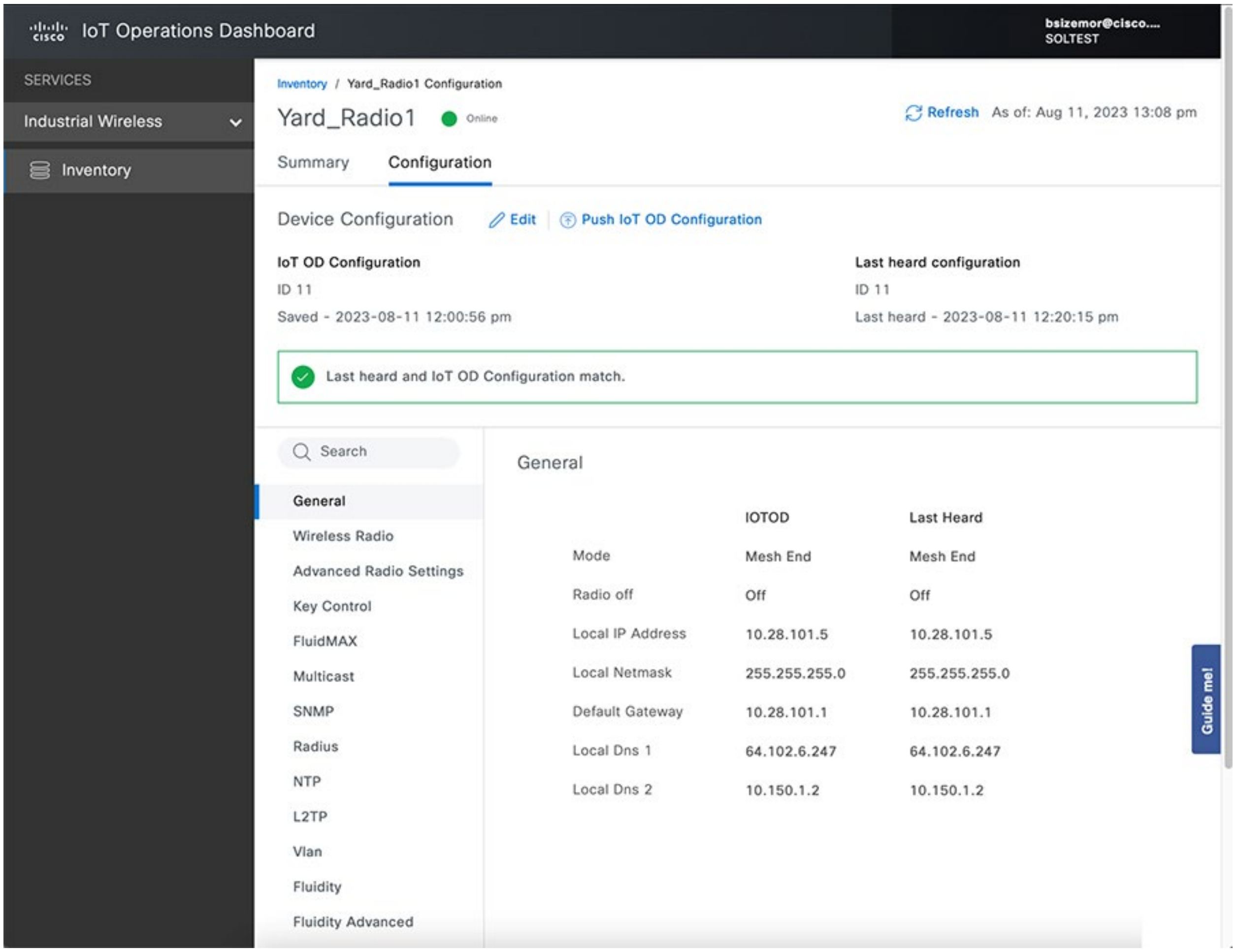
IP Address	10.28.101.5	FW Version	17.11.0.155
Model	IW9167EH-B	Serial Number	KWC272100TK
Last heard	an hour ago	Mode	Mesh End

Licensing

Level	Premier	IW9167 Networks seats	0

Detailed CURWB configuration from the Industrial Wireless service in IoT Operations Dashboard are shown below. This is an example of a possible configuration that was verified in a lab environment. Real-world deployments may require modification.

Figure 18. Cisco URWB managed by IoT OD – Device Configuration - General



Yard_Radio1 ● Online

As of: Aug 11, 2023 13:08 pm

Device Configuration

IoT OD Configuration
ID 11
Saved - 2023-08-11 12:00:56 pm

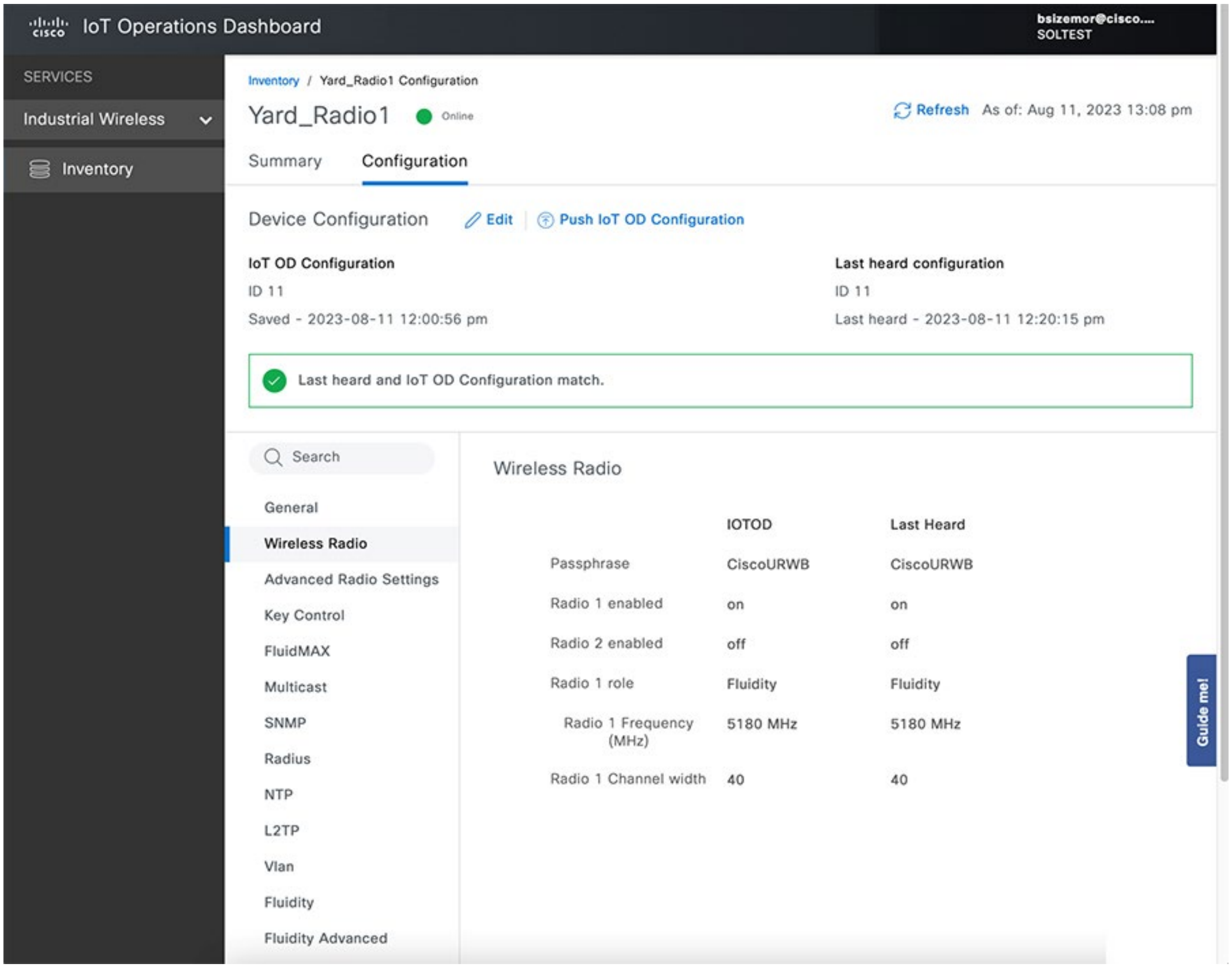
Last heard configuration
ID 11
Last heard - 2023-08-11 12:20:15 pm

✓ Last heard and IoT OD Configuration match.

General

	IOTOD	Last Heard
Mode	Mesh End	Mesh End
Radio off	Off	Off
Local IP Address	10.28.101.5	10.28.101.5
Local Netmask	255.255.255.0	255.255.255.0
Default Gateway	10.28.101.1	10.28.101.1
Local Dns 1	64.102.6.247	64.102.6.247
Local Dns 2	10.150.1.2	10.150.1.2

Figure 19. Cisco URWB managed by IoT OD – Device Configuration – Wireless Radio



Yard_Radio1 ● Online

As of: Aug 11, 2023 13:08 pm

Device Configuration

IoT OD Configuration
ID 11
Saved - 2023-08-11 12:00:56 pm

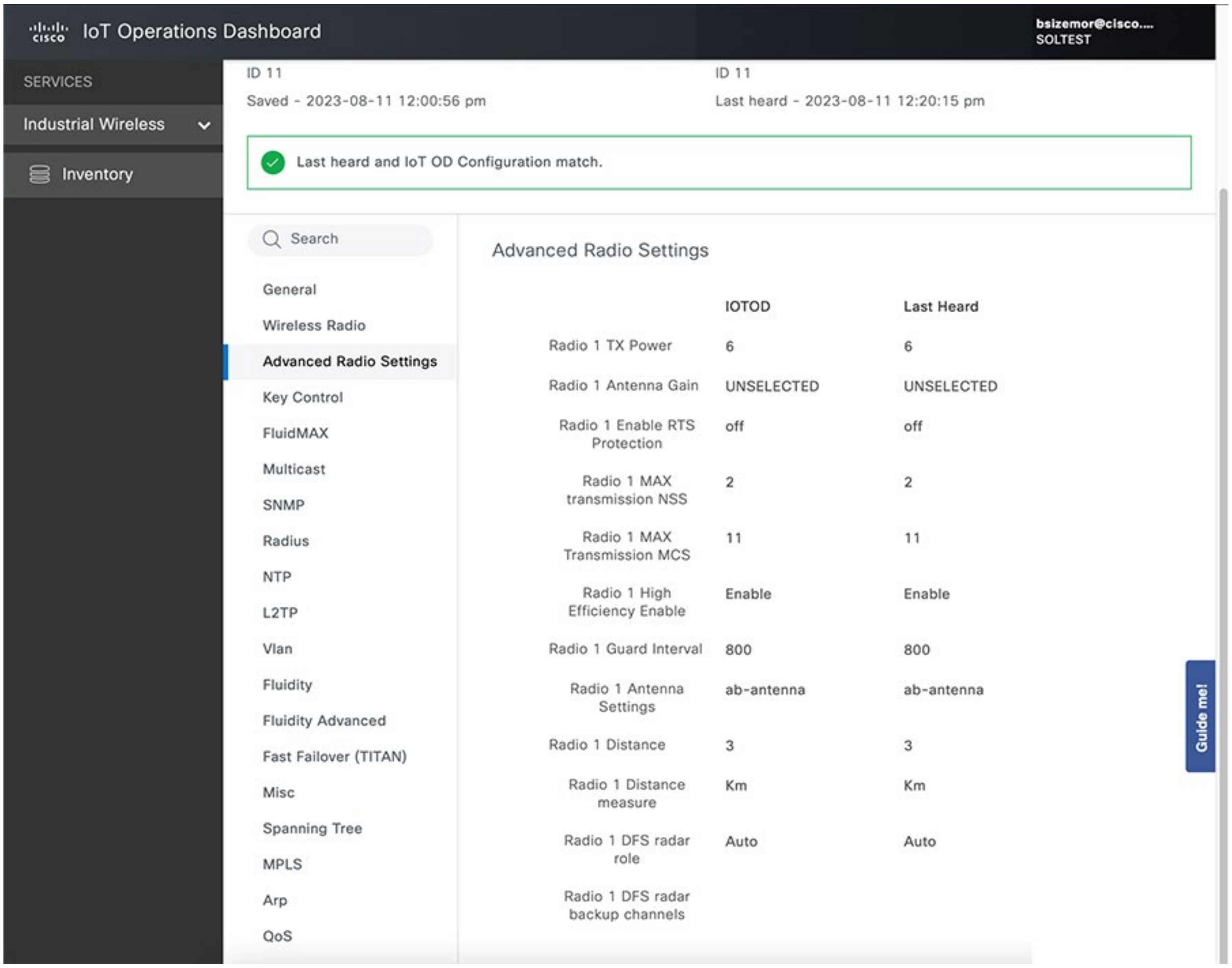
Last heard configuration
ID 11
Last heard - 2023-08-11 12:20:15 pm

✓ Last heard and IoT OD Configuration match.

Wireless Radio

	IOTOD	Last Heard
Passphrase	CiscoURWB	CiscoURWB
Radio 1 enabled	on	on
Radio 2 enabled	off	off
Radio 1 role	Fluidity	Fluidity
Radio 1 Frequency (MHz)	5180 MHz	5180 MHz
Radio 1 Channel width	40	40

Figure 20. Cisco URWB managed by IoT OD – Device Configuration – Advanced Radio Settings



ID 11
Saved - 2023-08-11 12:00:56 pm

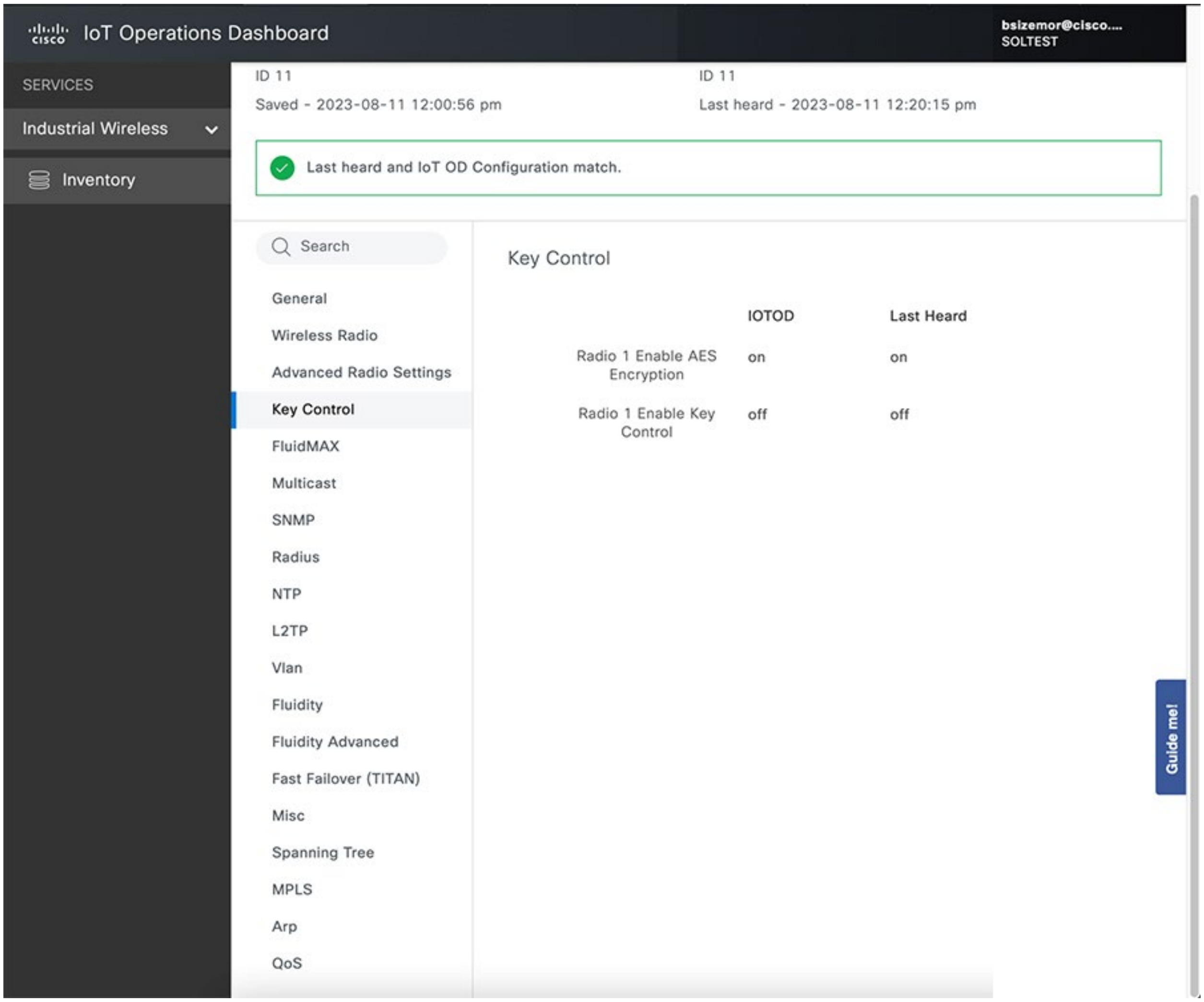
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Advanced Radio Settings

	IOTOD	Last Heard
Radio 1 TX Power	6	6
Radio 1 Antenna Gain	UNSELECTED	UNSELECTED
Radio 1 Enable RTS Protection	off	off
Radio 1 MAX transmission NSS	2	2
Radio 1 MAX Transmission MCS	11	11
Radio 1 High Efficiency Enable	Enable	Enable
Radio 1 Guard Interval	800	800
Radio 1 Antenna Settings	ab-antenna	ab-antenna
Radio 1 Distance	3	3
Radio 1 Distance measure	Km	Km
Radio 1 DFS radar role	Auto	Auto
Radio 1 DFS radar backup channels		

Figure 21. Cisco URWB managed by IoT OD – Device Configuration – Key Control



ID 11
Saved - 2023-08-11 12:00:56 pm

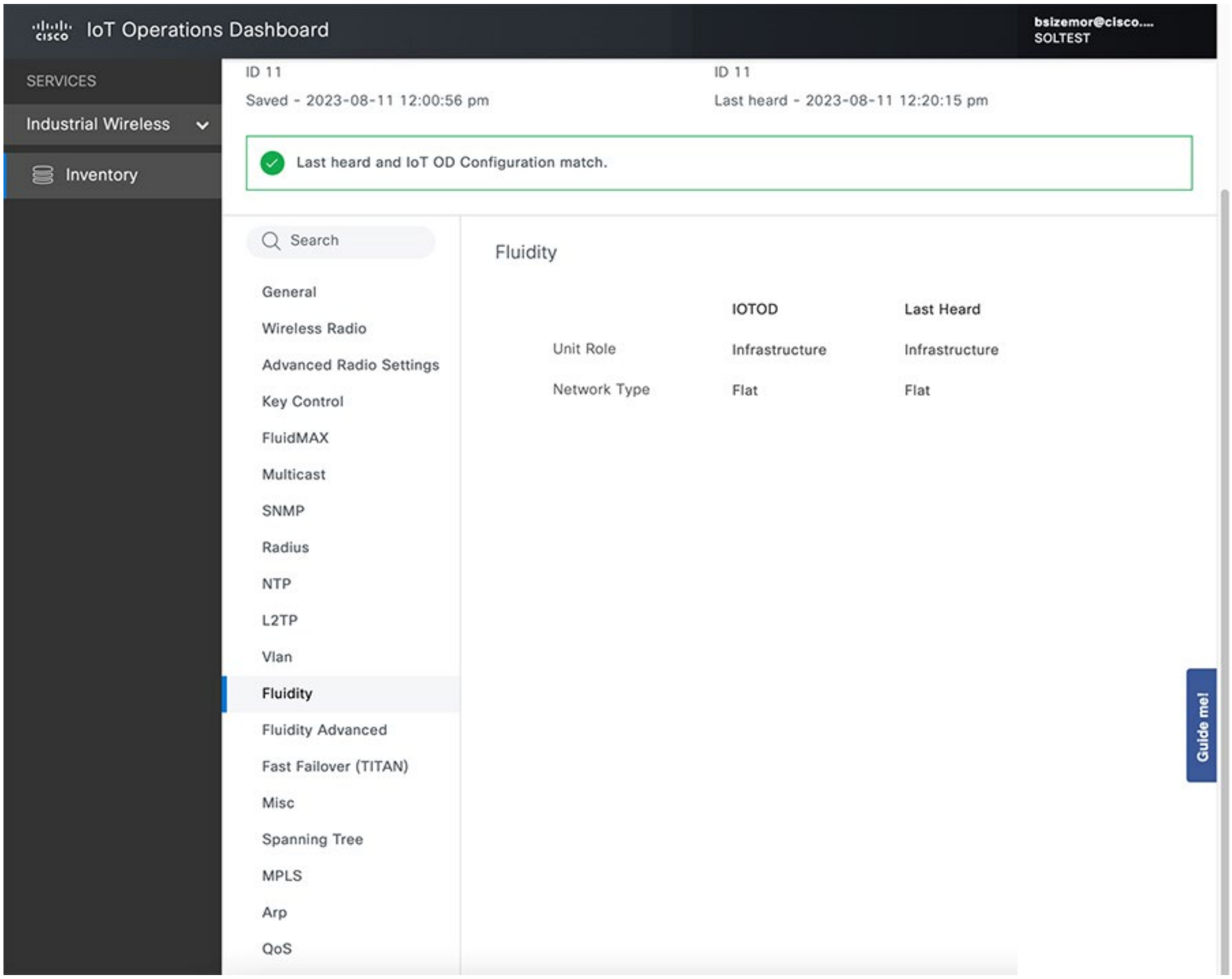
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Key Control

	IOTOD	Last Heard
Radio 1 Enable AES Encryption	on	on
Radio 1 Enable Key Control	off	off

