Cisco IoT Device Manager Installation and User Guide, Release 5.x

First Published: 2015-11-18

Last Modified: 2020-07-10

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

CHAPTER 3

CHAPTER 4

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

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

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

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

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

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

CHAPTER 1

Overview of Cisco IoT Device Manager

This chapter provides an overview of the Cisco IoT Device Manager (Device Manager or IoT-DM) for Cisco 1000 Series Connected Grid Routers (CGR 1000 or router) running Cisco IOS, Cisco 809 Industrial Integrated Services Routers (IR800), and Cisco 500 Series WPAN Industrial Routers (IR500).

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note You must uninstall any instance of CG-DM 4.x or earlier, before you install IoT-DM on your laptop. The installer will not recognize the older installation given that the product name has changed from Cisco Connected Grid Device Manager (CG-DM) to Cisco IoT Device Manager (IoT-DM). As IoT-DM does not support CGR 1000 routers running CG-OS, do not uninstall CG-DM if you still need to manage CGR 1000 routers running CG-OS.

Application

Device Manager is a Windows-based application that field technicians can use to manage the CGR 1000 running Cisco IOS over WiFi or Ethernet. Beginning with Release 4.1, Device Manager supports management of the IR509, which supplies RF mesh connectivity to IPv4 and serial Internet of Things (IoT) devices (for example, recloser controls, capacitor bank controls, voltage regulator controls, and other remote terminal units). From Release 5.1, Device Manager supports management of the Cisco 800 Series Industria Integrated Services Routers (IR800) and IR510.

Cisco IoT Field Network Director (Cisco IoT-FND) manages multiple CGR 1000, IR800, and IR500 devices, whereas Device Manager connects and manages a single device at a time.

- Device Manager can manage CGR 1000 routers in Connected Grid field deployments operating with or without IoT-FND:
  - When operating with IoT-FND, a Device Manager user can retrieve work orders from the system as well as perform all supported tasks on the main page (see Figure 2: Device Manager Common Page Elements and Controls (CGR 1000), on page 4) except as limited by the privilege level that the administrator configures on the router for that user.
  - When operating without IoT-FND, the Device Manager user does not have access to work orders; however, the user can perform all supported tasks on the main page except as limited by the user’s privilege level.
- Device Manager can manage IR800 routers in Connected Grid field deployments operating with or without IoT-FND:
  - When operating with IoT-FND, a Device Manager user can retrieve work orders from the system as well as perform all supported tasks on the main page (see Device Manager and IR800, on page 7) except as limited by the privilege level that the administrator configures on the router for that user.
  - When operating without IoT-FND, the Device Manager user does not have access to work orders; however, the user can perform all supported tasks on the main page except as limited by the user’s privilege level.
- Device Manager can manage IR500 gateways in Connected Grid field deployments operating with or without IoT-FND:
  - When operating with IoT-FND, a Device Manager user can retrieve work orders from the system as well as perform all supported tasks on the main page (see Figure 6: Device Manager Common Page Elements and Controls (IR500), on page 12).