Figure 22. Cisco URWB managed by IoT OD – Device Configuration – Fluidity



ID 11
Saved - 2023-08-11 12:00:56 pm

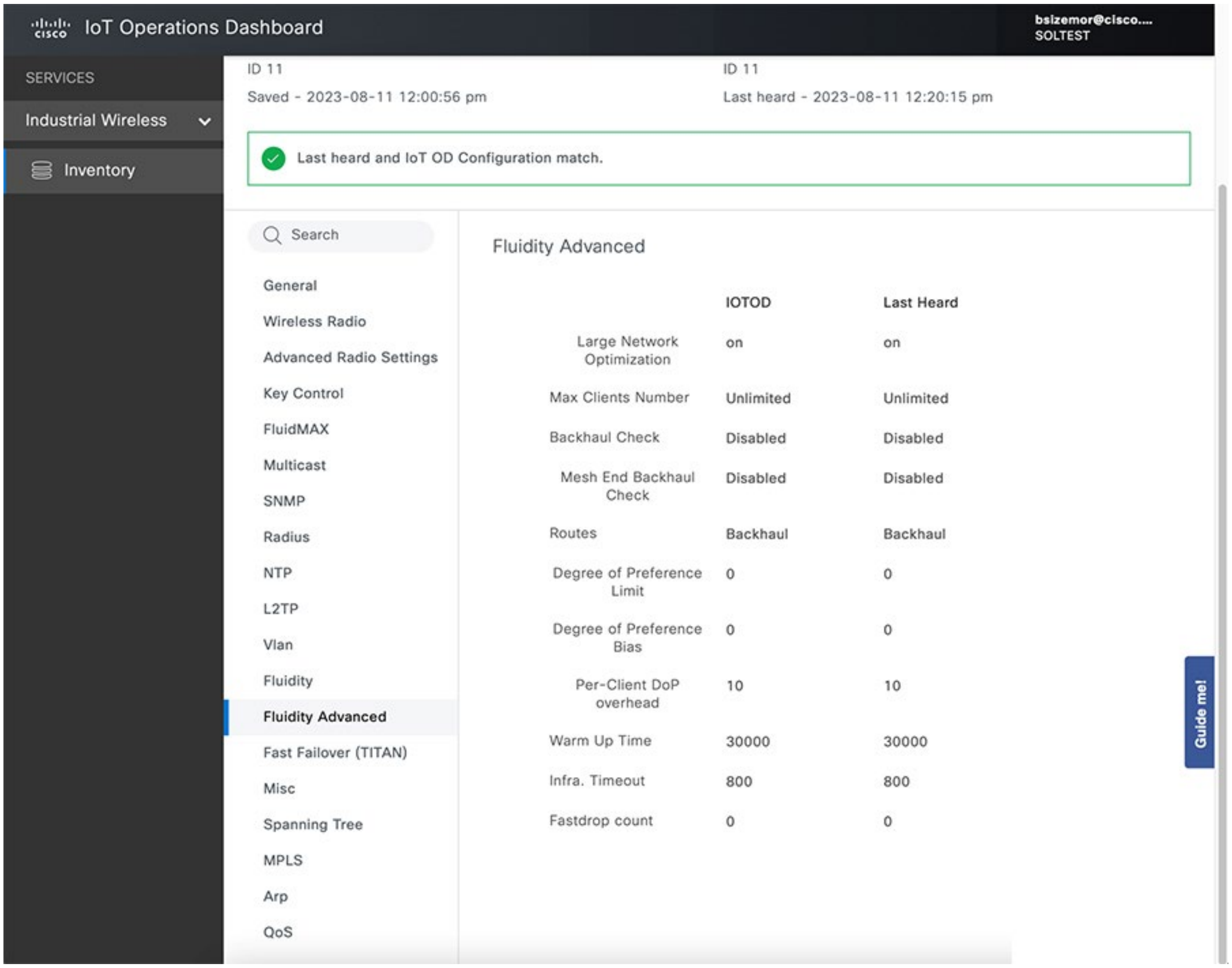
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Fluidity

	IOTOD	Last Heard
Unit Role	Infrastructure	Infrastructure
Network Type	Flat	Flat

Figure 23. Cisco URWB managed by IoT OD – Device Configuration – Fluidity Advanced



ID 11
Saved - 2023-08-11 12:00:56 pm

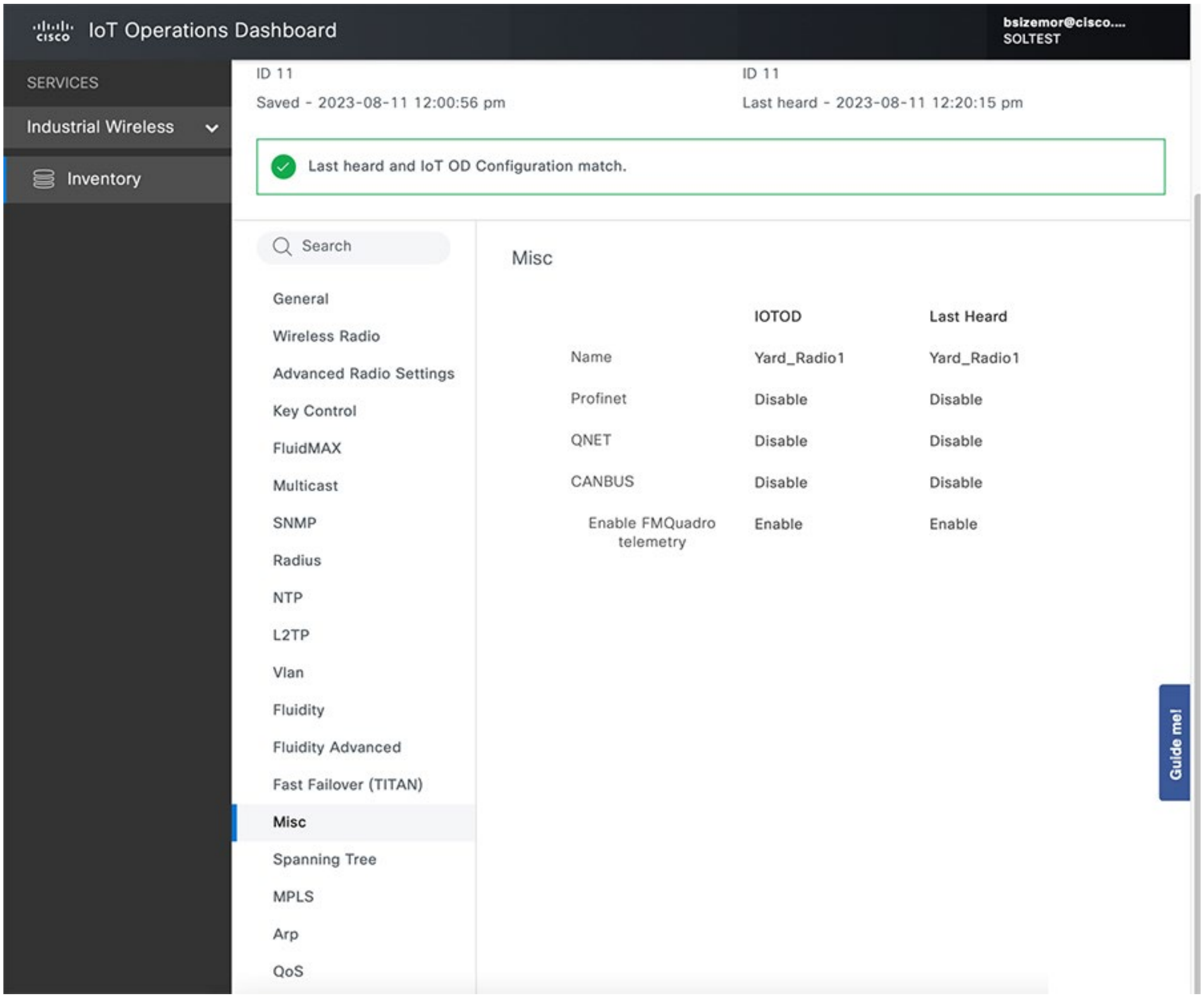
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Fluidity Advanced

	IOTOD	Last Heard
Large Network Optimization	on	on
Max Clients Number	Unlimited	Unlimited
Backhaul Check	Disabled	Disabled
Mesh End Backhaul Check	Disabled	Disabled
Routes	Backhaul	Backhaul
Degree of Preference Limit	0	0
Degree of Preference Bias	0	0
Per-Client DoP overhead	10	10
Warm Up Time	30000	30000
Infra. Timeout	800	800
Fastdrop count	0	0

Figure 24. Cisco URWB managed by IoT OD – Device Configuration – Misc



ID 11
Saved - 2023-08-11 12:00:56 pm

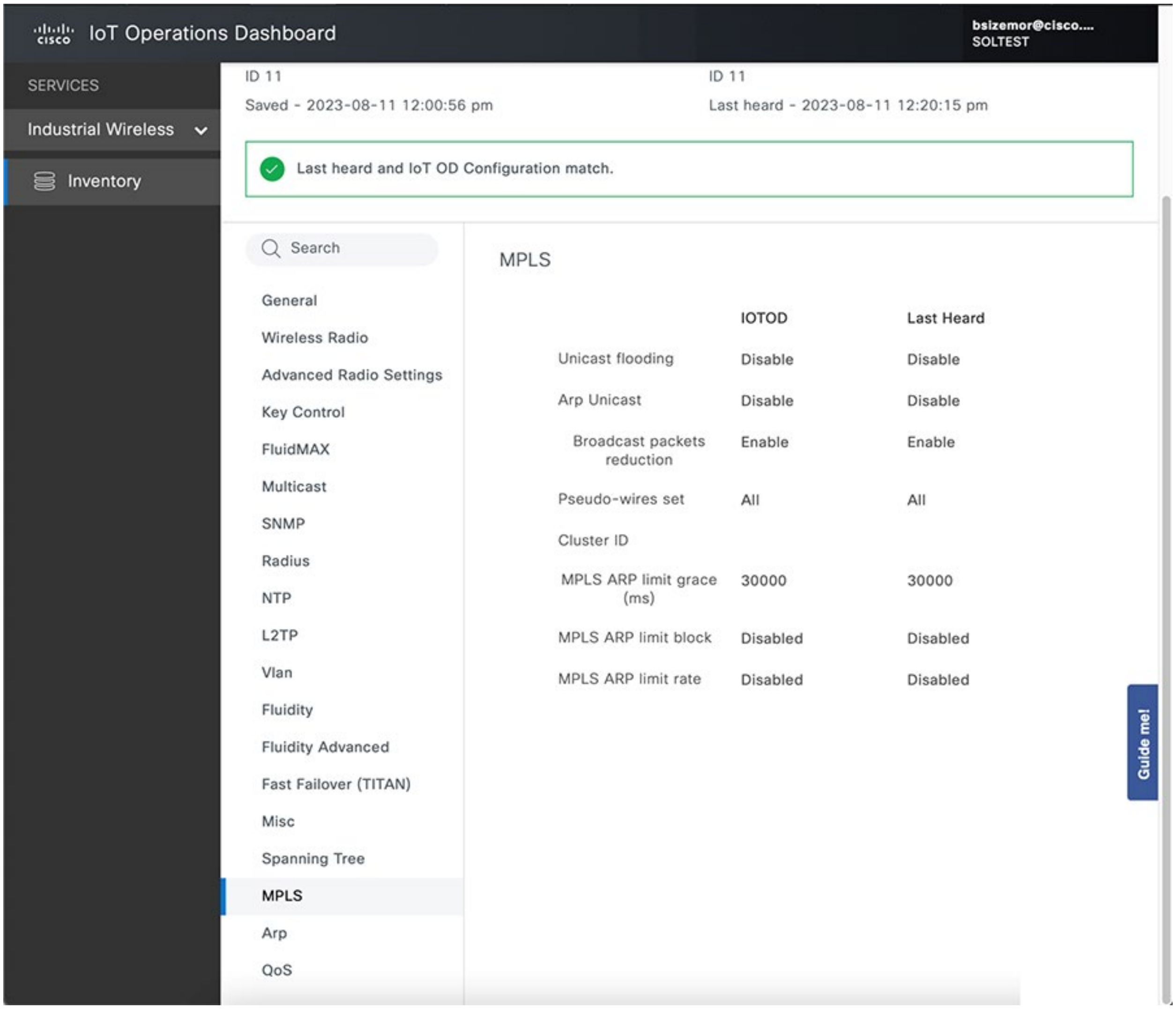
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Misc

	IOTOD	Last Heard
Name	Yard_Radio1	Yard_Radio1
Profinet	Disable	Disable
QNET	Disable	Disable
CANBUS	Disable	Disable
Enable FMQuadro telemetry	Enable	Enable

Figure 25. Cisco URWB managed by IoT OD – Device Configuration - MPLS



ID 11
Saved - 2023-08-11 12:00:56 pm

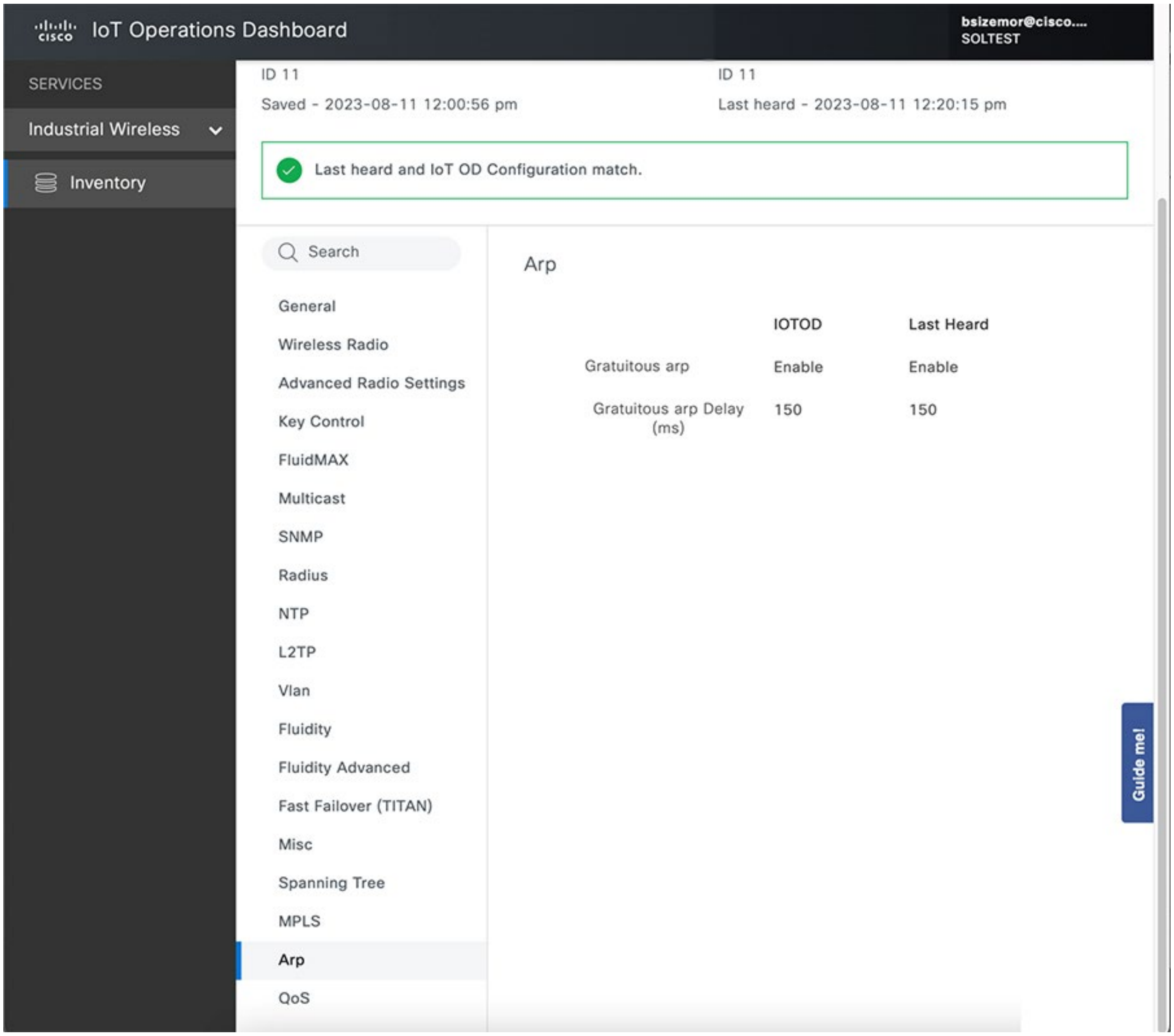
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

MPLS

	IOTOD	Last Heard
Unicast flooding	Disable	Disable
Arp Unicast	Disable	Disable
Broadcast packets reduction	Enable	Enable
Pseudo-wires set	All	All
Cluster ID		
MPLS ARP limit grace (ms)	30000	30000
MPLS ARP limit block	Disabled	Disabled
MPLS ARP limit rate	Disabled	Disabled

Figure 26. Cisco URWB managed by IoT OD – Device Configuration - ARP



ID 11
Saved - 2023-08-11 12:00:56 pm

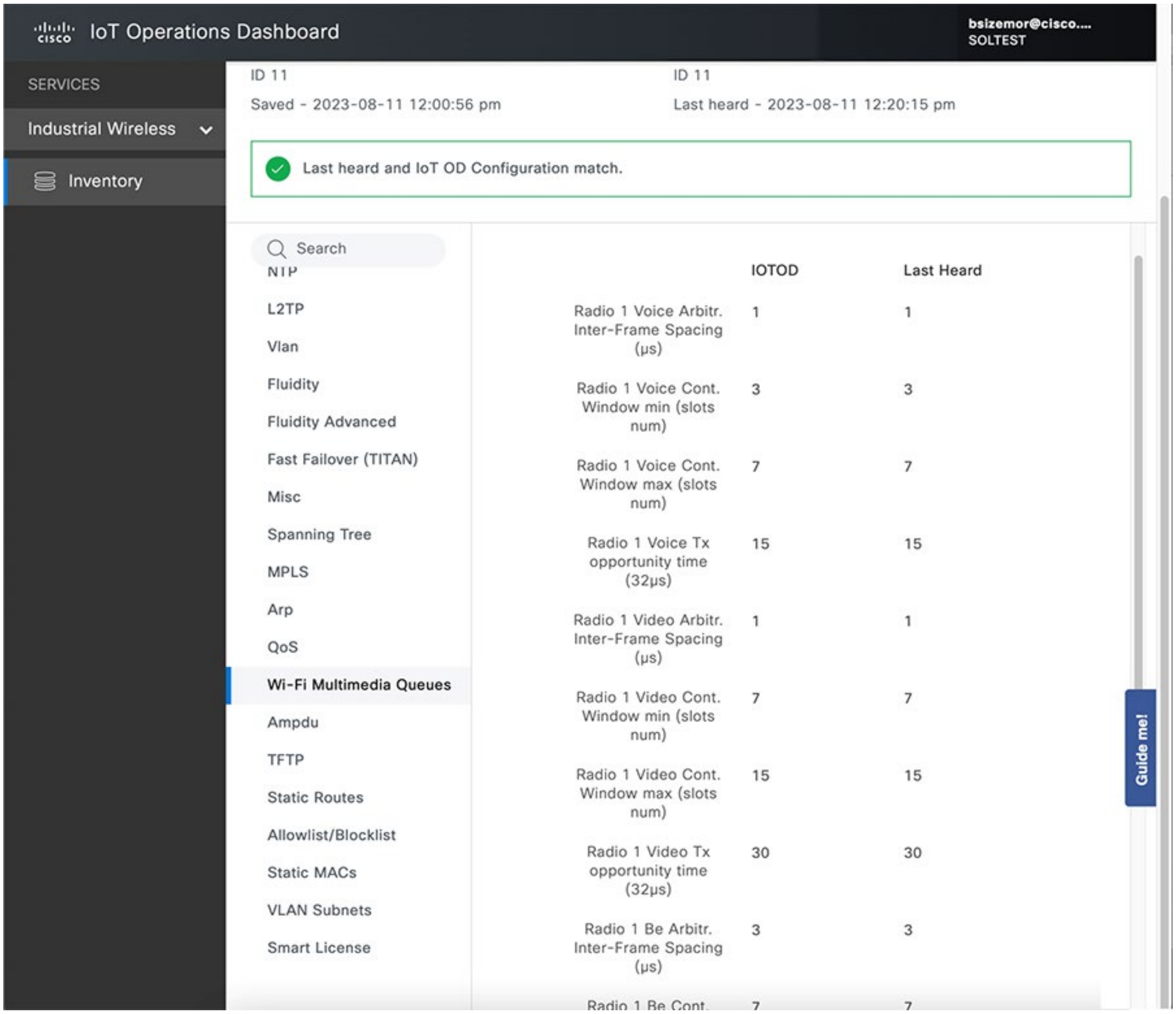
ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Arp

	IOTOD	Last Heard
Gratuitous arp	Enable	Enable
Gratuitous arp Delay (ms)	150	150

Figure 27. Cisco URWB managed by IoT OD – Device Configuration - Wi-Fi Multimedia Queues



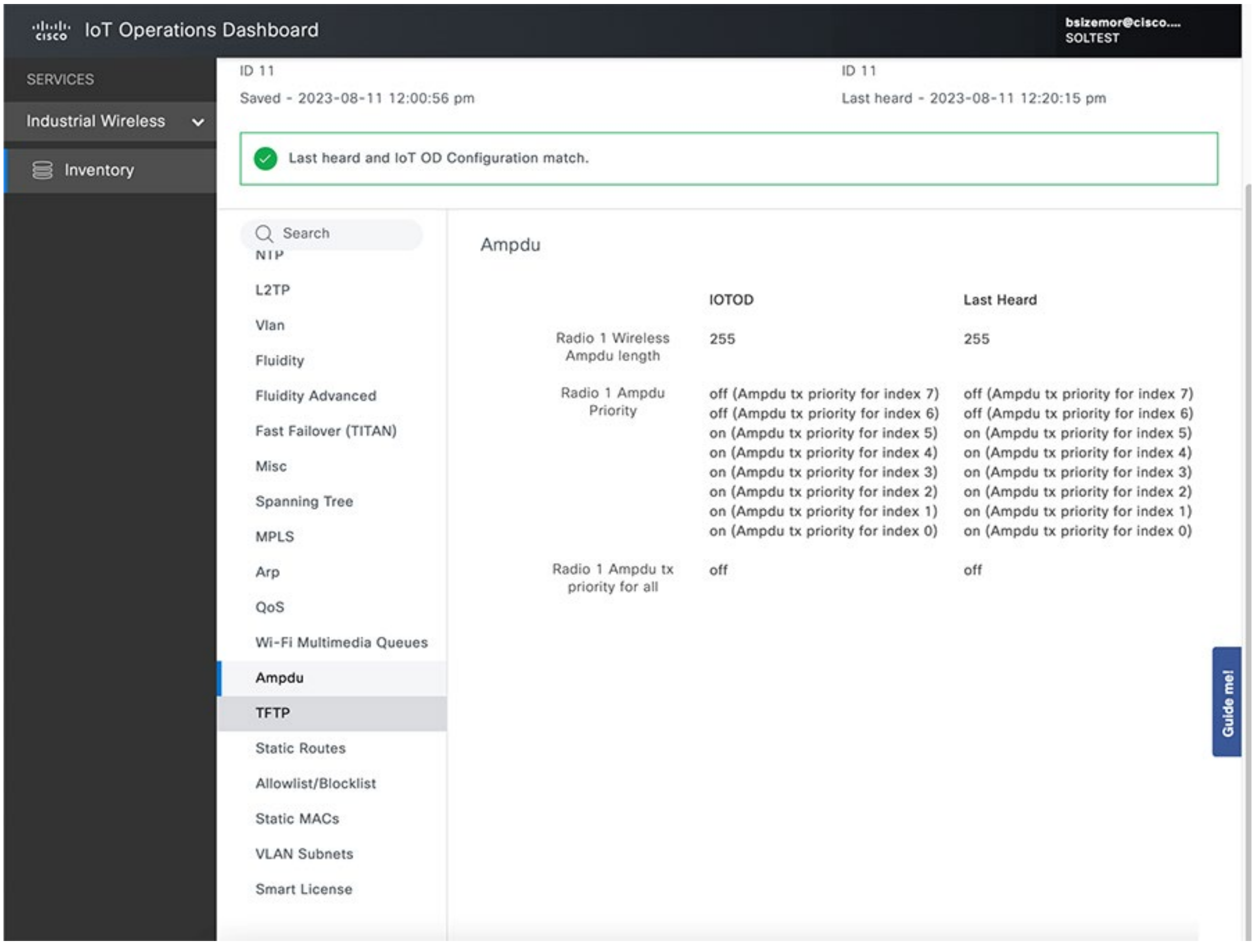
ID 11
Saved - 2023-08-11 12:00:56 pm

ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

	IOTOD	Last Heard
Radio 1 Voice Arbitr. Inter-Frame Spacing (μs)	1	1
Radio 1 Voice Cont. Window min (slots num)	3	3
Radio 1 Voice Cont. Window max (slots num)	7	7
Radio 1 Voice Tx opportunity time (32μs)	15	15
Radio 1 Video Arbitr. Inter-Frame Spacing (μs)	1	1
Radio 1 Video Cont. Window min (slots num)	7	7
Radio 1 Video Cont. Window max (slots num)	15	15
Radio 1 Video Tx opportunity time (32μs)	30	30
Radio 1 Be Arbitr. Inter-Frame Spacing (μs)	3	3
Radio 1 Be Cont.	7	7

Figure 28. Cisco URWB managed by IoT OD – Device Configuration – Ampdu



ID 11
Saved - 2023-08-11 12:00:56 pm

ID 11
Last heard - 2023-08-11 12:20:15 pm

Last heard and IoT OD Configuration match.

Ampdu

	IOTOD	Last Heard
Radio 1 Wireless Ampdu length	255	255
Radio 1 Ampdu Priority	off (Ampdu tx priority for index 7) off (Ampdu tx priority for index 6) on (Ampdu tx priority for index 5) on (Ampdu tx priority for index 4) on (Ampdu tx priority for index 3) on (Ampdu tx priority for index 2) on (Ampdu tx priority for index 1) on (Ampdu tx priority for index 0)	off (Ampdu tx priority for index 7) off (Ampdu tx priority for index 6) on (Ampdu tx priority for index 5) on (Ampdu tx priority for index 4) on (Ampdu tx priority for index 3) on (Ampdu tx priority for index 2) on (Ampdu tx priority for index 1) on (Ampdu tx priority for index 0)
Radio 1 Ampdu tx priority for all	off	off

C9800 WLC Configuration for IR1800 Wi-Fi in CAPWAP Mode with Captive Portal

The screenshots in this section summarize the Catalyst 9800 configuration used to implement Captive Portal authentication for mass transit passengers connected to either the IR1800 onboard AP, or a fixed AP in the transit station. The access points in both cases are managed by the Catalyst 9800 wireless LAN controller over a CAPWAP tunnel.

The access points are configured with FlexConnect Local Switching to optimize the data path from passenger wireless clients to the Internet.

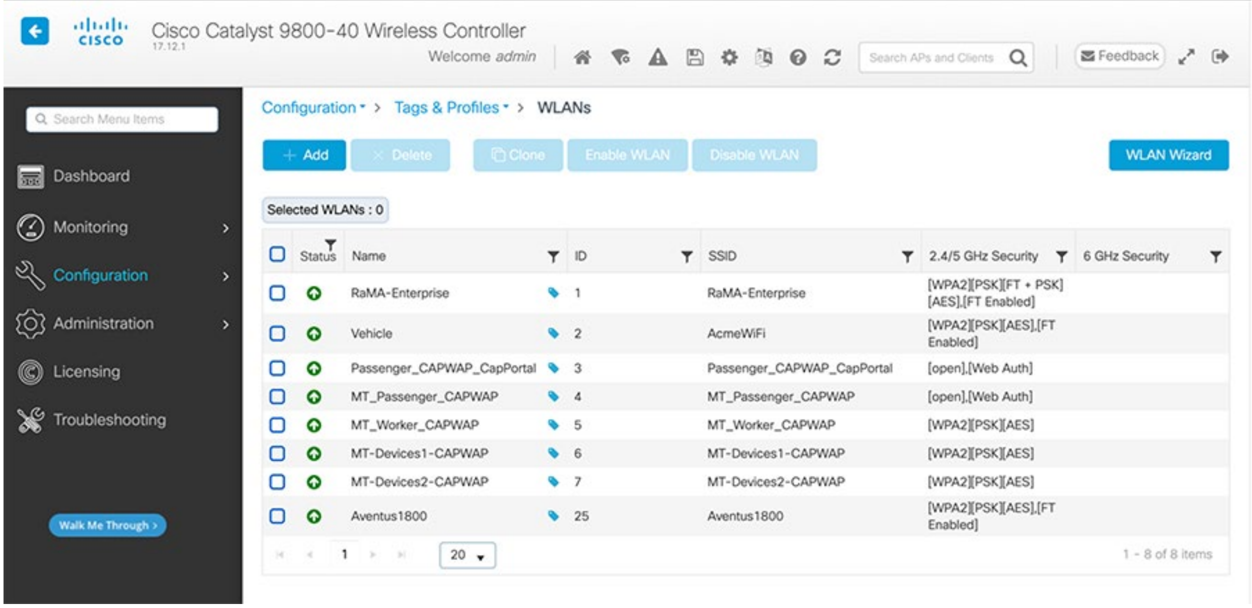
The configuration of the C9800 for CAPWAP and Captive Portal is divided into the following parts:

- Configure WLAN
  - WAN General
  - WAN Security
- Configure Profiles
- Configure Tags
- Verification

Configure WLAN

The first screenshot shows multiple WLANs have been created, all starting with "MT-" in this example. All of these SSIDs will be extended to the IR1800 built in APs. The "MT_Passenger_CAPWAP" SSID is the focus of this section. Notice how it is using Web Auth, versus WPA2-PSK for the other SSIDs.

Figure 29. Cisco Catalyst 9800 – WLANs list



Selected WLANs : 0

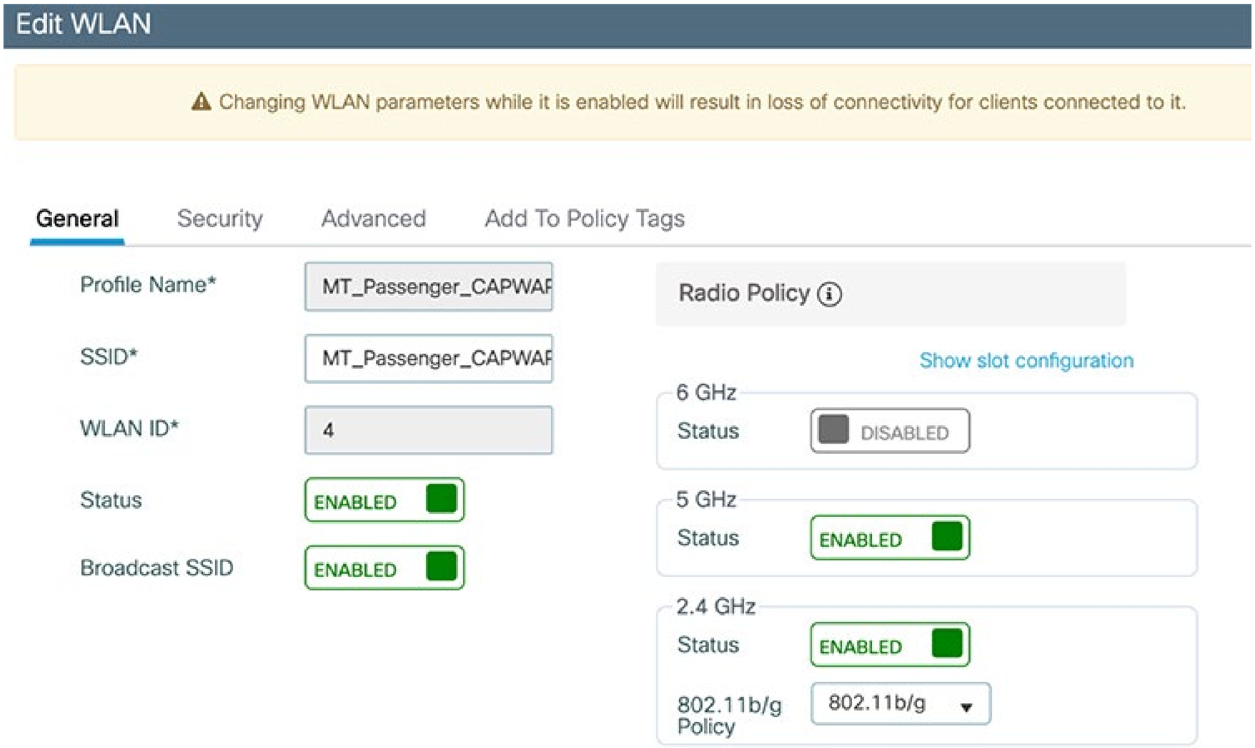
□	Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
□	●	RaMA-Enterprise	1	RaMA-Enterprise	[WPA2][PSK][FT + PSK][AES],[FT Enabled]	
□	●	Vehicle	2	AcmeWiFi	[WPA2][PSK][AES],[FT Enabled]	
□	●	Passenger_CAPWAP_CapPortal	3	Passenger_CAPWAP_CapPortal	[open],[Web Auth]	
□	●	MT_Passenger_CAPWAP	4	MT_Passenger_CAPWAP	[open],[Web Auth]	
□	●	MT_Worker_CAPWAP	5	MT_Worker_CAPWAP	[WPA2][PSK][AES]	
□	●	MT-Devices1-CAPWAP	6	MT-Devices1-CAPWAP	[WPA2][PSK][AES]	
□	●	MT-Devices2-CAPWAP	7	MT-Devices2-CAPWAP	[WPA2][PSK][AES]	
□	●	Aventus1800	25	Aventus1800	[WPA2][PSK][AES],[FT Enabled]	

1 20 1 - 8 of 8 items

WLAN General

The WLAN is **Enabled** for both 2.4 GHz and 5 GHz bands.

Figure 30. Cisco Catalyst 9800 – Edit WLAN - General



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Profile Name* MT_Passenger_CAPWAF

SSID* MT_Passenger_CAPWAF

WLAN ID* 4

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

6 GHz
Status DISABLED

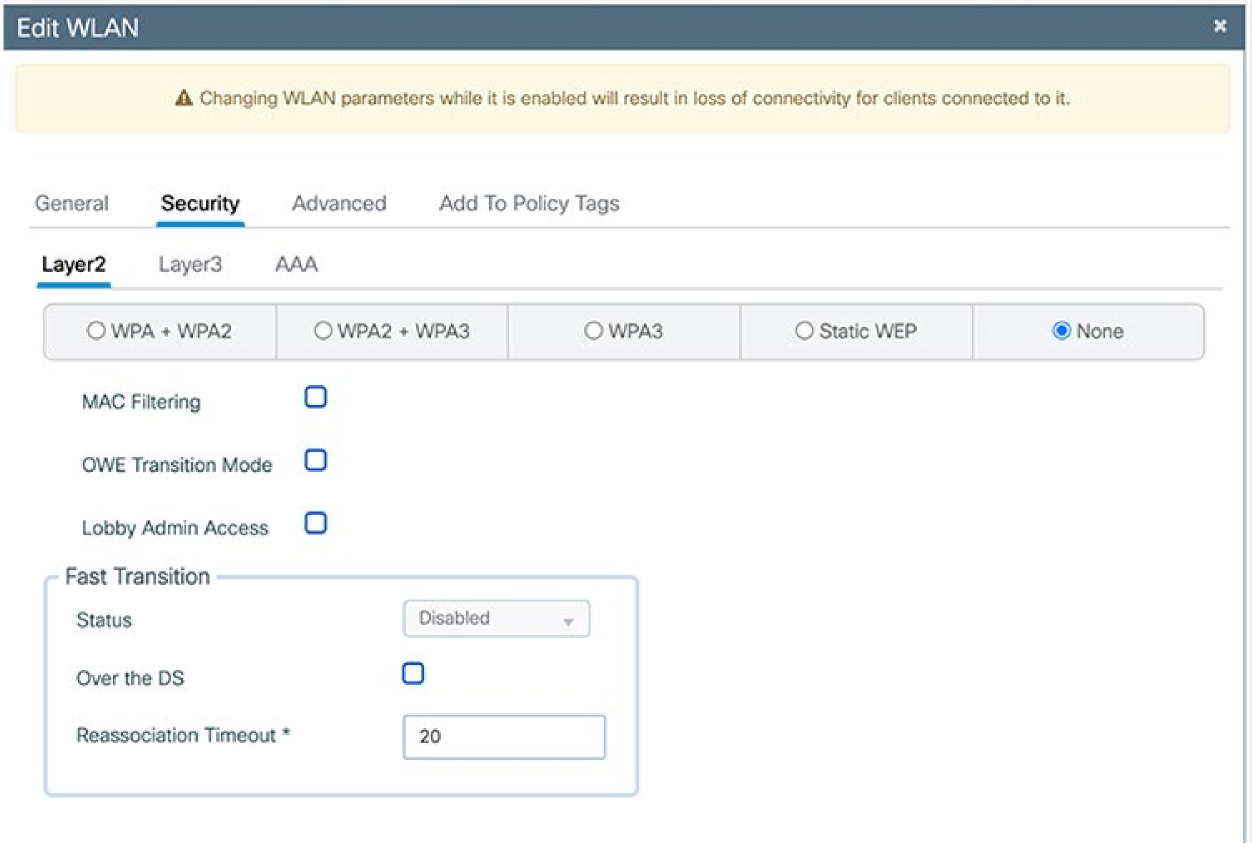
5 GHz
Status ENABLED

2.4 GHz
Status ENABLED
802.11b/g Policy 802.11b/g ▾

WLAN Security

The security configuration for the Passenger SSID is where the captive portal authentication method is defined. In the Layer2 tab, **None** is selected as the security mechanism.

Figure 31. Cisco Catalyst 9800 – Edit WLAN – Security – Layer2



⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

○ WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ● None

MAC Filtering □

OWE Transition Mode □

Lobby Admin Access □

Fast Transition

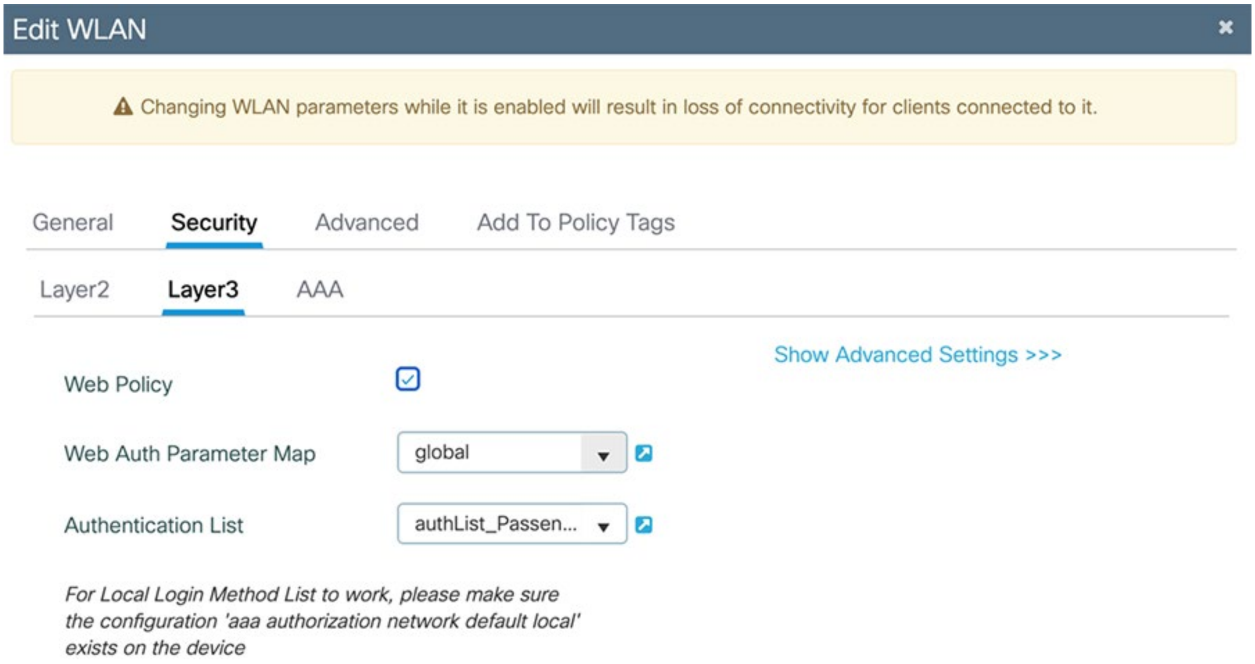
Status: Disabled

Over the DS □

Reassociation Timeout *: 20

The WLAN Layer3 Security settings enable Web authentication (also known as Captive Portal). The Web Auth Parameter Map is set to **global**.

Figure 32. Cisco Catalyst 9800 – Edit WLAN – Security – Layer3



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Web Policy ☑

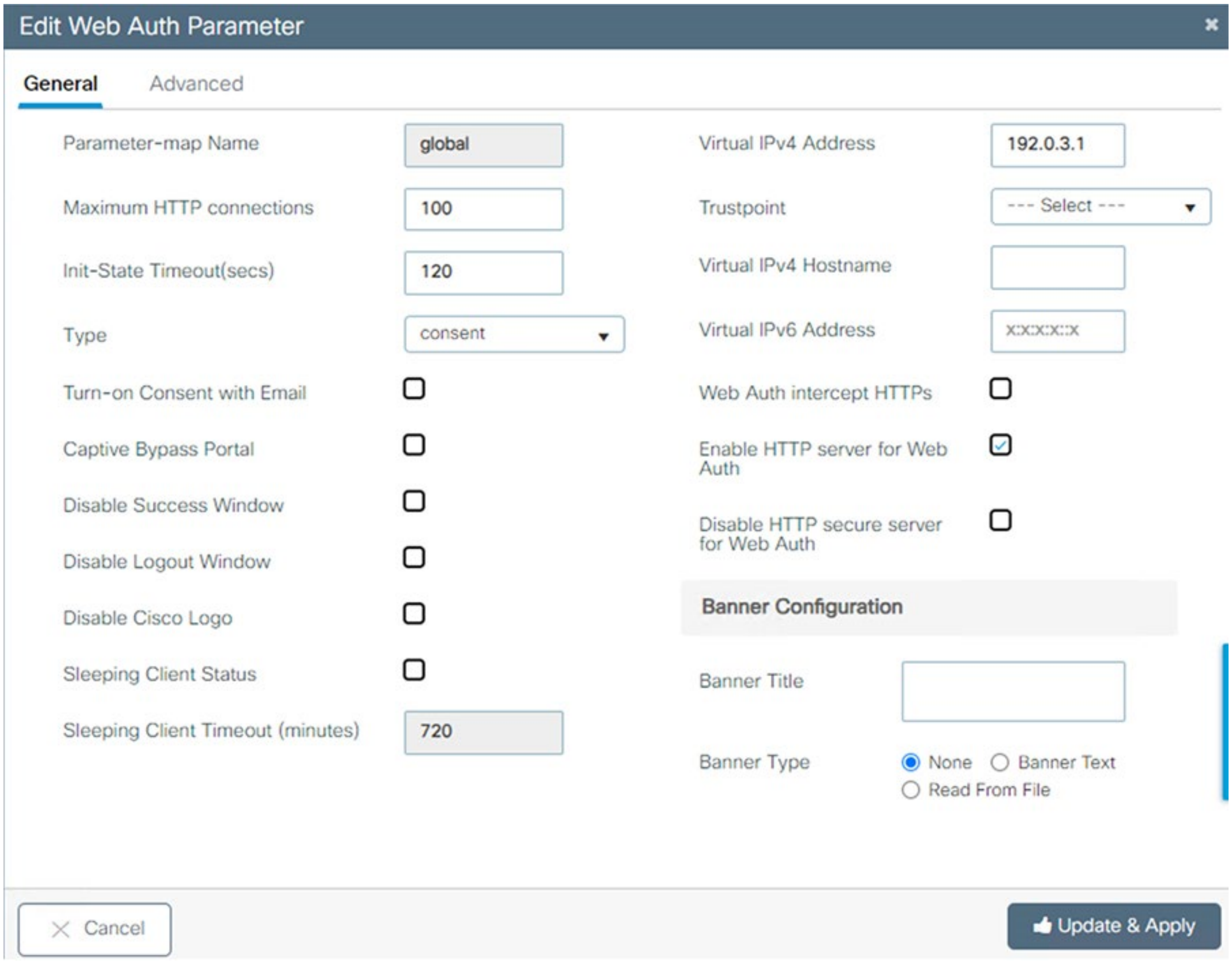
Web Auth Parameter Map: global

Authentication List: authList_Passen...

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

The **global** web auth parameter is set to type **consent** so that when users attempt to connect, they are presented with a web page on which they need to click **Accept** to acknowledge the terms before being allowed access to the network. This option is set under **Configuration > Security > Web Auth**.

Figure 34. Cisco Catalyst 9800 – Edit Web Auth Parameter



Edit Web Auth Parameter

General | Advanced

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: consent

Turn-on Consent with Email □

Captive Bypass Portal □

Disable Success Window □

Disable Logout Window □

Disable Cisco Logo □

Sleeping Client Status □

Sleeping Client Timeout (minutes): 720

Virtual IPv4 Address: 192.0.3.1

Trustpoint: --- Select ---

Virtual IPv4 Hostname:

Virtual IPv6 Address: X:X:X:X::X

Web Auth intercept HTTPs □

Enable HTTP server for Web Auth ☑

Disable HTTP secure server for Web Auth □

Banner Configuration

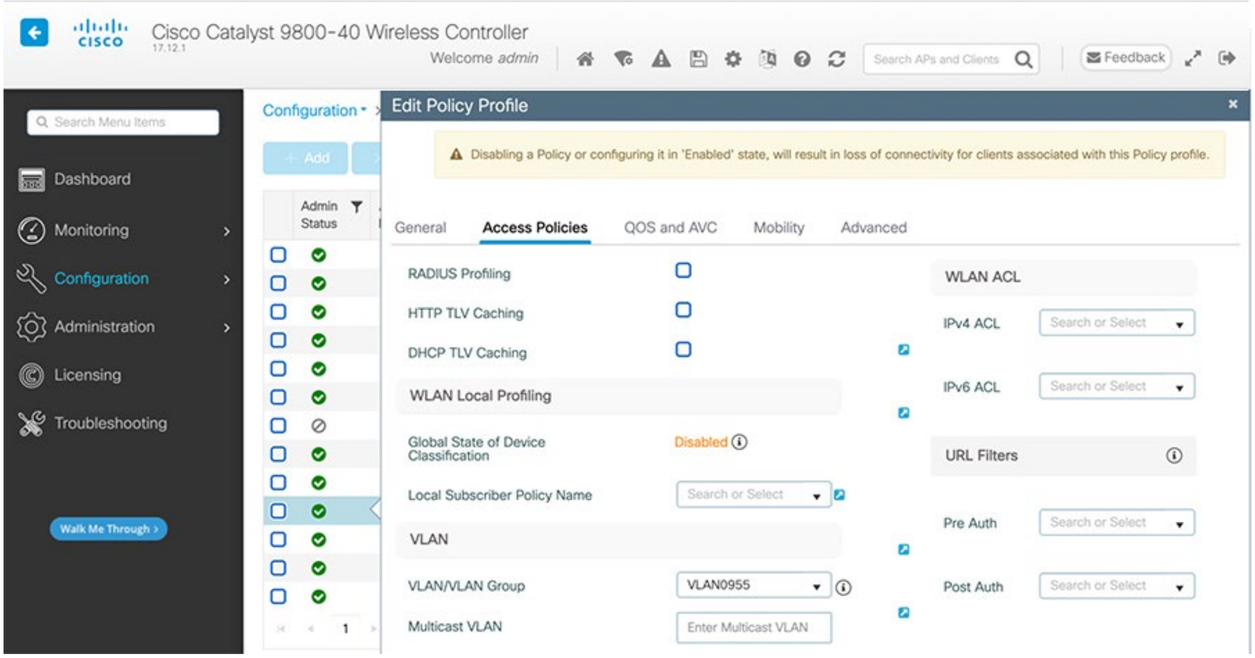
Banner Title:

Banner Type: ● None ○ Banner Text ○ Read From File

Configure Profiles

Edit the **Policy Profile** to associate the WLAN to the correct VLAN, which is **VLAN0955** in this case, and is reserved for passenger data.