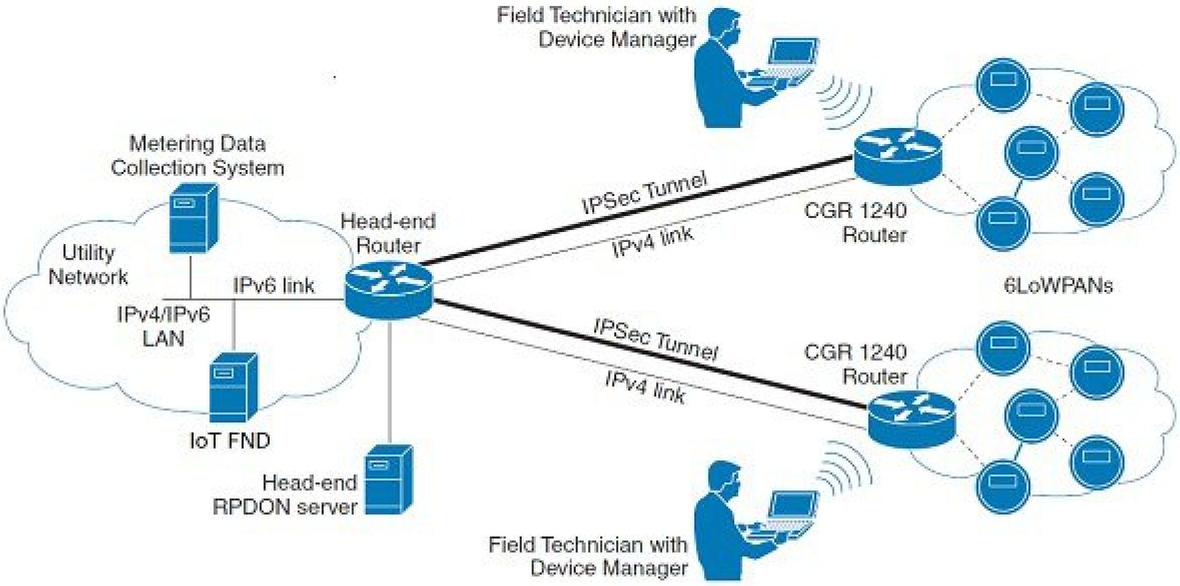
    IR500 devices use CoAP Simple Management Protocol (CSMP) for communicating with IoT-FND. The IR500 gateways regularly report inventory metrics to IoT-FND using CSMP. IoT-FND stores the reported properties and metrics.
  - When operating without IoT-FND, the Device Manager user does not have access to work orders. The user can view device settings and status but cannot make configuration changes or send data to IoT-FND.

Device Manager and CGR 1000

CGR 1000 routers are multi-service communications platforms designed for use in a field area network (FAN). The portfolio consists of two models–CGR 1240 and CGR 1120–both ruggedized to varying degrees for outdoor and indoor deployments. Both models are modular and support a wide-range of communications interfaces such as 2G/3G, 4G LTE, Ethernet, and WiFi.

Device Manager connects to the CGR 1000 by using a secure Ethernet or WiFi link. (See the following figure.)

Figure 1: Device Manager Application Within a Connected Grid Network



User Interface

When you first start Device Manager, it displays the Device Manager opening page with a list of work orders, if any are available. From this page, you can connect to the CGR 1000 either with or without a work order. (See Connecting to the CGR 1000.)

After connecting to the router, Device Manager displays the Dashboard. On the left-hand side of the Dashboard, you can view the router and any installed Connected Grid modules. LEDs indicate the current state of the router and modules. You can also view the status of Ethernet ports and modules while hovering over them.

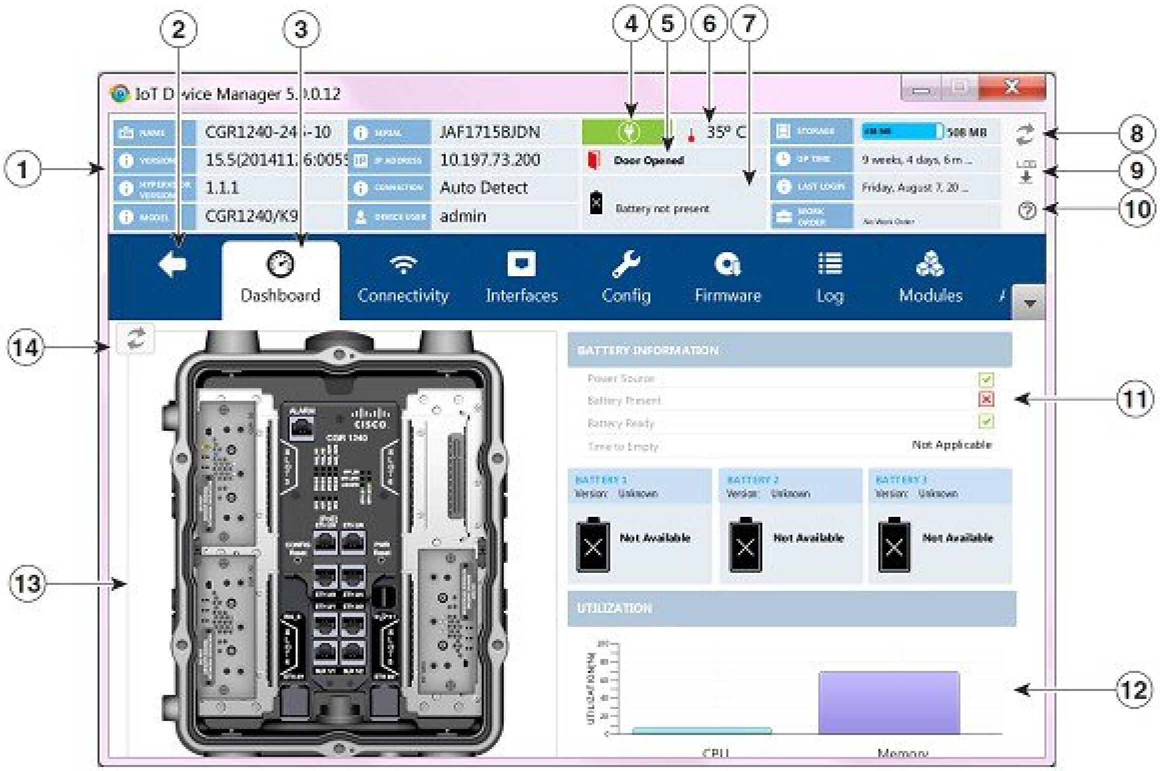
On the right-hand side of the Dashboard, you can view a graph of CPU and memory utilization. For the CGR 1240, you can view battery information.

At the top of the screen, a mini-dashboard provides additional details on the router as detailed in Table 1: Mini-dashboard information (CGR 1000) , on page 5.

For an overview of all the tasks that you can perform with Device Manager, refer to Table 2: Device Manager Tasks (CGR 1000) , on page 6.

The following figure shows the common page elements and controls for the Device Manager pages.

Figure 2: Device Manager Common Page Elements and Controls (CGR 1000)



CGR1240-24 -10
15.5(201411: 6:005
1.1.1
CGR1240/K9
JAF1715BJDN
10.197.73.200
Auto Detect
admin
35° C
Door Opened
Battery not present
508 MB
9 weeks, 4 days, 6 m ...
Friday, August 7, 20 ...

Power Source ✓
Battery Present ☒
Battery Ready ✓
Time to Empty Not Applicable

BATTERY 1 Version: Unknown Not Available
BATTERY 2 Version: Unknown Not Available
BATTERY 3 Version: Unknown Not Available

1	Mini-dashboard	8	Refresh button for mini-dashboard
2	Disconnect from device	9	IoT-DM application log file
3	Menu tabs	10	Troubleshooting wizard
4	Power status (CGR 1240 only)	11	Battery information (CGR1240 only)
5	Door status (CGR 1240 only)	12	Graph of CPU and memory utilization
6	Device temperature	13	View of device
7	Battery Information (CGR 1240 only)	14	Refresh button for Dashboard

Note Point to an active LED or module in the front or rear view of the device to display a tooltip. Items on the mini-dashboard also have tooltips.

The mini-dashboard (see Figure 2: Device Manager Common Page Elements and Controls (CGR 1000), on page 4) appears at the top of every Device Manager page, and provides the information listed in the following table.

Table 1: Mini-dashboard information (CGR 1000)

Field	Description
Name	Name of the router
Version	Cisco IOS version
Hypervisor Version	Hypervisor (virtual machine monitor) version
Model	Model number of the device
Serial	Serial number of the device
IP Address	Device IP address
Connection	Connection method—Ethernet, WiFi, or Auto Detect
Device User	User logged in to device
Power status (plug icon)	AC ON (green) or AC OFF (red) (CGR 1240 only)
Temperature	Temperature of the router
Door	Displays whether door to router is open or not (CGR 1240 only)
Battery	Displays status of the optional Battery Backup Unit (BBU) when installed (CGR 1240 only)
Storage	Amount of used and total space on the SD Flash Memory Module (hover the cursor over the Storage icon to view the amount of free space)
Up Time	Length of time that the device has been up
Last Login	Time that the user last logged in to Device Manager
Work Order	Work order number, work order name, and time remaining to complete the work (Device Manager is connected to a router using IoT-FND and an active work order exists). If you have not synchronized with IoT-FND to download the work orders, No Work Order is displayed in this field.