Figure 34. Cisco Catalyst 9800 – Edit Policy Profile – Access Policies



Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

RADIUS Profiling □
HTTP TLV Caching □
DHCP TLV Caching □

WLAN Local Profiling

Global State of Device Classification: Disabled
Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: VLAN0955
Multicast VLAN: Enter Multicast VLAN

WLAN ACL

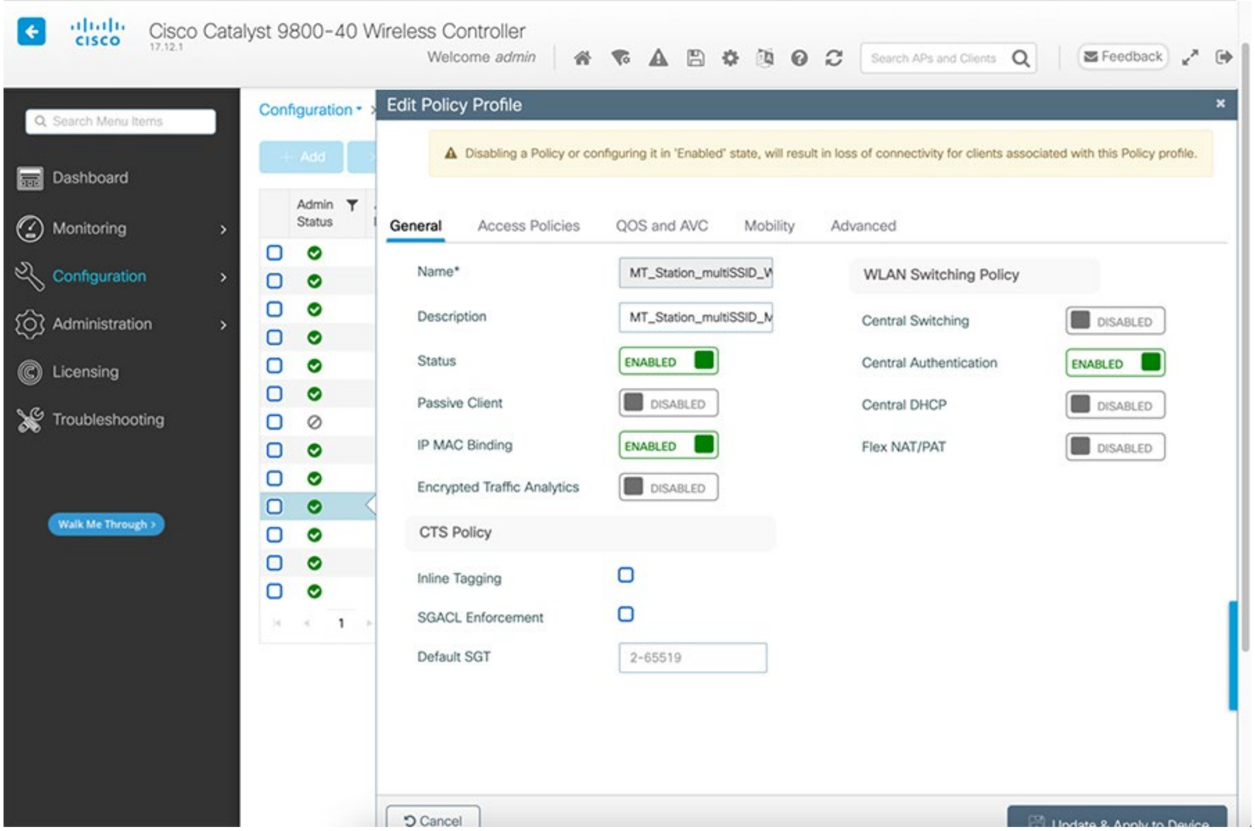
IPv4 ACL: Search or Select
IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select
Post Auth: Search or Select

Also configure the profile for **Central Authentication Enabled**, as shown in the screenshot that follows. Note that **Central Switching** is **Disabled** – resulting in FlexConnect local switching being used so that passenger traffic does not need to be backhauled to the enterprise datacenter. Additional FlexConnect settings are defined later.

Figure 35. Cisco Catalyst 9800 – Edit Policy Profile – General



Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*: MT_Station_multiSSID_W
Description: MT_Station_multiSSID_M
Status: ENABLED
Passive Client: DISABLED
IP MAC Binding: ENABLED
Encrypted Traffic Analytics: DISABLED

CTS Policy

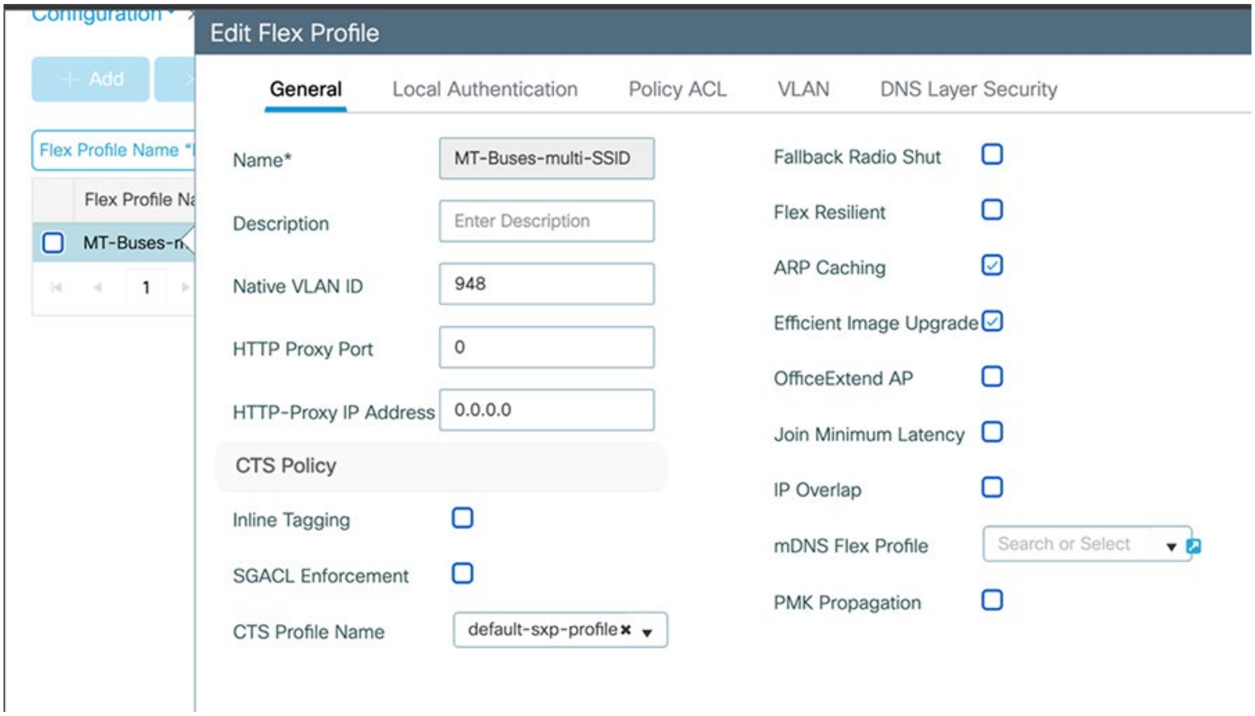
Inline Tagging: □
SGACL Enforcement: □
Default SGT: 2-65519

WLAN Switching Policy

Central Switching: DISABLED
Central Authentication: ENABLED
Central DHCP: DISABLED
Flex NAT/PAT: DISABLED

Edit the **Flex Profile** to identify the VLANs that will be locally switched. In the **General** tab, VLAN **948** is specified as the **Native VLAN**. This is the default LAN subnet that is created by the eCVD template and is used for AP management communication to the WLC. Passenger and other SSID traffic will each have their own separate VLAN to provide segmentation.

Figure 36. Cisco Catalyst 9800 – Edit Flex Profile – General



Name* MT-Buses-multi-SSID

Description Enter Description

Native VLAN ID 948

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

CTS Profile Name default-sxp-profile

Fallback Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

OfficeExtend AP □

Join Minimum Latency □

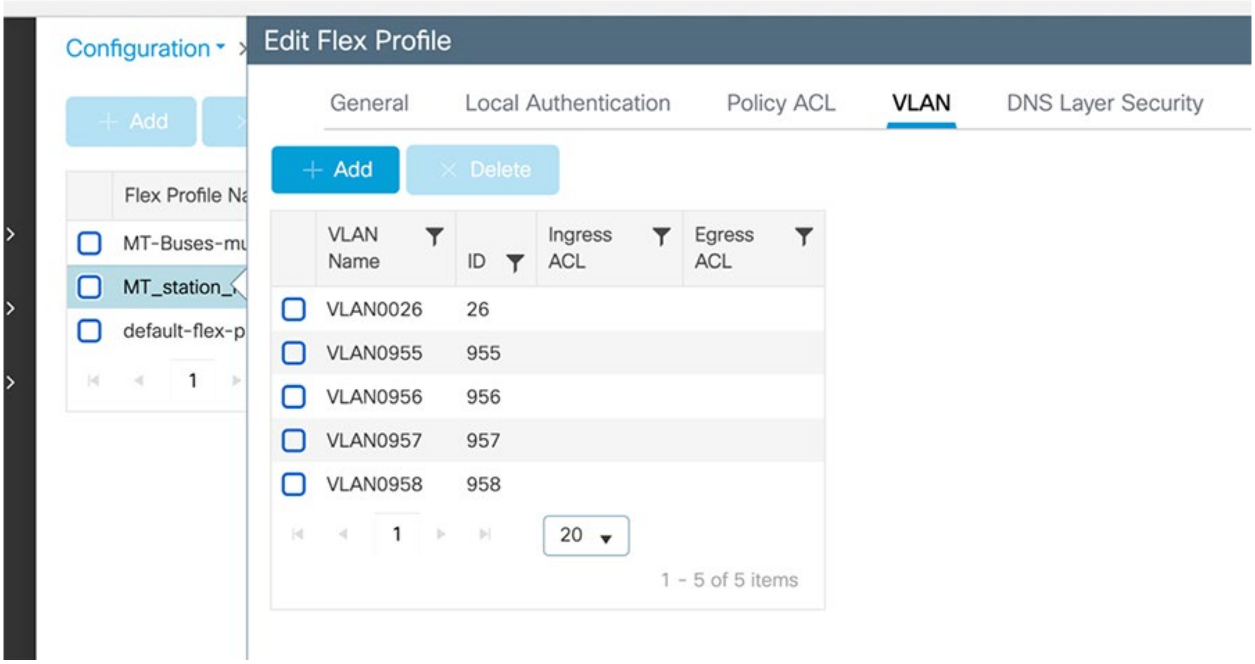
IP Overlap □

mDNS Flex Profile Search or Select

PMK Propagation □

Passenger clients will connect on **VLAN955**. Other VLANs for other SSIDs are also defined here.

Figure 37. Cisco Catalyst 9800 – Edit Flex Profile - VLAN

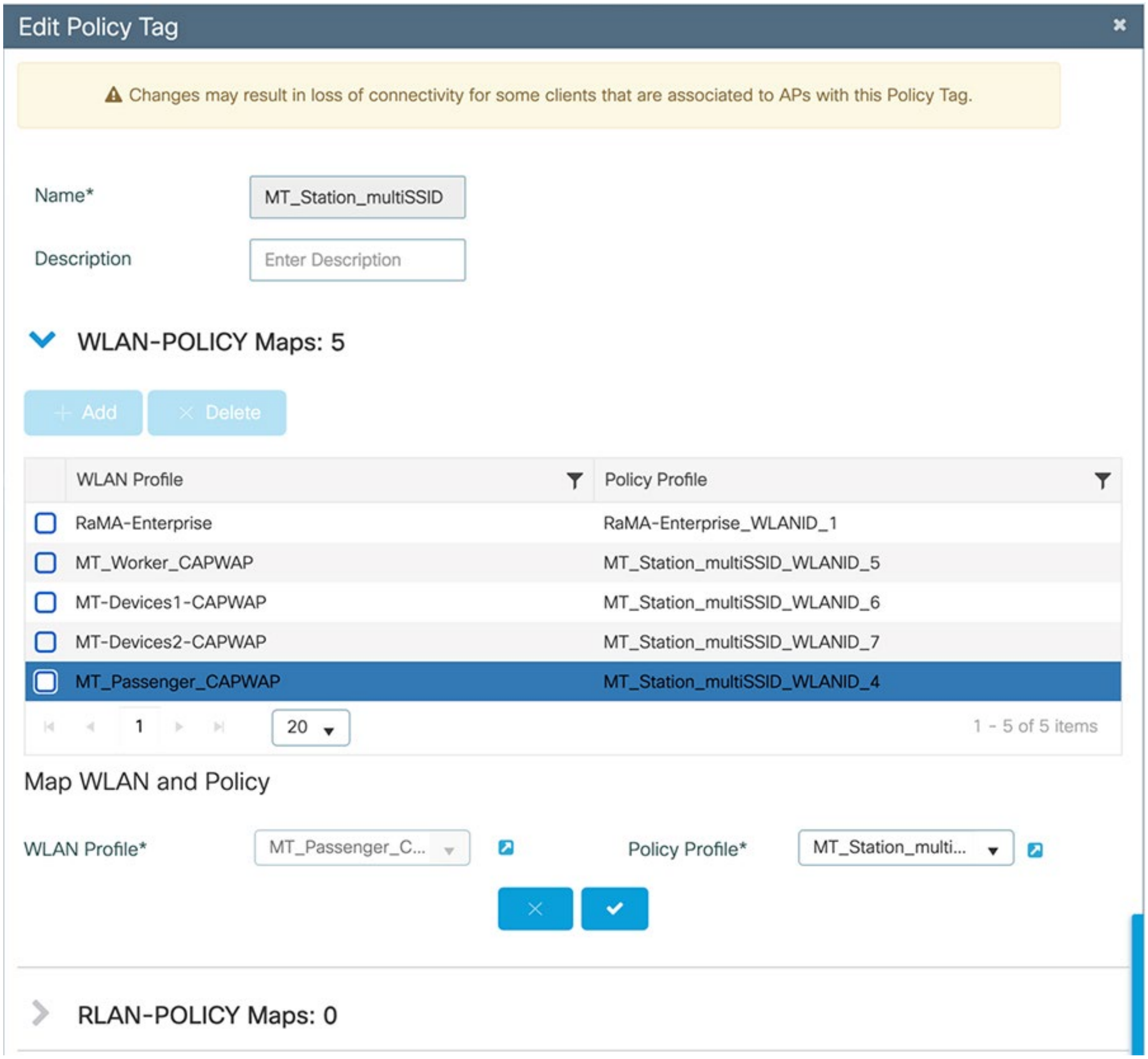


	VLAN Name	ID	Ingress ACL	Egress ACL
□	VLAN0026	26		
□	VLAN0955	955		
□	VLAN0956	956		
□	VLAN0957	957		
□	VLAN0958	958		

Configure Tags

Use a **Policy Tag** to associate a WLAN Profile and Policy Profile.

Figure 38. Cisco Catalyst 9800 – Edit Policy Tag – MT_Passenger_CAPWAP



Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: MT_Station_multiSSID

Description: Enter Description

WLAN-POLICY Maps: 5

	WLAN Profile	Policy Profile
□	RaMA-Enterprise	RaMA-Enterprise_WLANID_1
□	MT_Worker_CAPWAP	MT_Station_multiSSID_WLANID_5
□	MT-Devices1-CAPWAP	MT_Station_multiSSID_WLANID_6
□	MT-Devices2-CAPWAP	MT_Station_multiSSID_WLANID_7
□	MT_Passenger_CAPWAP	MT_Station_multiSSID_WLANID_4

Map WLAN and Policy

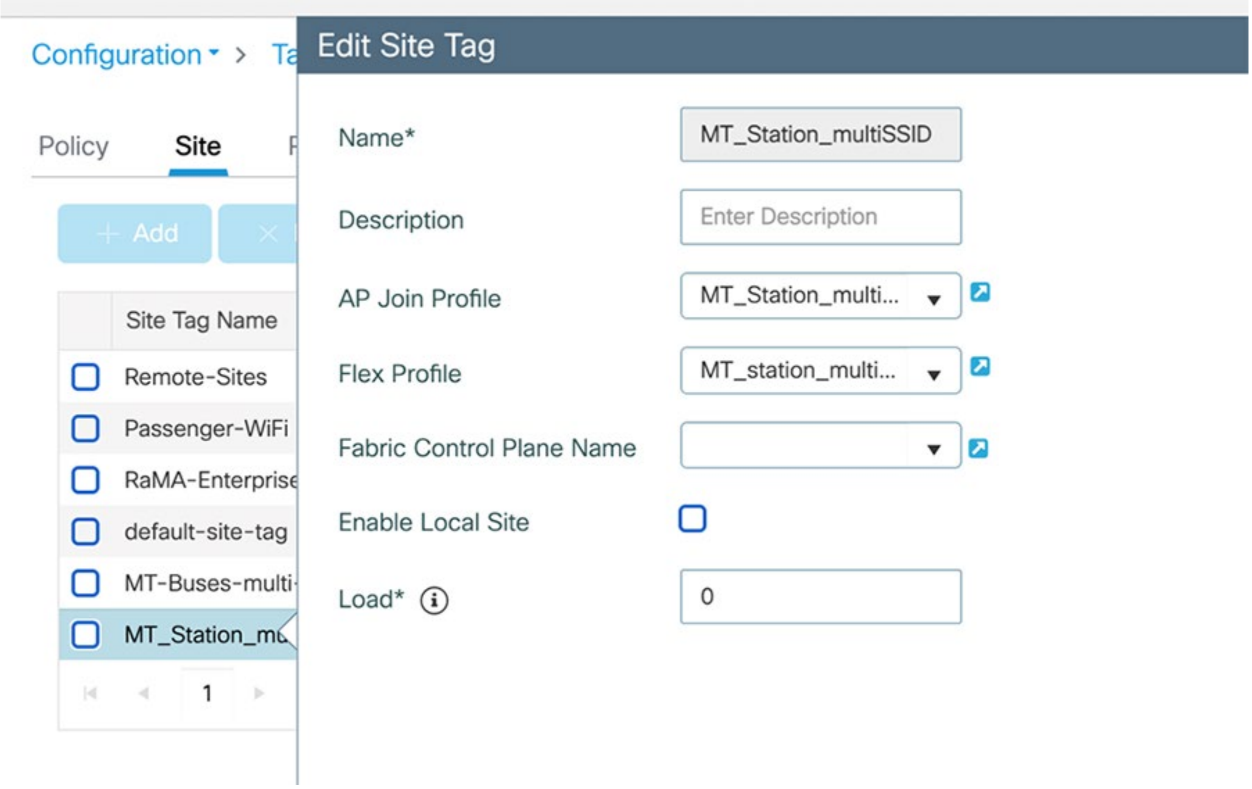
WLAN Profile*: MT_Passenger_C...

Policy Profile*: MT_Station_multi...

RLAN-POLICY Maps: 0

Use the **Site Tag** to associate the **Flex Profile**.

Figure 39. Cisco Catalyst 9800 – Edit Site Tag



Name* MT_Station_multiSSID

Description Enter Description

AP Join Profile MT_Station_multi...

Flex Profile MT_station_multi...

Fabric Control Plane Name

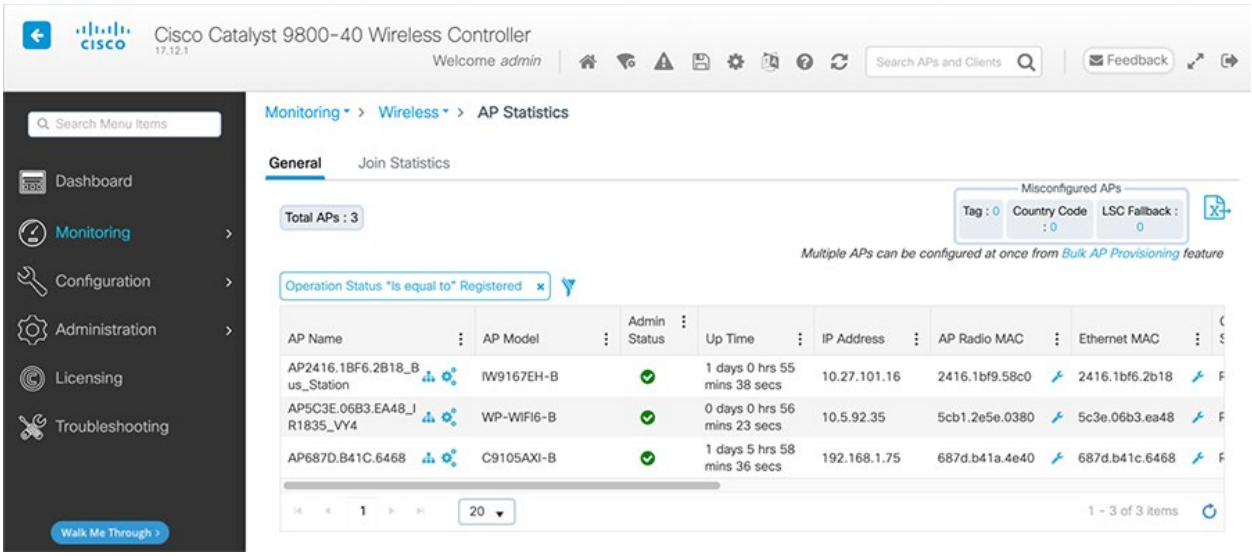
Enable Local Site □

Load* 0

Verify

Verify that the access points are registered with the Catalyst 9800 wireless LAN controller.

Figure 40. Cisco Catalyst 9800 – Monitoring – AP Statistics



Total APs : 3

Misconfigured APs: Tag : 0 | Country Code : 0 | LSC Fallback : 0

Multiple APs can be configured at once from Bulk AP Provisioning feature

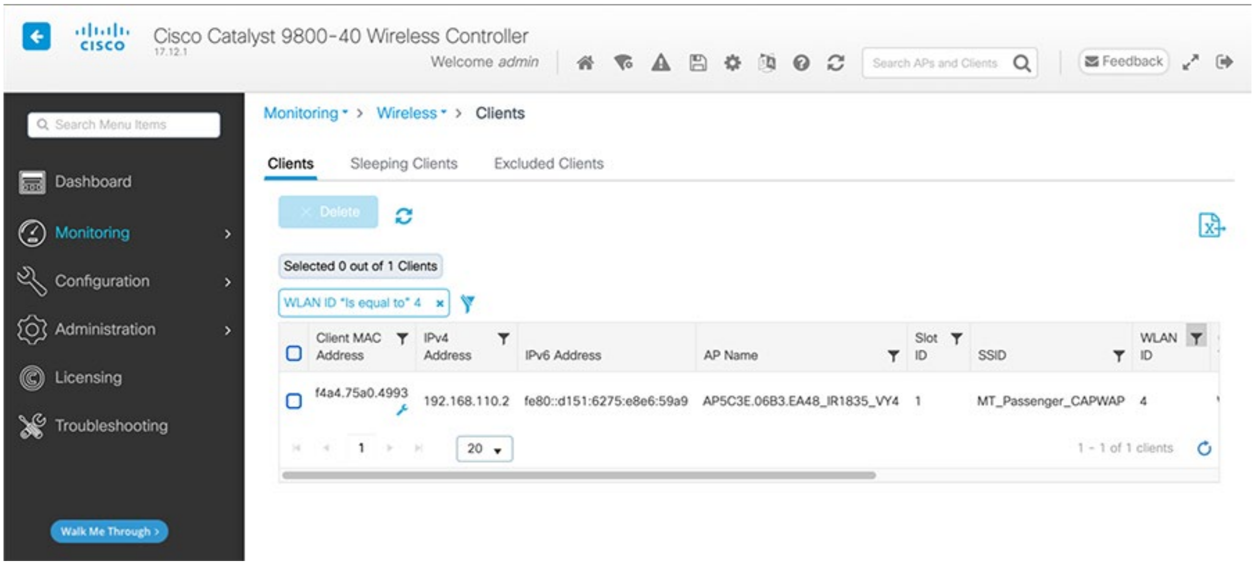
Operation Status "Is equal to" Registered

AP Name	AP Model	Admin Status	Up Time	IP Address	AP Radio MAC	Ethernet MAC
AP2416.1BF6.2B18_Bus_Station	IW9167EH-B	✓	1 days 0 hrs 55 mins 38 secs	10.27.101.16	2416.1bf9.58c0	2416.1bf6.2b18
AP5C3E.06B3.EA48_IR1835_VY4	WP-WIFI6-B	✓	0 days 0 hrs 56 mins 23 secs	10.5.92.35	5cb1.2e5e.0380	5c3e.06b3.ea48
AP687D.B41C.6468	C9105AXI-B	✓	1 days 5 hrs 58 mins 36 secs	192.168.1.75	687d.b41a.4e40	687d.b41c.6468

1 20 ▾ 1 - 3 of 3 items

Verify that wireless clients can connect to the **MT_Passenger_CAPWAP** SSID.