Tasks

Device Manager displays the main page (see Figure 2: Device Manager Common Page Elements and Controls (CGR 1000), on page 4) after securely connecting to the CGR 1000. From the Menu tabs on the main page, you can perform the following tasks as determined by your privilege level. (See User Accounts, on page 14 for more information about user accounts and privilege levels.) The following table lists all the tasks that a user with privilege level 15 (default privileged EXEC mode) can perform with Device Manager and provides an example of when to perform each task.

Table 2: Device Manager Tasks (CGR 1000)

Task	Example of When to Perform Task
Use the Dashboard to check the status of router hardware, such as BBU (CGR 1240 option only), power, and modules. (See User Interface, on page 3.)	• Newly deployed CGR 1000s do not appear in the back-end system. Start the Device Manager and review the router graphic on the Dashboard. • Check the installed modules and their LEDs to verify their operation. When the LEDs are not flashing, check the installation status of the modules. • (CGR 1240 only) The door of the CGR 1240 is open. Start the Device Manager and check the status of the door (top of the main page). When the door status indicates a status of *System Casing Open* , you must physically access the CGR 1240 to verify the status of the door. After closing the door, click the Refresh icon (upper right) on the Device Manager and verify that the door status displays *System Casing Closed* .
Verify access to a device (IP address) from the CGR 1000 by using ping to check link connectivity and quality, and initiate a traceroute for an inaccessible IP address. (See Testing Connectivity.)	• Devices connected to a CGR 1000 cannot be reached. Start the Device Manager, connect to the router, and then check connectivity to the device.
Bring up or shut down a CGR 1000 interface and view details for an interface. (See Managing Interfaces.)	• When there are issues related to WiMAX connectivity, (for instance, after a storm, the WiMAX antenna may not be pointing in the right direction, which can cause RSSI/CINR values to drop), view details for the WiMAX module to help troubleshoot the issue. If the issue involves a directional antenna, you can change the direction of the antenna and watch RSSI/CINR values change accordingly. • You can check the details of 4G LTE interfaces like the status of modem.
Update the CGR 1000 configuration with a provided configuration file, and then reboot the router with the new configuration. (See Changing the Configuration.)	• When the configuration information is incorrect, update the configuration by adding a configuration file to the Device Manager and then installing the configuration file on the CGR 1000. After you install the configuration file, the router automatically reboots with the new configuration.
Upload a copy of a software image onto the CGR 1000 for immediate installation or for a deferred update of the image. (See Updating the Firmware Image.)	• A firmware image update must be uploaded and installed on the CGR 1000. Start the Device Manager, upload the new image file, and then update the router with the new image. The router automatically reboots after you update the software image.
Download and view the CGR 1000 system logs. (See Retrieving Logs.)	• You need to review the CGR 1000 system logs to troubleshoot the CGR 1000. Start Device Manager and click the **Log** tab.

Task	Example of When to Perform Task
Insert and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. (See Managing Modules.)	- A 4G LTE module is being added to a CGR 1240. Start Device Manager and click the **Modules** tab.
Execute CLI commands using a console-like interface to view system information. Supported queries include verifying the system time, viewing the current router configuration, saving the current configuration, viewing the current file directory, rebooting the router, or saving the window output to a file. (See Executing Commands.)	- You need to review the CGR 1000 configuration information to troubleshoot the CGR 1000. Start Device Manager and click the **Advanced** tab.

Device Manager and IR800

The Cisco 800 Series Industrial Integrated Services Routers are compact, ruggedized, Cisco IOS Softwar routers. They offer support for integrated 4G LTE wireless WAN (both 809 and 829 models) and wireles LAN capabilities (829 model only). Device Manager connects to the IR809 by using a secure Ethernet link and to the IR829 by using a secure Ethernet or WiFi link. The IR809 must have IPv6 option enabled to connec with work order.