Figure 41. Cisco Catalyst 9800 – Monitoring – Wireless Clients in MT_Passenger_CAPWAP



Selected 0 out of 1 Clients

WLAN ID "Is equal to" 4

□	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID
□	f4a4.75a0.4993	192.168.110.2	fe80::d151:6275:e8e6:59a9	AP5C3E.06B3.EA48_IR1835_VY4	1	MT_Passenger_CAPWAP	4

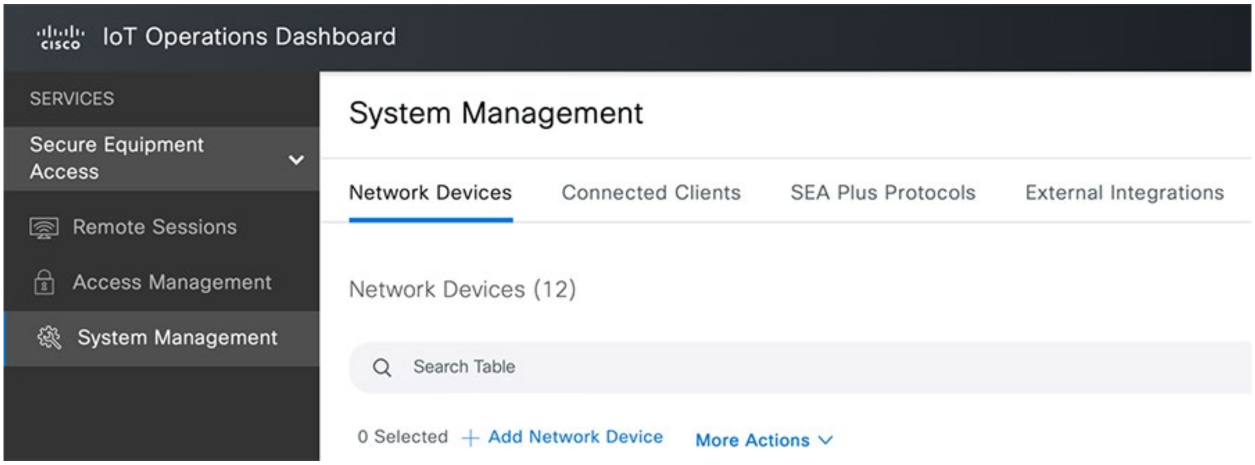
1 20 ▾ 1 - 1 of 1 clients

Secure Equipment Access to Onboard Equipment

Cisco Secure Equipment Access (SEA) is a service available in the IoT Operations Dashboard that enables remote connectivity to applications and devices connected behind the industrial router. In this example, the SEA service is used to deploy the SEA agent on the IR1800 and enable remote connectivity to a Windows server running on the bus which hosts the Milestone XProtect application for video recording.

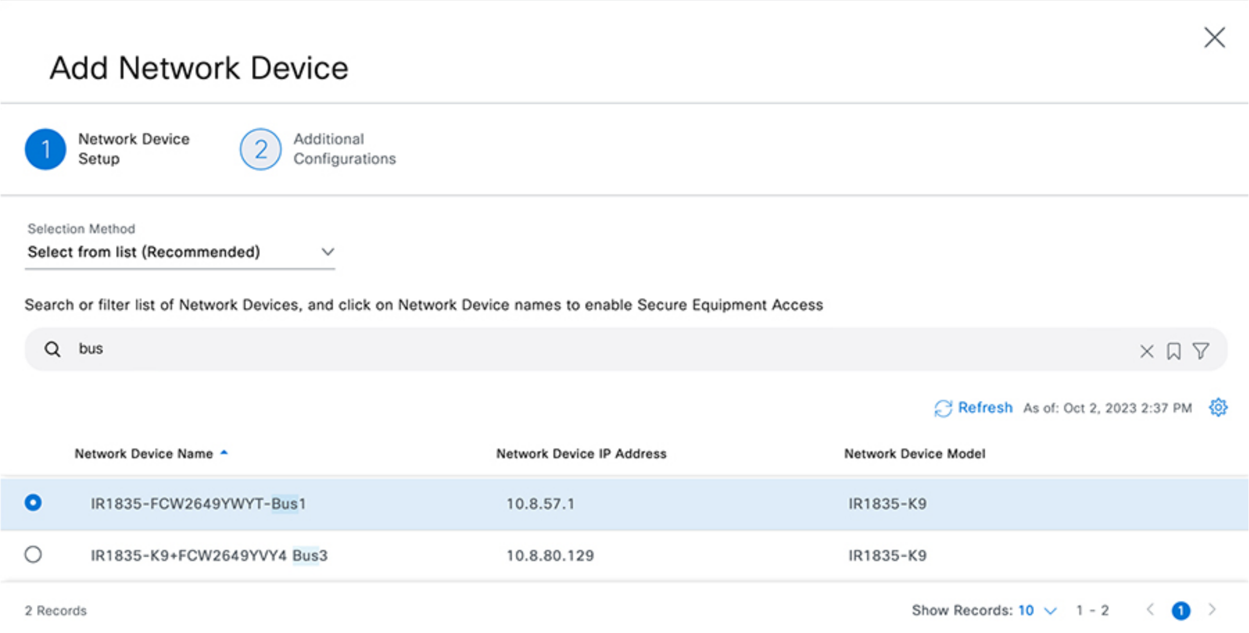
1. Install the SEA agent application from the IoT Operations Dashboard by navigating to the **Secure Equipment Access > System Management > Network Devices**, and then clicking **Add Network Device**.

Figure 42. SEA System Management



2. Select the network device that will host the SEA agent. In this example, an **IR1835** router is selected.

Figure 43. SEA – Add Network Device



Add Network Device

1 Network Device Setup

2 Additional Configurations

Selection Method
Select from list (Recommended)

Search or filter list of Network Devices, and click on Network Device names to enable Secure Equipment Access

bus

Refresh As of: Oct 2, 2023 2:37 PM

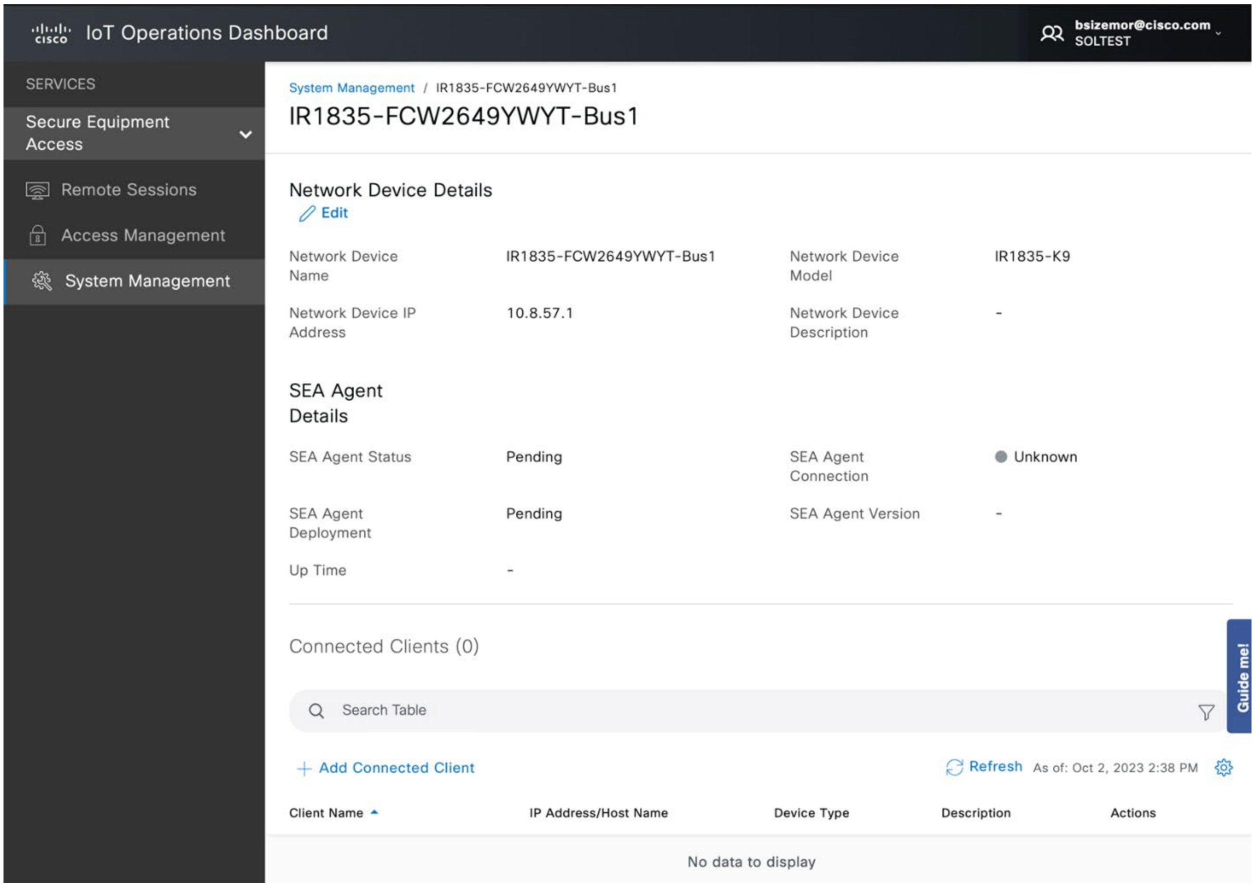
	Network Device Name	Network Device IP Address	Network Device Model
●	IR1835-FCW2649YWYT-Bus1	10.8.57.1	IR1835-K9
○	IR1835-K9+FCW2649YVY4 Bus3	10.8.80.129	IR1835-K9

2 Records

Show Records: 10 1 - 2 1

3. The agent is then deployed on the router. During the deployment (or later), click **Add Connected Client**.

Figure 44. SEA Network Device Details and Connected Clients list



IR1835-FCW2649YWYT-Bus1

Network Device Details

Network Device Name	IR1835-FCW2649YWYT-Bus1	Network Device Model	IR1835-K9
Network Device IP Address	10.8.57.1	Network Device Description	-

SEA Agent Details

SEA Agent Status	Pending	SEA Agent Connection	● Unknown
SEA Agent Deployment	Pending	SEA Agent Version	-
Up Time	-		

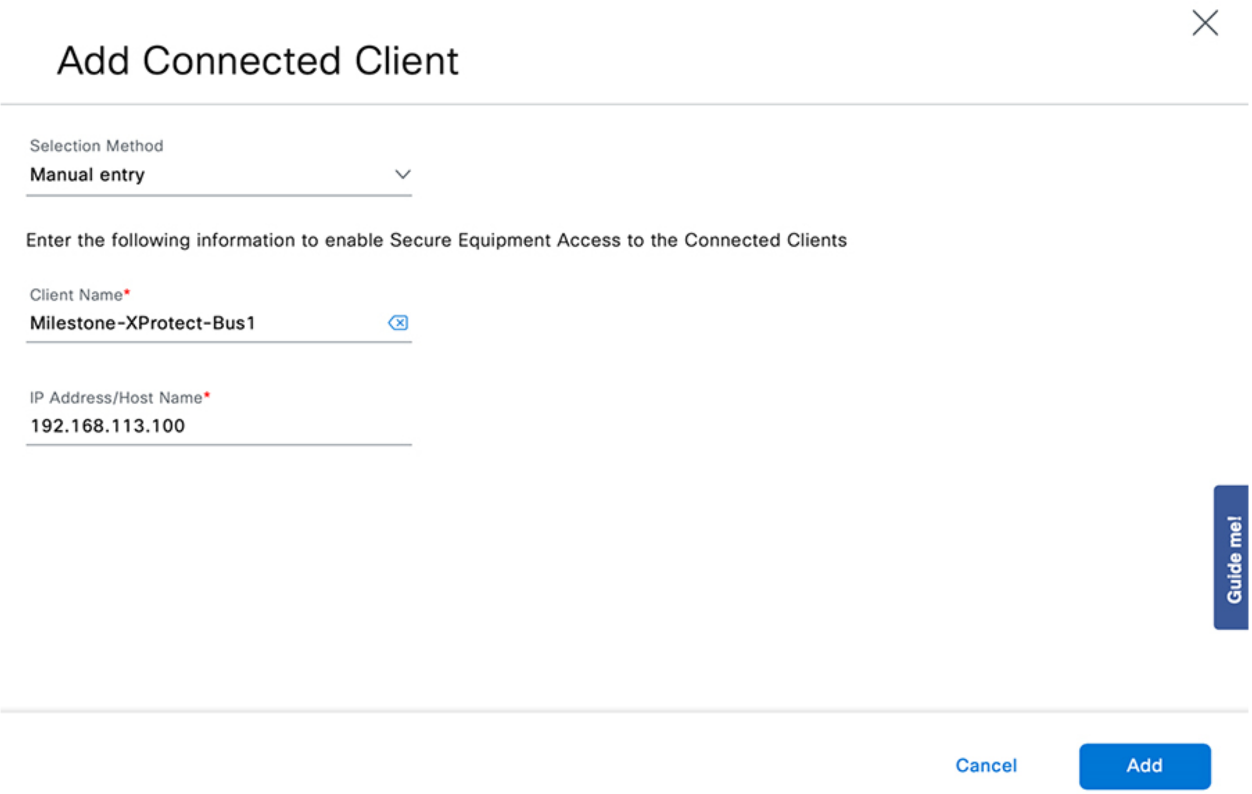
Connected Clients (0)

As of: Oct 2, 2023 2:38 PM

Client Name ▲	IP Address/Host Name	Device Type	Description	Actions
No data to display				

4. Enter a descriptive name and IP address for the client device. In this case, **192.168.113.100** is the address of the Windows server running the Milestone XProtect application on bus #1.

Figure 45. SEA – Add Connected Client



Add Connected Client

Selection Method
Manual entry

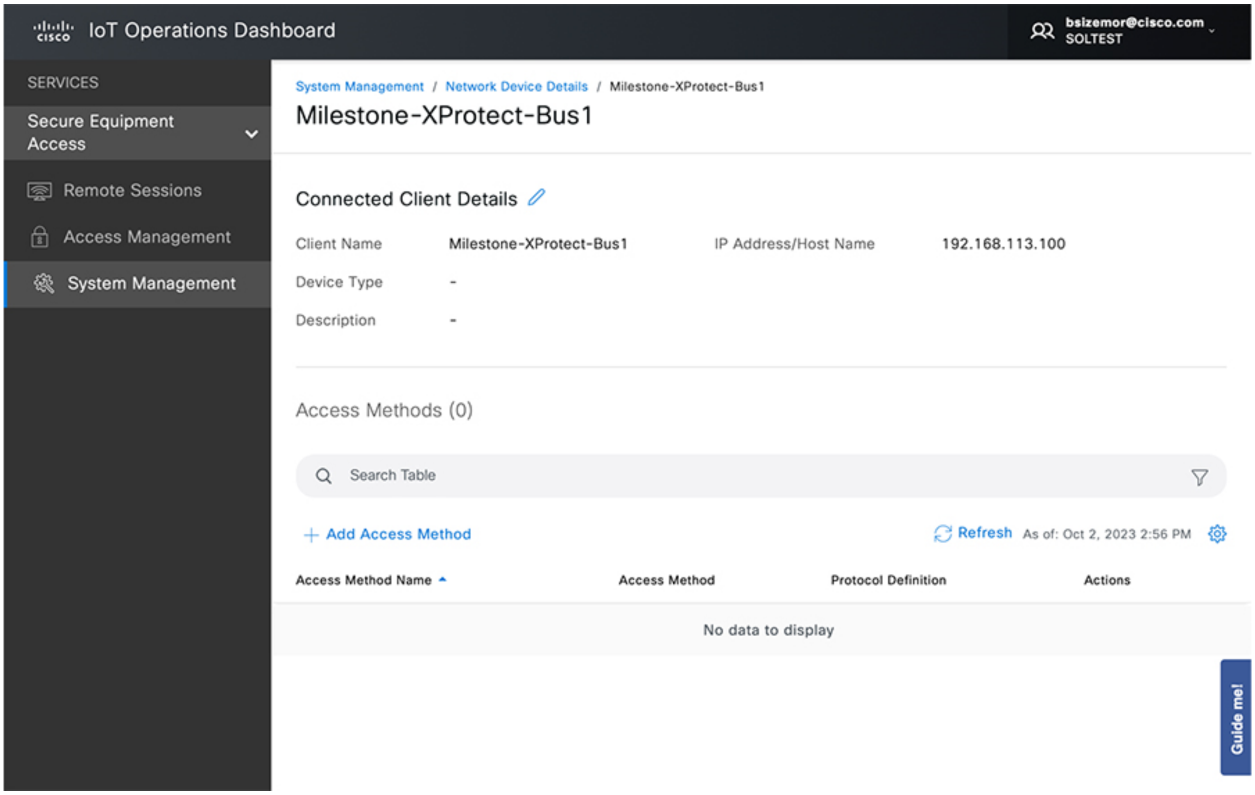
Enter the following information to enable Secure Equipment Access to the Connected Clients

Client Name*
Milestone-XProtect-Bus1

IP Address/Host Name*
192.168.113.100

5. After the connected client is added, one or more access methods can be added to connect to the client device. Click **Add Access Method**.

Figure 46. SEA – Connected Client Details



Milestone-XProtect-Bus1

Connected Client Details

Client Name	Milestone-XProtect-Bus1	IP Address/Host Name	192.168.113.100
Device Type	-		
Description	-		

Access Methods (0)

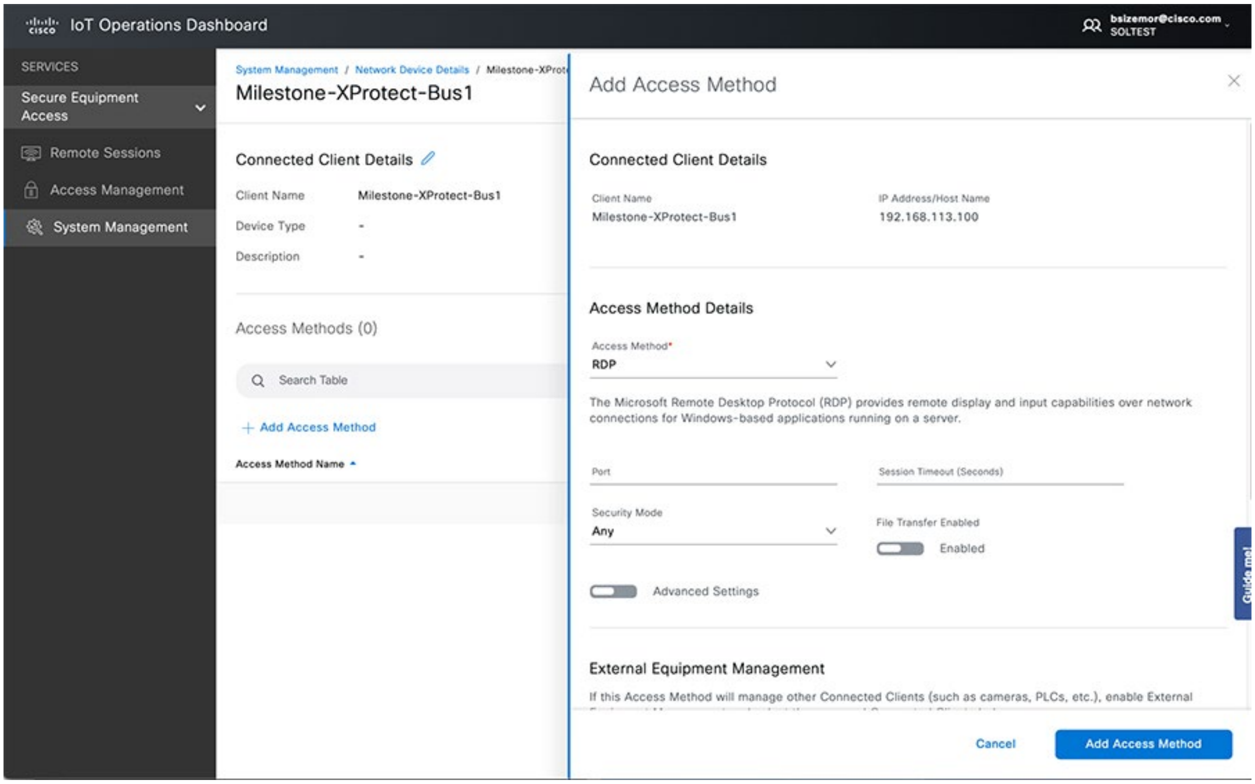
As of: Oct 2, 2023 2:56 PM

Access Method Name	Access Method	Protocol Definition	Actions

No data to display

6. In this example, the Windows server is accessed using Remote Desktop Protocol (RDP). For other types of devices, access methods like SSH or HTTPS, or even product specific native protocols could be configured here.

Figure 47. SEA – Add Access Method



Milestone-XProtect-Bus1

Connected Client Details

Client Name Milestone-XProtect-Bus1

Device Type -

Description -

Access Methods (0)

Add Access Method

Connected Client Details

Client Name: Milestone-XProtect-Bus1

IP Address/Host Name: 192.168.113.100

Access Method Details

Access Method*: RDP

The Microsoft Remote Desktop Protocol (RDP) provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Port

Session Timeout (Seconds)

Security Mode: Any

File Transfer Enabled: Enabled

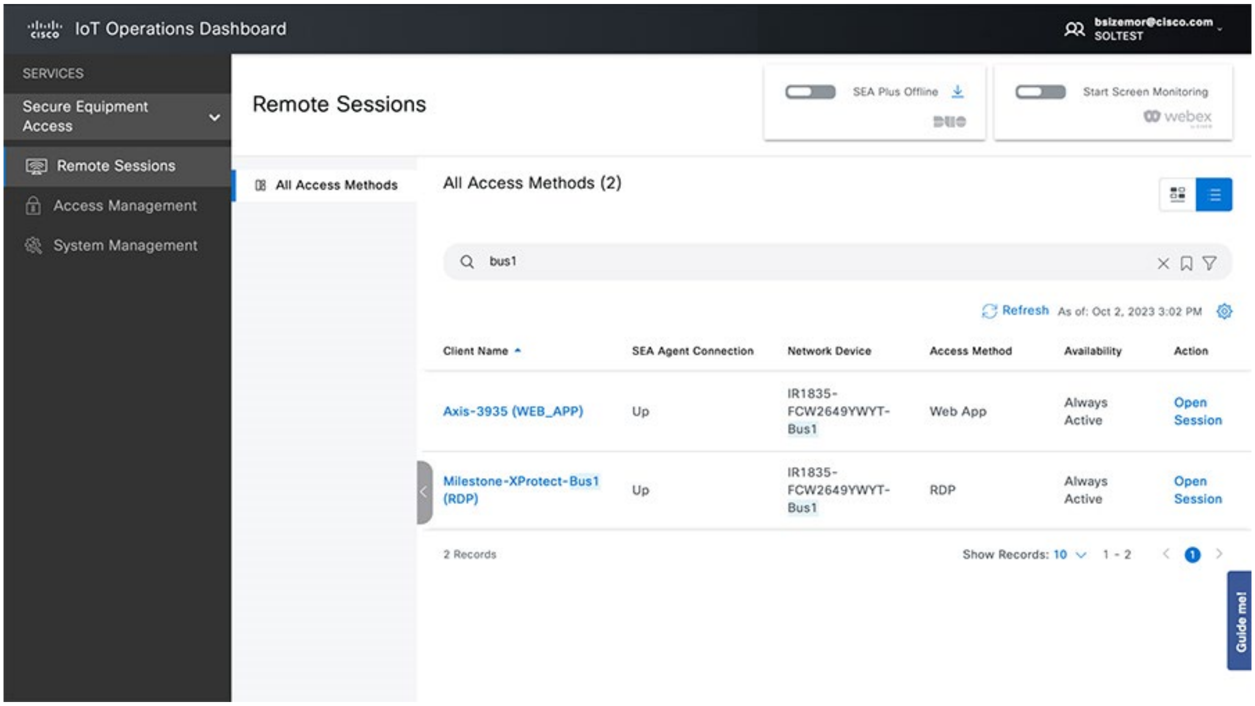
Advanced Settings

External Equipment Management

If this Access Method will manage other Connected Clients (such as cameras, PLCs, etc.), enable External

7. Click **Remote Sessions.** All the available access methods for all connected client devices are displayed. Use the search box to narrow down the list of items you want to view. In this example, the IR1835 on Bus1 is configured to access the Milestone Windows server with RDP and an AXIS video camera with HTTPS.