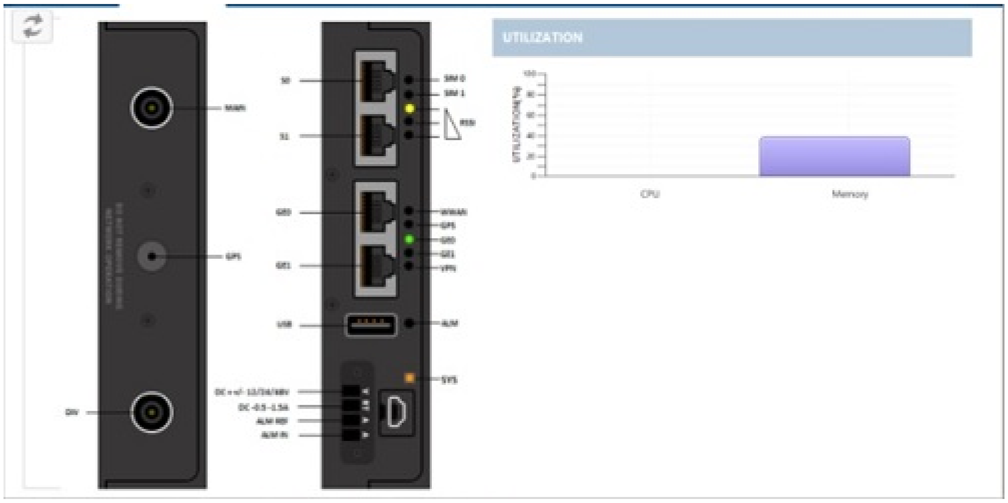
User Interface

When you first start Device Manager, it displays the Device Manager opening page with a list of work orders, if any are available. From this page, you can connect to the IR800 router either with or without a work order.

After connecting to the router, Device Manager displays the Dashboard (see the following figure for an example of IR809 dashboard). On the left-hand side of the Dashboard, you can view the front and rear of the router. LEDs indicate the current state of the router and ports. You can also view the status of ports while hovering over them.

On the right-hand side of the Dashboard, you can view details about the router settings and status.

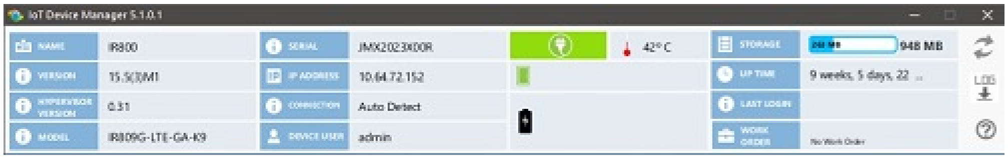
Figure 3: IR809 DashBoard in the Device Manager



Note Point to an active LED or port in the front or rear view of the device to display a tooltip. Items on the mini-dashboard also have tooltips.

At the top of the screen, a mini-dashboard provides additional details on the router as shown in the following figure.

Figure 4: IR800 Mini-DashBoard in the Device Manager



IoT Device Manager 5.1.0.1

NAME	IR800	SERIAL	JMX2023X0DR		42° C	STORAGE	948 MB
VERSION	15.5(3)M1	IP ADDRESS	10.64.72.152			UP TIME	9 weeks, 5 days, 22 ...
HYPERVISOR VERSION	0.31	CONNECTION	Auto Detect			LAST LOGIN	
MODEL	IR809G-LTE-GA-K9	DEVICE USER	admin			WORK ORDER	No Work Order

The mini-dashboard appears at the top of every Device Manager page, and provides the information listed in the following table.