Figure 48. SEA – Remote Sessions



Remote Sessions

All Access Methods (2)

bus1

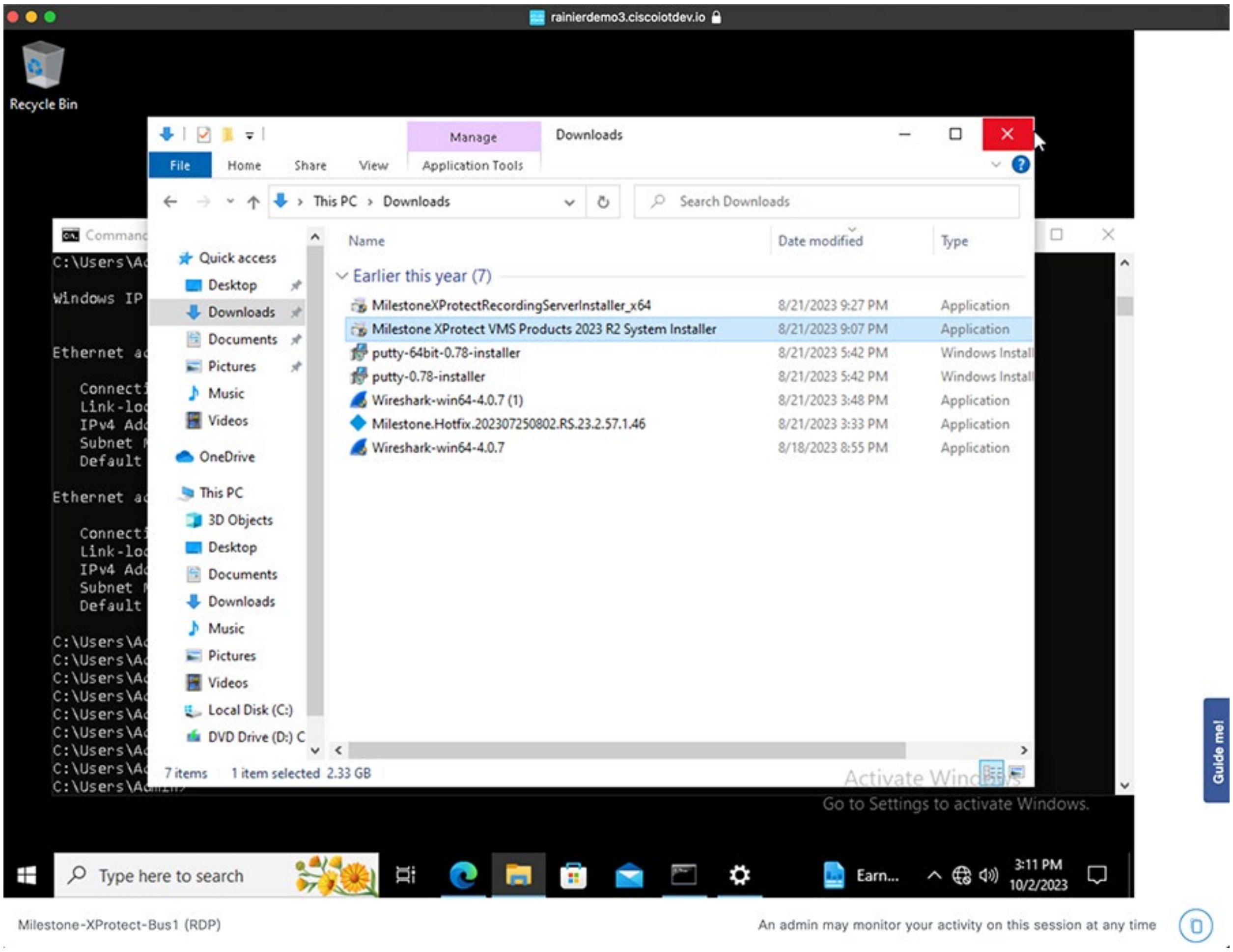
Refresh As of: Oct 2, 2023 3:02 PM

Client Name	SEA Agent Connection	Network Device	Access Method	Availability	Action
Axis-3935 (WEB_APP)	Up	IR1835-FCW2649YWYT-Bus1	Web App	Always Active	Open Session
Milestone-XProtect-Bus1 (RDP)	Up	IR1835-FCW2649YWYT-Bus1	RDP	Always Active	Open Session

2 Records   Show Records: 10   1 - 2   1

8. Clicking **Open Session** for the RDP remote session opens up a new window in the browser with an RDP session to the Windows server. Other access methods (except for SEA Plus) have a similar experience. SEA Plus enables the use of other applications on the local user's computer to connect to remote devices.

Figure 49. SEA – Remote Desktop Session



```
C:\Users\A

Windows IP


Ethernet a

   Connect
   Link-lo
   IPv4 Ad
   Subnet
   Default

Ethernet a

   Connect
   Link-lo
   IPv4 Ad
   Subnet
   Default

C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\A
C:\Users\Admin>
```

Earlier this year (7)

Name	Date modified	Type
MilestoneXProtectRecordingServerInstaller_x64	8/21/2023 9:27 PM	Application
Milestone XProtect VMS Products 2023 R2 System Installer	8/21/2023 9:07 PM	Application
putty-64bit-0.78-installer	8/21/2023 5:42 PM	Windows Install
putty-0.78-installer	8/21/2023 5:42 PM	Windows Install
Wireshark-win64-4.0.7 (1)	8/21/2023 3:48 PM	Application
Milestone.Hotfix.202307250802.RS.23.2.57.1.46	8/21/2023 3:33 PM	Application
Wireshark-win64-4.0.7	8/18/2023 8:55 PM	Application

7 items 1 item selected 2.33 GB

Milestone-XProtect-Bus1 (RDP)

An admin may monitor your activity on this session at any time

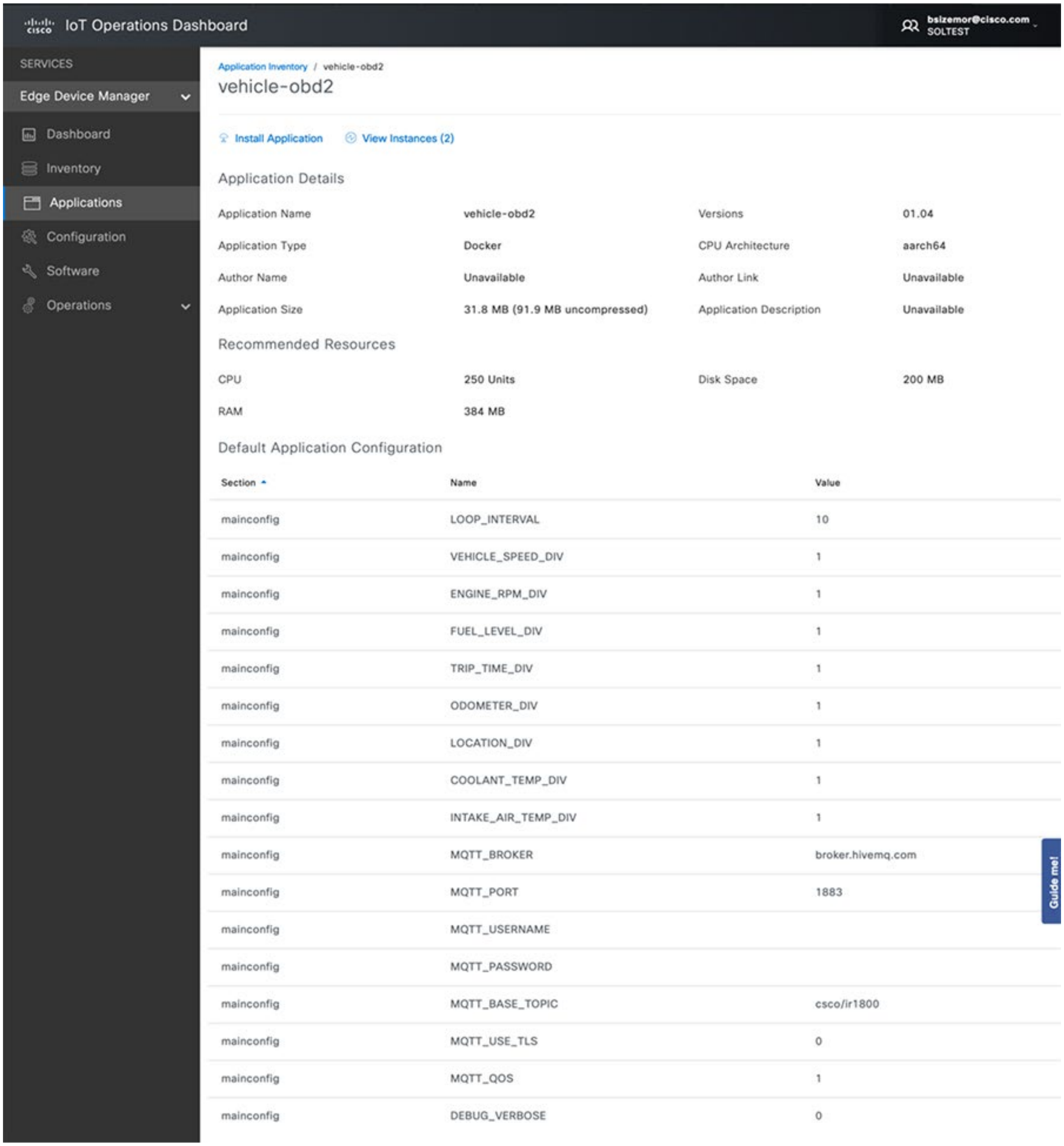
IOx Applications

Example Vehicle CANBUS Data Application

This section shows an example IOx application written by Cisco to demonstrate some of the capabilities of the IR1800 router in conjunction with IOx edge computing. The application is available in Github, but is not supported by Cisco: https://github.com/keholcom/vehicle-obd2

The app is installed and managed through IoT Operations Dashboard. After installed and configured, it pulls data from the IR1800 GPS receiver (on Cellular 0/4/0 in this case) and polls the CANBUS for vehicle information. The type of information available on the CANBUS is vehicle dependent. On the test vehicle (2017 Chevrolet Silverado), the following metrics were available: speed, engine RPM, fuel level, trip time, coolant temperature, and intake air temperature.

Figure 50. IOx Application "vehicle-obd2" Details in IOT OD



vehicle-obd2

Application Details

Application Name	vehicle-obd2	Versions	01.04
Application Type	Docker	CPU Architecture	aarch64
Author Name	Unavailable	Author Link	Unavailable
Application Size	31.8 MB (91.9 MB uncompressed)	Application Description	Unavailable

Recommended Resources

CPU	250 Units	Disk Space	200 MB
RAM	384 MB		

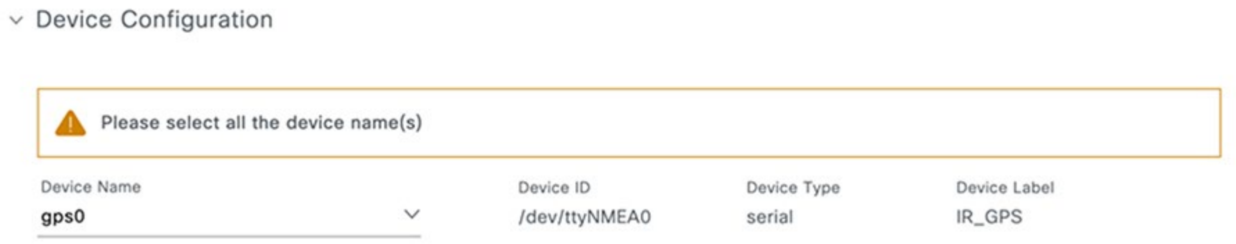
Default Application Configuration

Section ▴	Name	Value
mainconfig	LOOP_INTERVAL	10
mainconfig	VEHICLE_SPEED_DIV	1
mainconfig	ENGINE_RPM_DIV	1
mainconfig	FUEL_LEVEL_DIV	1
mainconfig	TRIP_TIME_DIV	1
mainconfig	ODOMETER_DIV	1
mainconfig	LOCATION_DIV	1
mainconfig	COOLANT_TEMP_DIV	1
mainconfig	INTAKE_AIR_TEMP_DIV	1
mainconfig	MQTT_BROKER	broker.hivemq.com
mainconfig	MQTT_PORT	1883
mainconfig	MQTT_USERNAME	
mainconfig	MQTT_PASSWORD	
mainconfig	MQTT_BASE_TOPIC	csco/ir1800
mainconfig	MQTT_USE_TLS	0
mainconfig	MQTT_QOS	1
mainconfig	DEBUG_VERBOSE	0

In the screenshot above, the application configuration details are visible. This is where the application is set to point to an external MQTT broker which will receive the formatted vehicle telemetry messages.

The Device Configuration section is used to bind the **gps0** data source to the application. In this case, **gps0** refers to the GPS receiver on the first cellular modem (interface Cellular 0/4/0).

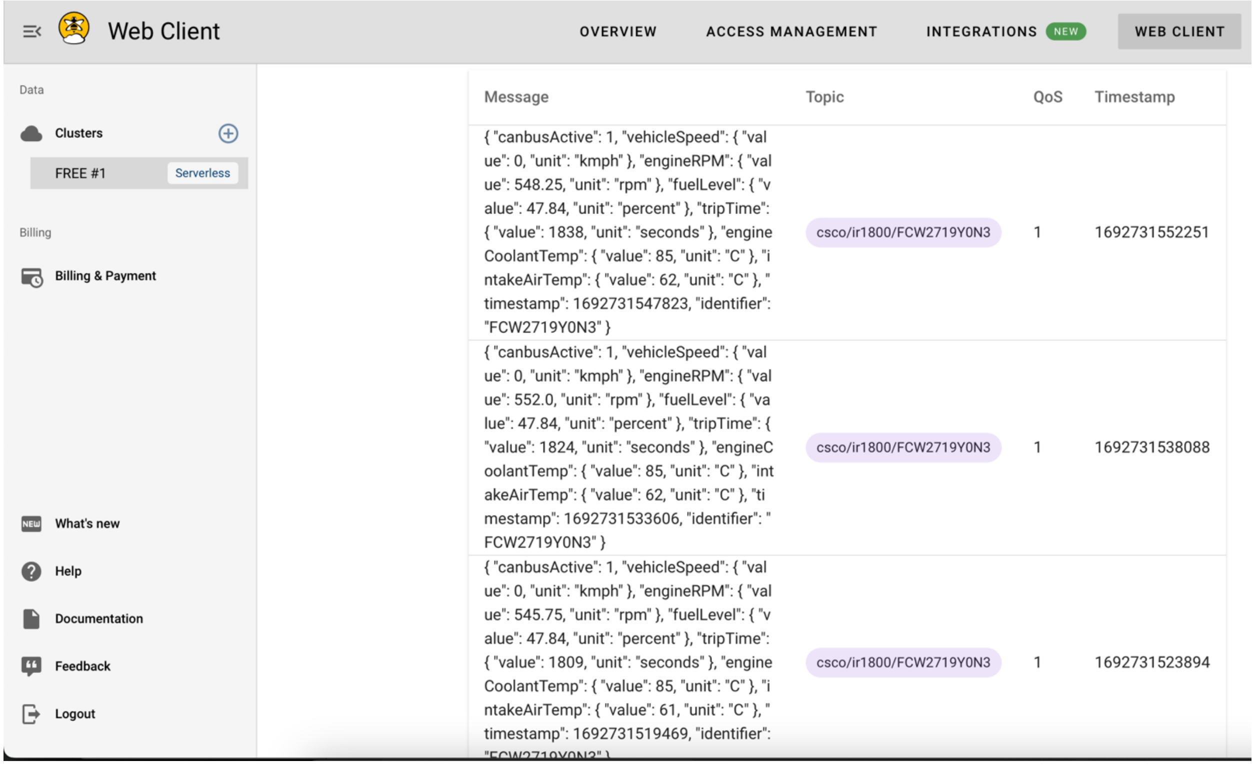
Figure 51. IOX Application "vehicle-obd2" Device Configuration



Device Name	Device ID	Device Type	Device Label
gps0	/dev/ttyNMEA0	serial	IR_GPS

The MQTT broker receives the formatted vehicle telemetry messages from the IOx application. Subsequently, the data is written into a database for historical records and summarized in a dashboard view using Grafana. The dashboard shows a map of the historical geo-location of the vehicle, vehicle speed, engine RPM, altitude, and coolant temperature.

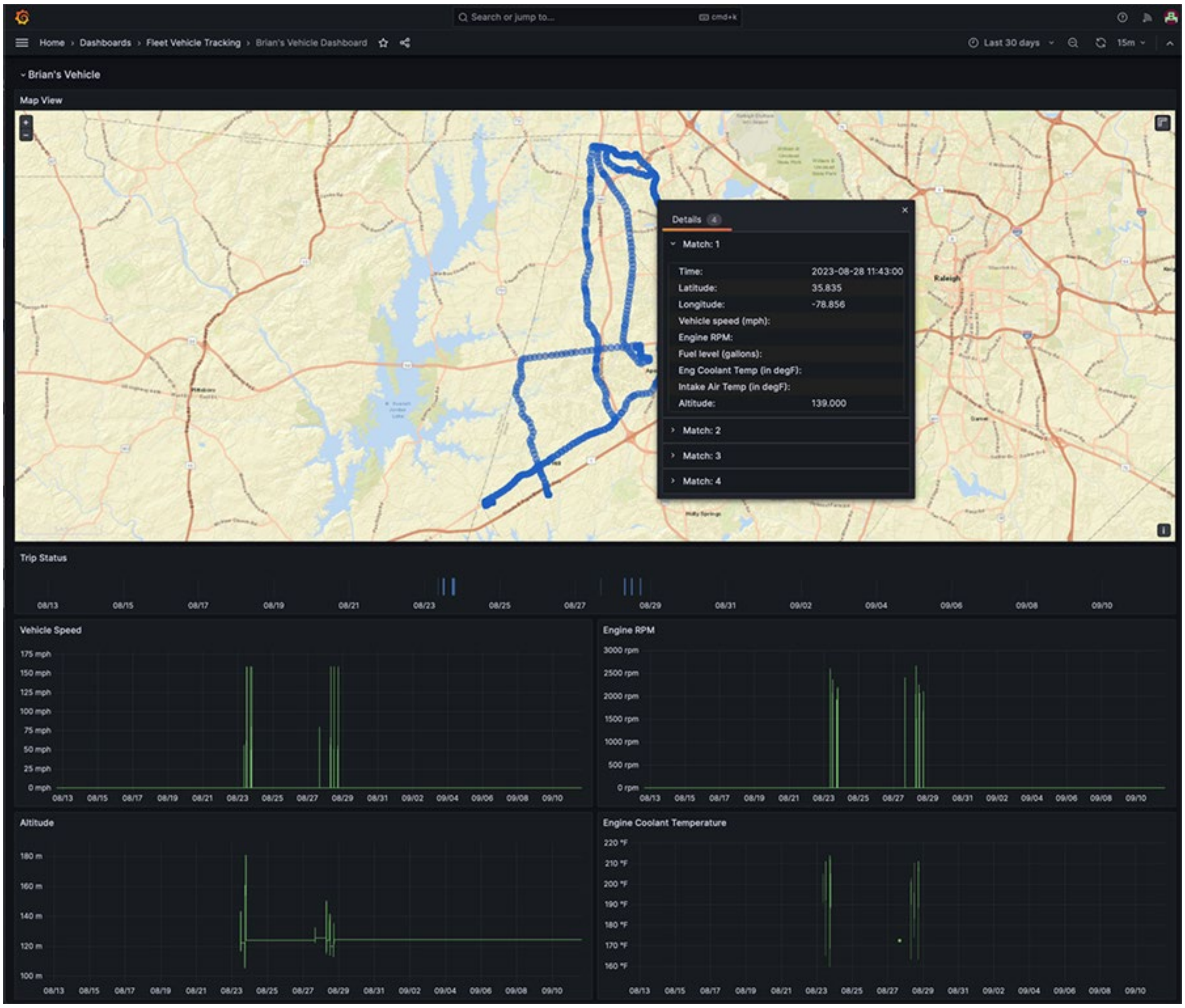
Figure 52. IOx Application "vehicle-obd2" MQTT Messages



Message	Topic	QoS	Timestamp
{ "canbusActive": 1, "vehicleSpeed": { "value": 0, "unit": "kmph" }, "engineRPM": { "value": 548.25, "unit": "rpm" }, "fuelLevel": { "value": 47.84, "unit": "percent" }, "tripTime": { "value": 1838, "unit": "seconds" }, "engineCoolantTemp": { "value": 85, "unit": "C" }, "intakeAirTemp": { "value": 62, "unit": "C" }, "timestamp": 1692731547823, "identifier": "FCW2719Y0N3" }	csco/ir1800/FCW2719Y0N3	1	1692731552251
{ "canbusActive": 1, "vehicleSpeed": { "value": 0, "unit": "kmph" }, "engineRPM": { "value": 552.0, "unit": "rpm" }, "fuelLevel": { "value": 47.84, "unit": "percent" }, "tripTime": { "value": 1824, "unit": "seconds" }, "engineCoolantTemp": { "value": 85, "unit": "C" }, "intakeAirTemp": { "value": 62, "unit": "C" }, "timestamp": 1692731533606, "identifier": "FCW2719Y0N3" }	csco/ir1800/FCW2719Y0N3	1	1692731538088
{ "canbusActive": 1, "vehicleSpeed": { "value": 0, "unit": "kmph" }, "engineRPM": { "value": 545.75, "unit": "rpm" }, "fuelLevel": { "value": 47.84, "unit": "percent" }, "tripTime": { "value": 1809, "unit": "seconds" }, "engineCoolantTemp": { "value": 85, "unit": "C" }, "intakeAirTemp": { "value": 61, "unit": "C" }, "timestamp": 1692731519469, "identifier": "FCW2719Y0N3" }	csco/ir1800/FCW2719Y0N3	1	1692731523894

The screenshots of the MQTT broker and dashboard are just for illustrative purposes, showing what is possible to do with data extracted using the IR1800 and IOX. This is not publicly available.

Figure 53. IOx Application "vehicle-obd2" Dashboard


Search or jump to...
cmd+k
Home › Dashboards › Fleet Vehicle Tracking › Brian's Vehicle Dashboard
Last 30 days
15m
Brian's Vehicle
Map View
Raleigh
Trip Status
08/13 08/15 08/17 08/19 08/21 08/23 08/25 08/27 08/29 08/31 09/02 09/04 09/06 09/08 09/10
Vehicle Speed
175 mph 150 mph 125 mph 100 mph 75 mph 50 mph 25 mph 0 mph
Engine RPM
3000 rpm 2500 rpm 2000 rpm 1500 rpm 1000 rpm 500 rpm 0 rpm
Altitude
180 m 160 m 140 m 120 m 100 m
Engine Coolant Temperature
220 °F 210 °F 200 °F 190 °F 180 °F 170 °F 160 °F

Details 4

Match: 1

Time: 2023-08-28 11:43:00
Latitude: 35.835
Longitude: -78.856
Vehicle speed (mph):
Engine RPM:
Fuel level (gallons):
Eng Coolant Temp (in degF):
Intake Air Temp (in degF):
Altitude: 139.000

Match: 2

Match: 3

Match: 4

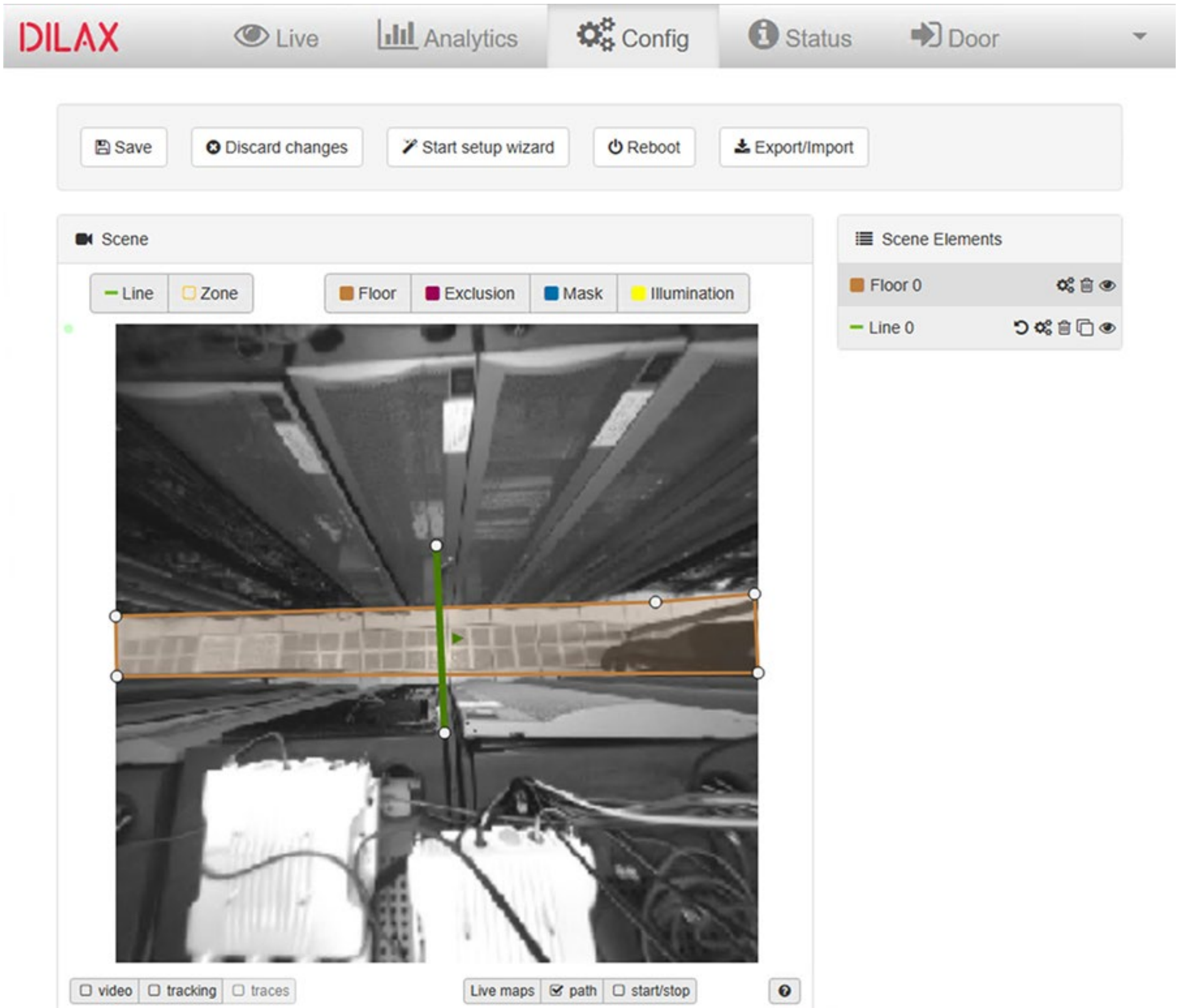
Bus Services

A mass transit bus will typically have a variety of services provided by different vendors. These services include automatic passenger counting, emissions monitoring, video surveillance, and voice communications. The subsections that follow illustrate what these systems can look like for a bus deployment and are not meant to document how to configure or operate these services. Please refer to the vendor documentation for more information.

Automatic Passenger Counting with DILAX

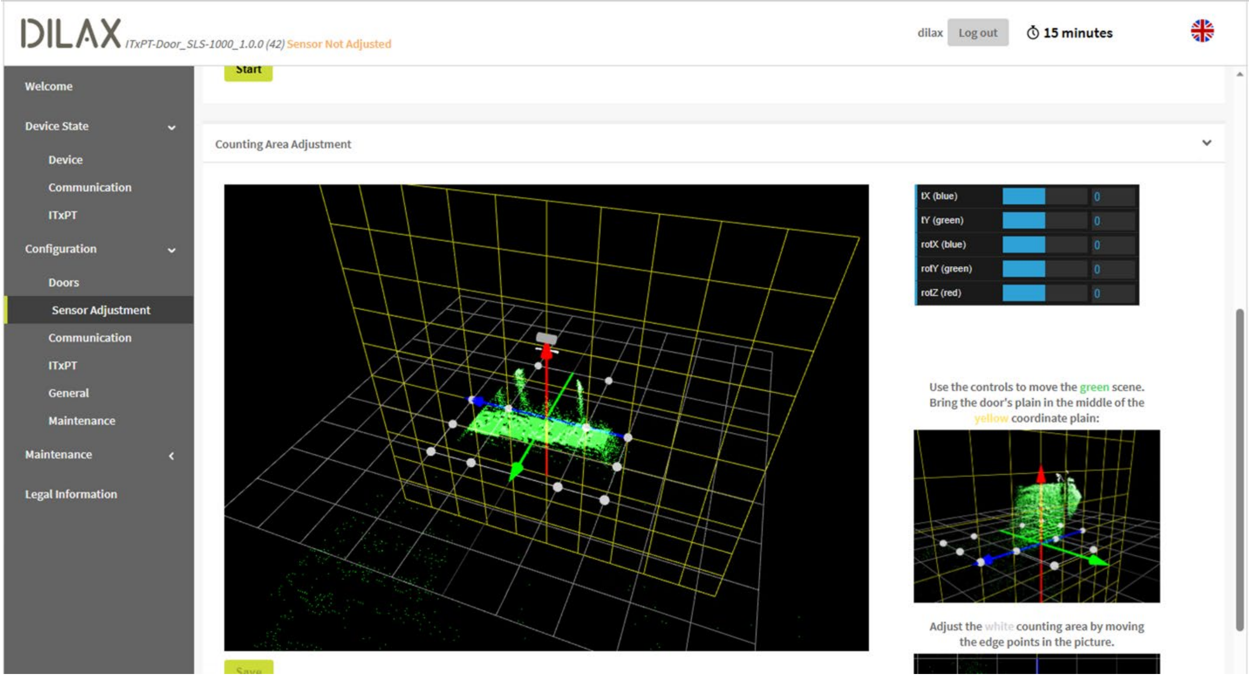
DILAX provides the automatic passenger counting functionality as validated in the Cisco IoT solutions lab. The PRT-400 sensor is mounted above the equipment racks in the lab and calibrated for the actual height above the floor. An orange box was drawn to identify the floor as a zone. A green line was also drawn across the floor in the PRT-400 interface to simulate a doorway on a transit vehicle. The arrow on the green line identifies the exit direction. Each time a person walked from left to right in the photo, across the green line, the PRT-400 counted the movement as an exit. When a person walked from right to left across the green line, the sensor counted it as an entrance.

Figure 54. DILAX PRT-400 passenger counter view of "doorway" and floor



The DILAX SLS-1000 was then similarly setup in the lab and used stereoscopic vision to monitor the scene, identifying entrances and exits.

Figure 55. DILAX SLS-1000 passenger counter sensor 3D view



tX (blue) 0
tY (green) 0
rotX (blue) 0
rotY (green) 0
rotZ (red) 0

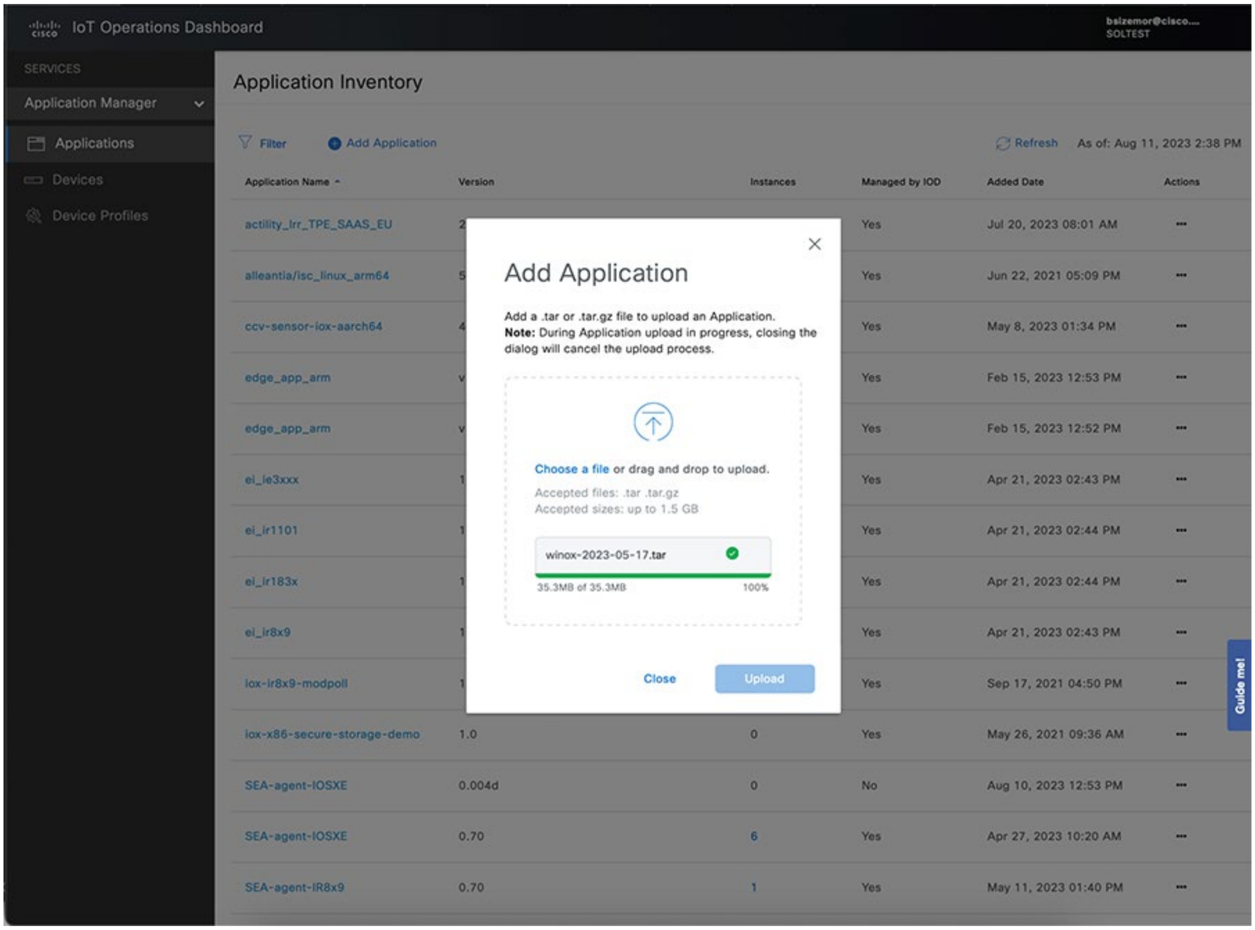
Use the controls to move the green scene. Bring the door's plain in the middle of the yellow coordinate plain:

Adjust the white counting area by moving the edge points in the picture.

Emissions Monitoring with SensorComm Wi-NOx

SensorComm provides the Wi-NOx emissions monitoring system as validated for this Converged Public Transport solution. The Wi-NOx system comprises a sensor mounted in the exhaust pipe of the vehicle, and a readout electronics and interface board to convert the sensor signal into a serial data stream. The serial data is input into the IR1835 RS232 serial port which is mapped to an IOx app developed by SensorComm. The IOx app was installed using IoT OD App Management capability as shown in the figure that follows.

Figure 56. SensorComm Wi-NOx emissions monitoring IOX app upload with IoT OD



Application Inventory

As of: Aug 11, 2023 2:38 PM

Application Name	Version	Instances	Managed by IOD	Added Date	Actions
actility_lrr_TPE_SAAS_EU	2		Yes	Jul 20, 2023 08:01 AM	•••
alleantia/isc_linux_arm64	5		Yes	Jun 22, 2021 05:09 PM	•••
ccv-sensor-iox-aarch64	4		Yes	May 8, 2023 01:34 PM	•••
edge_app_arm	v		Yes	Feb 15, 2023 12:53 PM	•••
edge_app_arm	v		Yes	Feb 15, 2023 12:52 PM	•••
ei_ie3xxx	1		Yes	Apr 21, 2023 02:43 PM	•••
ei_ir1101	1		Yes	Apr 21, 2023 02:44 PM	•••
ei_ir183x	1		Yes	Apr 21, 2023 02:44 PM	•••
ei_ir8x9	1		Yes	Apr 21, 2023 02:43 PM	•••
iox-ir8x9-modpoll	1		Yes	Sep 17, 2021 04:50 PM	•••
iox-x86-secure-storage-demo	1.0	0	Yes	May 26, 2021 09:36 AM	•••
SEA-agent-IOSXE	0.004d	0	No	Aug 10, 2023 12:53 PM	•••
SEA-agent-IOSXE	0.70	6	Yes	Apr 27, 2023 10:20 AM	•••
SEA-agent-IR8x9	0.70	1	Yes	May 11, 2023 01:40 PM	•••

Add Application

Add a .tar or .tar.gz file to upload an Application.
Note: During Application upload in progress, closing the dialog will cancel the upload process.

Choose a file or drag and drop to upload.

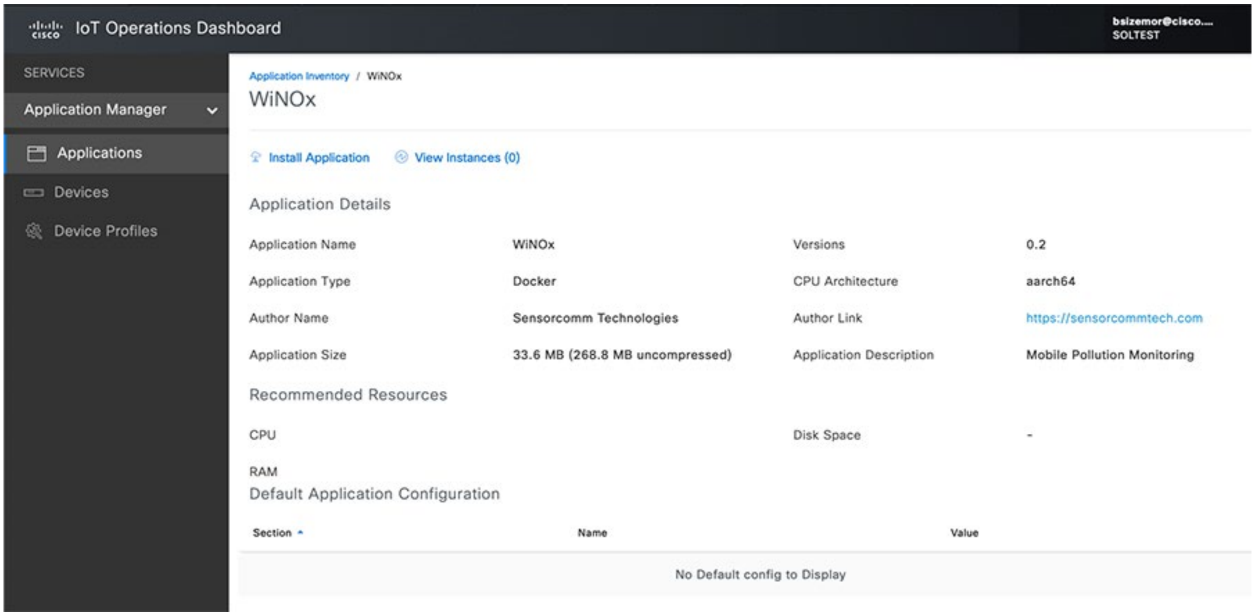
Accepted files: .tar .tar.gz
Accepted sizes: up to 1.5 GB

winox-2023-05-17.tar

35.3MB of 35.3MB 100%

After the app is uploaded to IoT OD App Manager service, it can be installed to the IR1800.

Figure 57. SensorComm Wi-NOx emissions monitoring IOX app installed on an IR1800



WiNOx

Application Details

Application Name	WiNOx	Versions	0.2
Application Type	Docker	CPU Architecture	aarch64
Author Name	Sensorcomm Technologies	Author Link	https://sensorcommtech.com
Application Size	33.6 MB (268.8 MB uncompressed)	Application Description	Mobile Pollution Monitoring

Recommended Resources

CPU		Disk Space	-
RAM			

Default Application Configuration

Section	Name	Value
No Default config to Display		

To get the Wi-NOx serial data into IOX, some simple router configuration is required. This can be added to the IoT OD eCVD template Extended Form section for CLI.

```
interface Async0/2/0
 no ip address
 encapsulation relay-line
line 0/2/0
 speed 115200
relay line 0/2/0 0/0/0
```

After configuration, the serial data from the Wi-NOx interface board is received by the IR1800 and relayed to the IOX app. The text below shows an example of the raw serial data coming from Wi-NOx.

```
[IR1800_FCW2649YWYT_RP_0:/]$ cat /dev/ttySerial
8183a6af8|18f00f52|8|c00fb0f1541f1f1f
8183a6b2a|18f00f52|8|c00fb0f1541f1f1f
8183a6b5c|18f00f52|8|c00fb0f1541f1f1f
8183a6b8e|18f00f52|8|c00fb0f1541f1f1f
8183a6bc0|18f00f52|8|c00fb0f1541f1f1f
8183a6bf2|18f00f52|8|c00fb0f1541f1f1f
8183a6c24|18f00f52|8|c00fb0f1541f1f1f
8183a6c56|18f00f52|8|c00fb0f1541f1f1f
8183a6c88|18f00f52|8|c00fb0f1541f1f1f
DEWPOINT
8183a6cba|18f00f52|8|c00fb0f1541f1f1f
8183a6cec|18f00f52|8|c00fb0f1541f1f1f
8183a6d1e|18f00f52|8|c00fb0f1541f1f1f
```

```
8183a6d50|18f00f52|8|c00fb0f1541f1f1f
8183a6d82|18f00f52|8|c80fb0f1541f1f1f
```

The Docker logs from the IOX app show how the serial data has been received and decoded into a format that can then be sent over IP to a dashboard, database, or other application in the cloud.

```
2023-08-14T20:44:44.226269992Z ENV
2023-08-14T20:44:44.226358993Z ENV
2023-08-14T20:44:44.226378994Z Starting gps serial
2023-08-14T20:44:44.226397394Z gps serial init ok
2023-08-14T20:44:44.226415195Z starting cisco serial
2023-08-14T20:44:44.226433195Z cisco serial init ok
2023-08-14T20:44:44.226451155Z 0 10000 : -1 10000 : -1
2023-08-14T20:44:44.226468636Z new  0   delete  10000
2023-08-14T20:44:44.226486036Z /media/pi/WiNOx/DATAA/WN0000
/media/pi/WiNOx/DATAA/
2023-08-14T20:44:44.226503636Z 0 10000 : -1 10000 : -1
2023-08-14T20:44:44.226520797Z new  0   delete  10000
2023-08-14T20:44:44.226537877Z /media/pi/WiNOx/DATAB/WN0000
/media/pi/WiNOx/DATAB/
2023-08-14T20:44:44.226555158Z init() finished
2023-08-16T12:48:29.486583075Z sh: ./ntpdate: not found
2023-08-16T12:50:16.462774847Z arduino received from tornado: first task
2023-08-16T12:50:16.462880890Z 2023-08-
16T12:48:34.470883,,,,,,0.0,0.0,0.0,,,,,,,,
2023-08-16T12:50:16.462906930Z curl http://179.15.202.183:8888/upload/fst --
connect-timeout 12 --max-time 30 --silent -X POST  -d
"token=1&mac_device=FCW2649YWYT&ip_device=-1.-1.-1.-1&temp_gateway=-
273.15&payload=2023-08-16T12:48:28.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:29.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:30.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:31.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:32.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:33.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:34.470883,,,,,,0.0,0.0,0.0,,,,,,,,#" > /dev/null &
2023-08-16T12:50:16.462938571Z 2023-08-
16T12:48:44.470883,,,,,,0.0,0.0,0.0,,,,,,,,
2023-08-16T12:50:16.462960371Z curl http://179.15.202.183:8888/upload/fst --
connect-timeout 12 --max-time 30 --silent -X POST  -d
"token=1&mac_device=FCW2649YWYT&ip_device=-1.-1.-1.-1&temp_gateway=-
273.15&payload=2023-08-16T12:48:35.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:36.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:37.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:38.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:39.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:40.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:41.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:42.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:43.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:44.470883,,,,,,0.0,0.0,0.0,,,,,,,,#" > /dev/null &
2023-08-16T12:50:16.462988812Z 2023-08-
16T12:48:54.470883,,,,,,0.0,0.0,0.0,,,,,,,,
2023-08-16T12:50:16.463070974Z curl http://179.15.202.183:8888/upload/fst --
connect-timeout 12 --max-time 30 --silent -X POST  -d
"token=1&mac_device=FCW2649YWYT&ip_device=-1.-1.-1.-1&temp_gateway=-
273.15&payload=2023-08-16T12:48:45.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:46.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:47.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:48.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:49.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:50.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
```