Table 3: Mini-dashboard information (IR800)

Field	Description
Name	Name of the router
Version	Cisco IOS version
Hypervisor Version	Hypervisor (virtual machine monitor) version
Model	Model number of the device
Serial	Serial number of the device
IP Address	Device IP address
Connection	Connection method—Ethernet, WiFi, or Auto Detect

Field	Description
Device User	User logged in to device
Power status (plug icon)	AC ON (green) or AC OFF (red)
Temperature	Temperature of the router
Storage	Amount of used and total space on the SD Flash Memory Module (hover the cursor over the Storage icon to view the amount of free space)
Up Time	Length of time that the device has been up
Last Login	Time that the user last logged in to Device Manager
Work Order	Work order number, work order name, and time remaining to complete the work (Device Manager is connected to a router using IoT-FND and an active work order exists). If you have not synchronized with IoT-FND to download the work orders, No Work Order is displayed in this field.

Tasks

Device Manager displays the main page after securely connecting to the IR800. From the Menu tabs on the main page, you can perform the tasks listed in the following table.

Table 4: Device Manager Tasks (IR800)

Task	Example of When to Perform Task
Use the Dashboard to check the status of the IR800 hardware, such as power and device ports. (See User Interface, on page 7 and Viewing Settings and Status.)	• You need to monitor the IR800 status, activity, and performance.
Use the Ethernet and Serial interface popup menus to view interface details. (See Viewing Details for an Interface, on page 73.)	• You need to check statistics for the Ethernet and Serial ports.
Use the Ethernet interface popup menu to manage the interface. (See Managing Interfaces, on page 72.)	• You need to bring up, shutdown, or reset the Ethernet interface.
Configure or modify general, MAP-T, and serial interface settings. (See Changing the Configuration, on page 75.)	• The IR800 needs to transfer serial data between RTUs and a utility management system across an IP network. Use the Config page to configure TCP raw socket session settings for the serial interface.
Upload, install, and back up a copy of a software image. (See Updating the Firmware Image.)	• A firmware image update must be uploaded and installed on the IR800. Use the Firmware page to upload the new image file, and then update the device with the new image.

Task	Example of When to Perform Task
Verify access to a device (IPv6 address) from the IR800 by using the Ping option to check link connectivity and quality. (See Testing Connectivity, on page 68.)	• Devices connected to an IR800 over the Ethernet or 6LoWPAN interface cannot be reached. Connect to the IR800 and then check connectivity to the device.

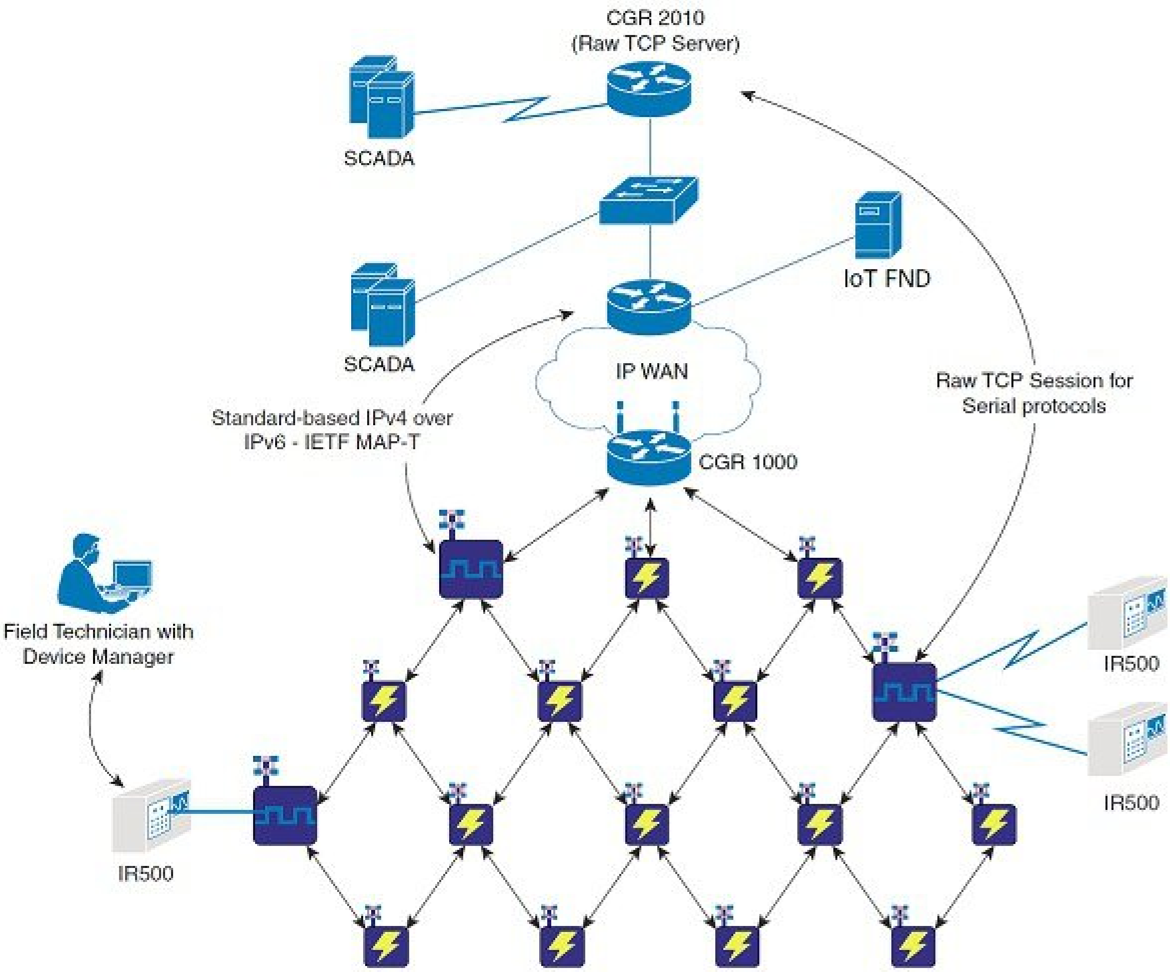
Device Manager and IR500

The IR500 is a distribution automation (DA) gateway that provides secure IPv4/IPv6 connectivity to DA devices such as capacitor bank controllers, reclosers, or other SCADA devices. The IR500 connects to DA devices using serial ports (RS232/RS485) and/or an Ethernet port using IPv4. The IR500 provides remote connectivity to serial DA devices over Cisco Resilient Mesh (formerly known as CG-Mesh) by transporting serial data over TCP/IP. The IR500 also provides remote connectivity to IPv4 DA devices over the IPv6-based Resilient Mesh by using Mapping of Address and Port using Translation (MAP-T). The IR500 performs NAT44 translation to translate private IPv4 addresses used by DA devices connected to the Ethernet port to public IPv4 addresses used with MAP-T.

For more information about MAP-T, see Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide. For more information about IR500, see http://www.cisco.com/go/ir500 .

The following figure shows the IR500 in a Cisco Resilient Mesh deployment.

Figure 5: IR500 in a Resilient Mesh Network



User Interface

When you first start Device Manager, it displays the Device Manager opening page with a list of work orders, if any are available. From this page, you can connect to the IR500 after physically connecting the IR500 to the laptop (see Connecting to the IR500).

After connecting to the IR500, Device Manager displays the Dashboard. On the left-hand side of the Dashboard, you can view the front and rear of the IR500. LEDs indicate the current state of the device and ports. You can also view the status of ports while hovering over them. The Ethernet port has a popup menu with options for managing the interface and viewing interface details. The two serial ports also have popup menus with the option to view interface details.