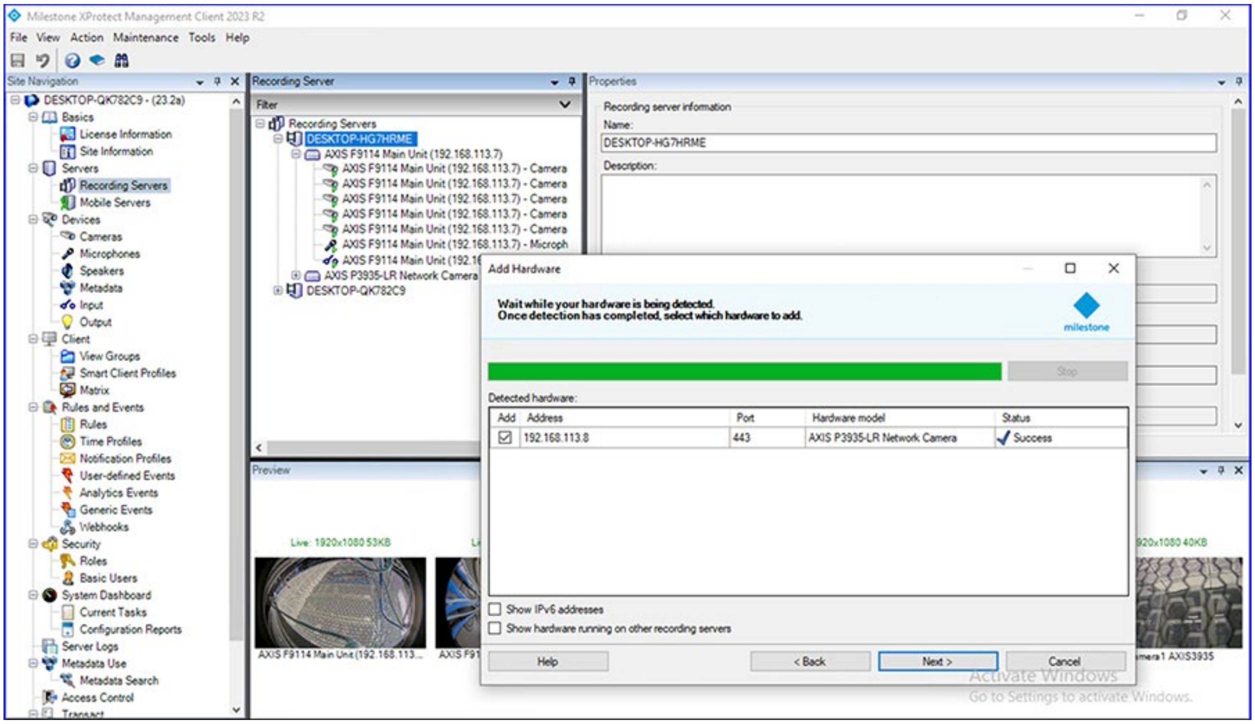
```
16T12:48:51.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:52.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:53.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:54.470883,,,,,,0.0,0.0,0.0,,,,,,,,#" > /dev/null &
2023-08-16T12:50:16.463100894Z 2023-08-
16T12:49:04.470883,,,,,,0.0,0.0,0.0,,,,,,,,
2023-08-16T12:50:16.463119775Z curl http://179.15.202.183:8888/upload/fst --
connect-timeout 12 --max-time 30 --silent -X POST  -d
"token=1&mac_device=FCW2649YWYT&ip_device=-1.-1.-1.-1&temp_gateway=-
273.15&payload=2023-08-16T12:48:55.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:56.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:57.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:58.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:48:59.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:00.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:01.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:02.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:03.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:04.470883,,,,,,0.0,0.0,0.0,,,,,,,,#" > /dev/null &
2023-08-16T12:50:16.463145055Z 2023-08-
16T12:49:14.470883,,,,,,0.0,0.0,0.0,,,,,,,,
2023-08-16T12:50:16.463163176Z curl http://179.15.202.183:8888/upload/fst --
connect-timeout 12 --max-time 30 --silent -X POST  -d
"token=1&mac_device=FCW2649YWYT&ip_device=-1.-1.-1.-1&temp_gateway=-
273.15&payload=2023-08-16T12:49:05.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:06.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:07.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:08.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:09.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:10.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:11.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:12.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:13.470883,,,,,,0.0,0.0,0.0,,,,,,,,#2023-08-
16T12:49:14.470883,,,,,,0.0,0.0,0.0,,,,,,,,#" > /dev/null &
2023-08-16T12:50:16.463187896Z 2023-08-
16T12:49:24.470883,,,,,,0.0,0.0,0.0,,,,,,,,
```

Video Surveillance with AXIS and Milestone

Video surveillance on the transit vehicle is provided by two vendors, AXIS and Milestone. AXIS provides a range of ruggedized video cameras that are suitable for installation on bus or similar vehicle – either inside or out. Milestone provides the X-Protect software suite that provides the camera management, recording, rules, events, and monitoring capability for the video coming off the bus cameras.

The AXIS cameras are connected to a PoE ethernet port, either on the IR1800 directly, or on the subtended IE3x00 switch. The cameras can be configured through a locally hosted GUI, but more typically a centralized solution like Milestone X-Protect provides a more scalable solution. Once the recording servers are installed in the bus (on ruggedized compute running Windows) and in the datacenter/SOC (also running Windows) – the cameras can be discovered automatically by scanning an IP subnet as shown in the figure that follows.

Figure 58. Milestone XProtect – Add Cameras



Milestone XProtect Management Client 2023 R2

Recording server information

Name: DESKTOP-HG7HRME

Description:

Add Hardware

Wait while your hardware is being detected.
Once detection has completed, select which hardware to add.

Detected hardware:

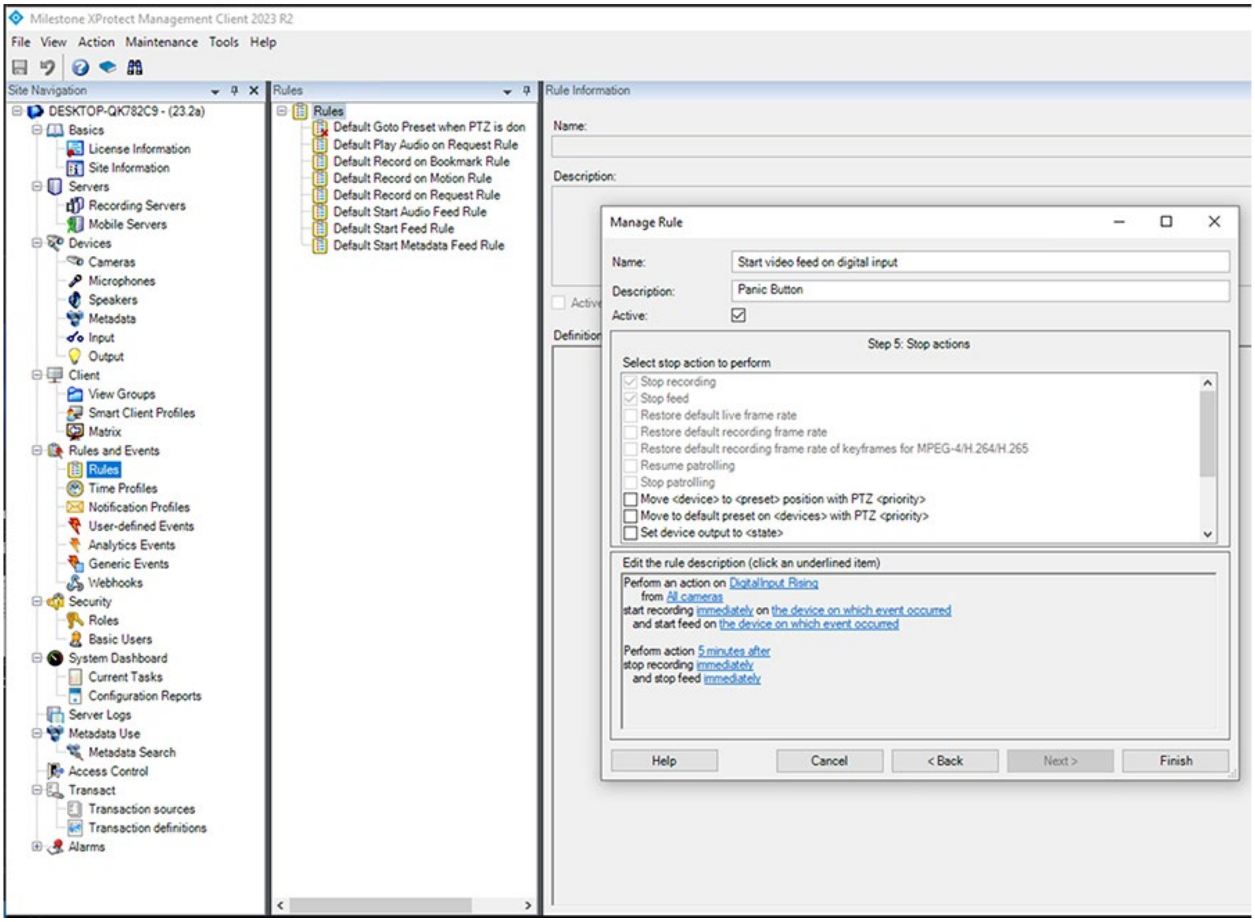
Add	Address	Port	Hardware model	Status
☑	192.168.113.8	443	AXIS P3935-LR Network Camera	✓ Success

□ Show IPv6 addresses

□ Show hardware running on other recording servers

After the cameras are configured to record to the recording server on the bus, rules can be configured to achieve the desired behavior. For example, a digital input on the AXIS camera can be connected to a panic button at the driver seat. When the panic button is pressed, the digital input causes the rule shown in the figure that follows to be activated and the camera to record video for 5 minutes. Alternatively, the digital input could be connected to a door open/close sensor.

Figure 59. Milestone XProtect – Rule for panic button with digital input



Manage Rule

Name: Start video feed on digital input

Description: Panic Button

Active: ☑

Step 5: Stop actions

Select stop action to perform

- ☑ Stop recording
- ☑ Stop feed
- ☐ Restore default live frame rate
- ☐ Restore default recording frame rate
- ☐ Restore default recording frame rate of keyframes for MPEG-4/H.264/H.265
- ☐ Resume patrolling
- ☐ Stop patrolling
- ☐ Move <device> to <preset> position with PTZ <priority>
- ☐ Move to default preset on <devices> with PTZ <priority>
- ☐ Set device output to <state>

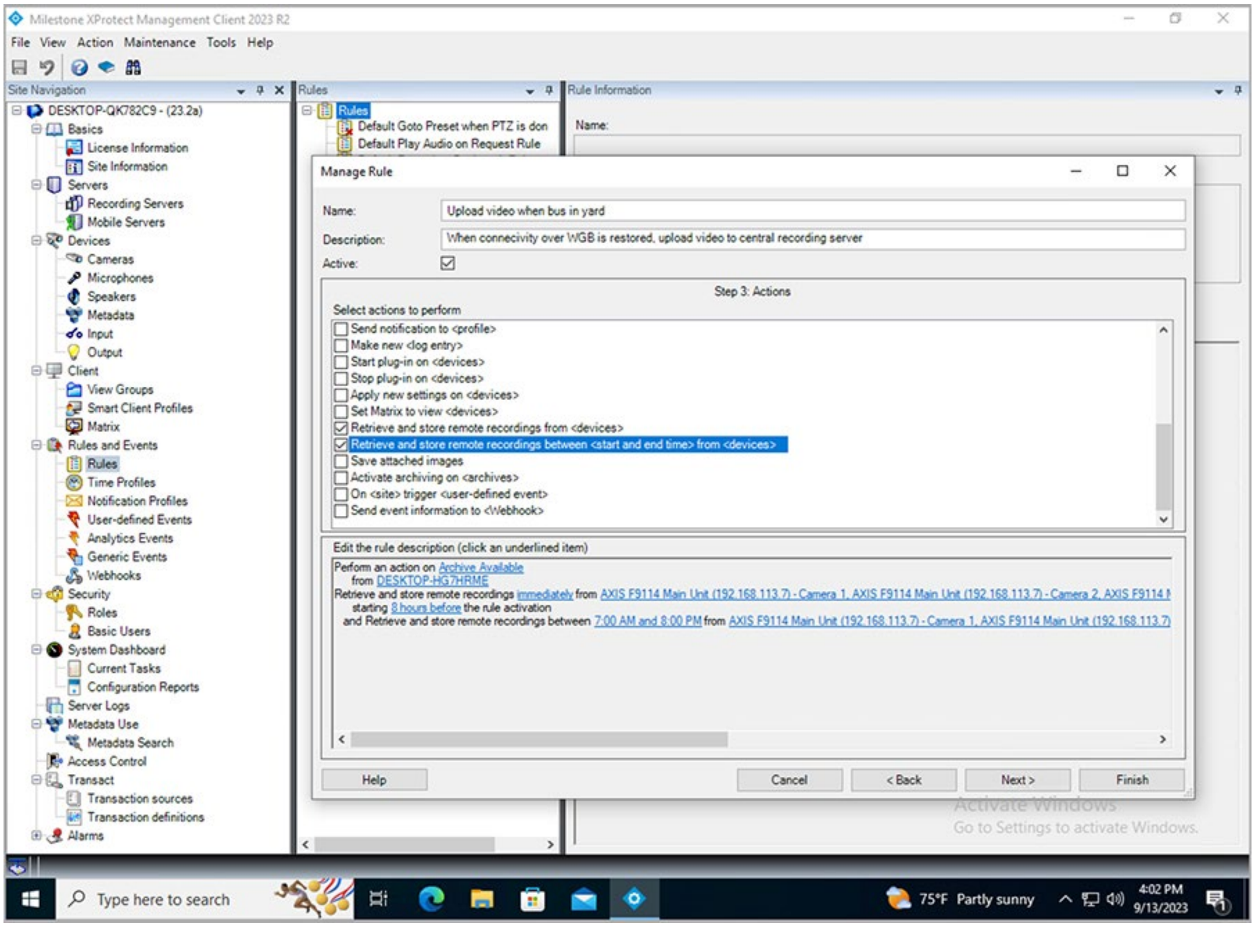
Edit the rule description (click an underlined item)

Perform an action on DigitalInput Rising
from All cameras
start recording immediately on the device on which event occured
and start feed on the device on which event occured

Perform action 5 minutes after
stop recording immediately
and stop feed immediately

An additional rule to monitor the availability of the recording server (or cameras) on the bus can be added. At the end of a shift, when the bus pulls into the yard and connectivity is restored over the WGB link, the rule could trigger and retrieve all recorded video for the day. Refer to the figure that follows.

Figure 60. Milestone XProtect – Rule for video recording upload after connectivity is restored



Manage Rule

Name: Upload video when bus in yard

Description: When connecivity over WGB is restored, upload video to central recording server

Active: ☑

Step 3: Actions

Select actions to perform

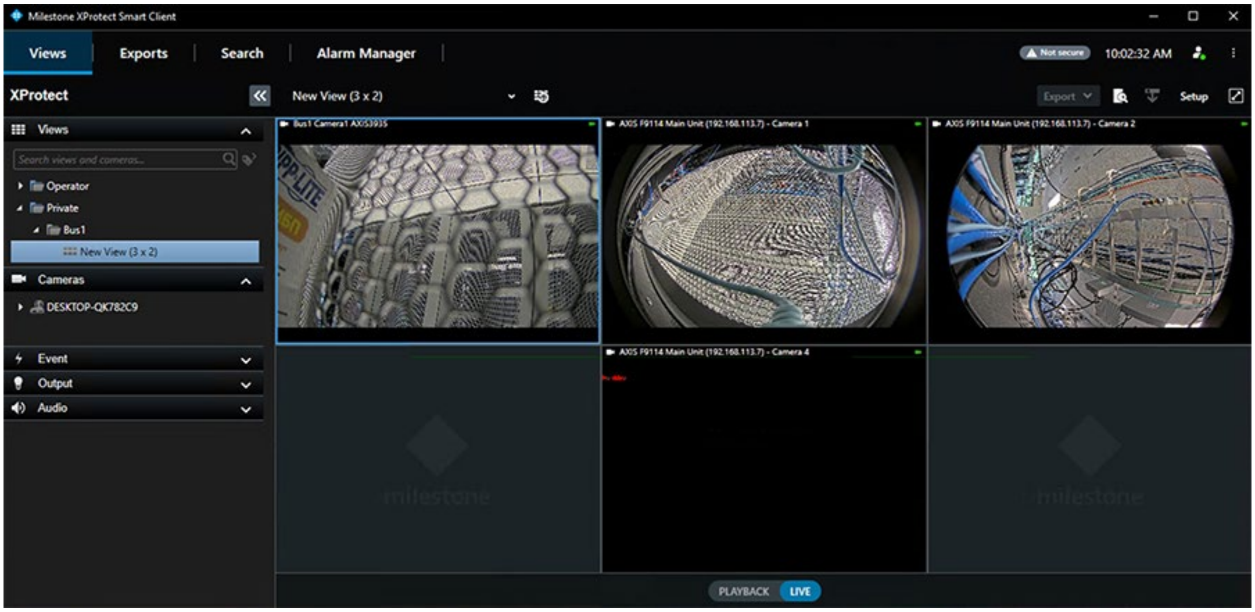
- ☐ Send notification to <profile>
- ☐ Make new <log entry>
- ☐ Start plug-in on <devices>
- ☐ Stop plug-in on <devices>
- ☐ Apply new settings on <devices>
- ☐ Set Matrix to view <devices>
- ☑ Retrieve and store remote recordings from <devices>
- ☑ Retrieve and store remote recordings between <start and end time> from <devices>
- ☐ Save attached images
- ☐ Activate archiving on <archives>
- ☐ On <site> trigger <user-defined event>
- ☐ Send event information to <Webhook>

Edit the rule description (click an underlined item)

```
Perform an action on Archive Available
   from DESKTOP-HG7HRME
Retrieve and store remote recordings immediately from AXIS F9114 Main Unit (192.168.113.7) - Camera 1, AXIS F9114 Main Unit (192.168.113.7) - Camera 2, AXIS F9114 M
   starting 8 hours before the rule activation
 and Retrieve and store remote recordings between 7:00 AM and 8:00 PM from AXIS F9114 Main Unit (192.168.113.7) - Camera 1, AXIS F9114 Main Unit (192.168.113.7)
```

The Milestone X-Protect Smart Client can also be used to monitor the video streams from all the managed cameras and recording servers. Refer to the figure that follows.

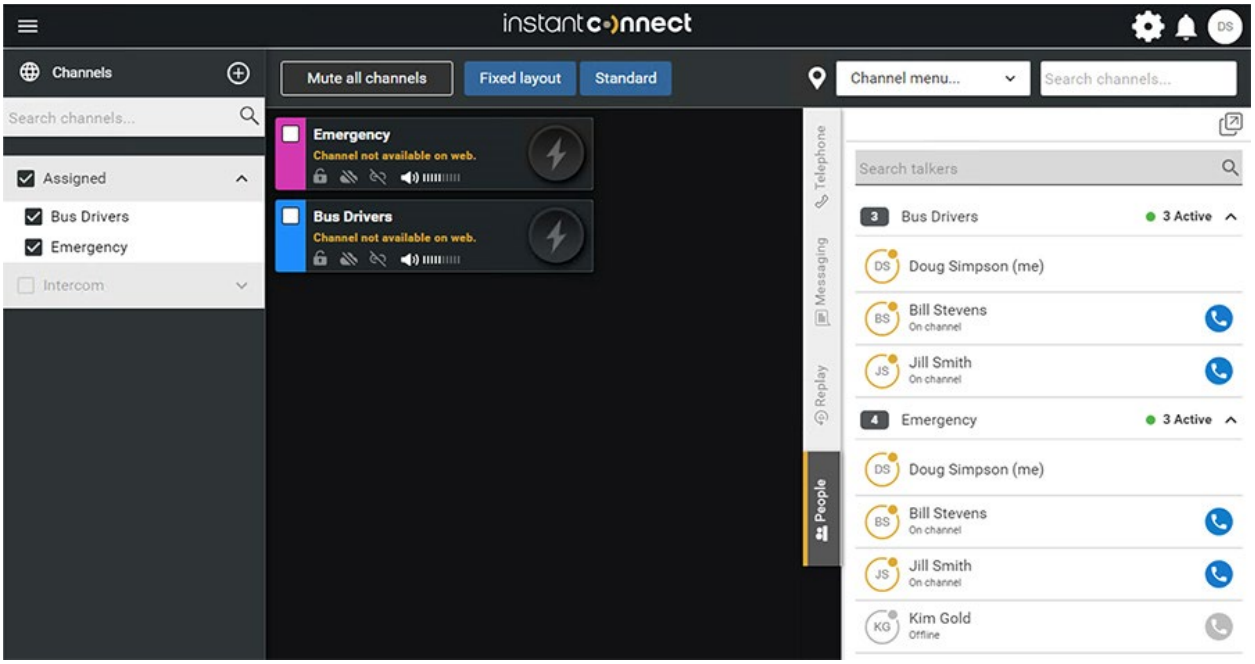
Figure 61. Milestone XProtect Smart Client



Voice Communication with InstantConnect

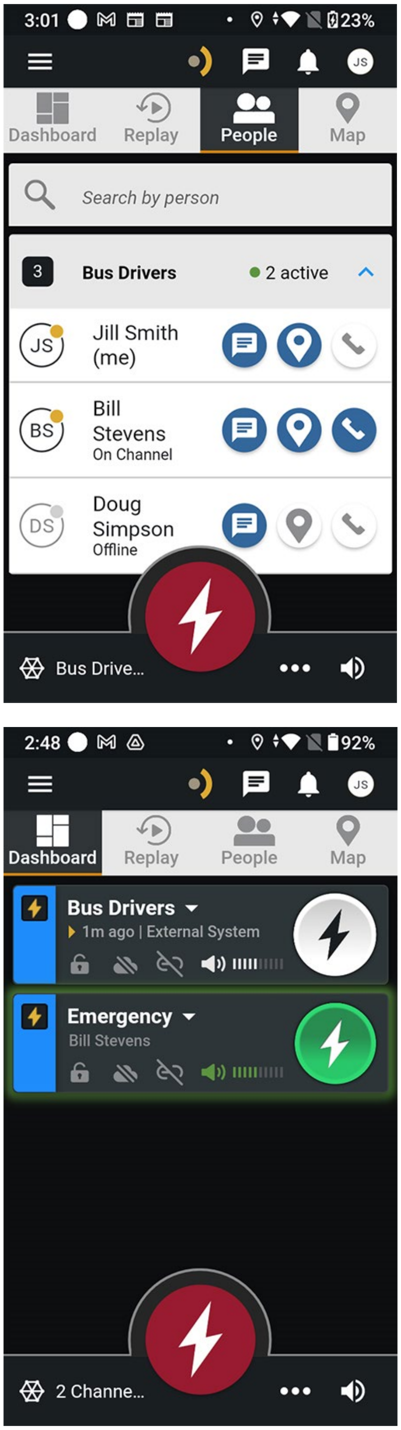
Voice communication between drivers, security personnel, and others can be implemented using the Instant Connect solution. This push-to-talk capability and advanced bridging of IP and LMR voice channels allows the agent at the central operations center to monitor multiple channels and speak on one or more channels simultaneously. The agent can use a desktop client as shown in the figure that follows.

Figure 62. Instant Connect desktop client



Drivers or other field personnel could similarly use a mobile client to participate in voice communications as well.

Figure 63. Instant Connect app on RugGear 750 Android phone



Additional Resources

Cisco References

IoT Operations Dashboard product documentation - https://developer.cisco.com/docs/iotod/

Cisco SD-WAN Configuration Guides - https://www.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration-guides-list.html

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.12.x - https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-12/config-guide/b_wl_17_12_cg.html

Cisco Identity Services Engine Configuration Guides - https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html

Cisco IOx product documentation - https://developer.cisco.com/docs/iox/

Third-party References

DILAX Automatic Passenger Counting - https://www.dilax.com/en/products/automatic-passenger-counting

AXIS Onboard Cameras - https://www.axis.com/en-us/products/onboard-cameras

SensorComm Technologies - https://www.sensorcommtech.com

Milestone XProtect - https://www.milestonesys.com/products/software/xprotect/

InstantConnect - https://www.instantconnectnow.com