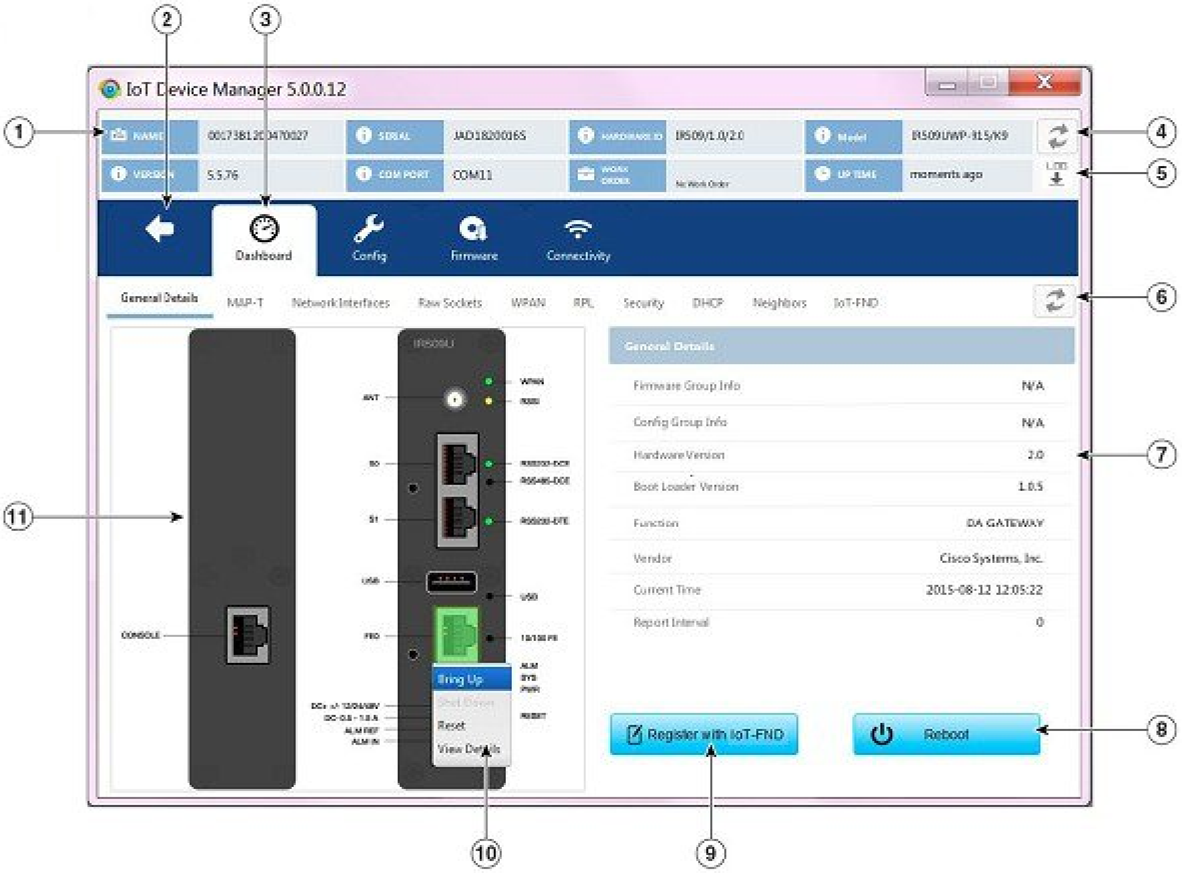
On the right-hand side of the Dashboard, you can view details about the device settings and status (see Viewing Settings and Status).

At the top of the screen, a mini-dashboard provides additional details on the device as detailed in Table 5: Mini-dashboard information (IR500) , on page 13.

For an overview of all the tasks that you can perform with Device Manager, refer to Table 6: Device Manager Tasks (IR500) , on page 13.

The following figure shows the common page elements and controls for the Device Manager pages.

Figure 6: Device Manager Common Page Elements and Controls (IR500)



IoT Device Manager 5.0.0.12

NAME	00173812D0470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

1	Mini-dashboard	7	Details area
2	Disconnect from device	8	Reboot device
3	Menu tabs	9	Register with IoT-FND
4	Refresh button for mini-dashboard	10	Pop-up menu
5	IoT-DM application log file	11	Front (right) and rear (left) views of device
6	Refresh button for Dashboard		

Note Point to an active LED or port in the front or rear view of the device to display a tooltip. Items on the mini-dashboard also have tooltips.

The min-dashboard (see above figure) appears at the top of every Device Manager page, and provides the information listed in the following table.

Table 5: Mini-dashboard information (IR500)

Field	Description
Name	Name of the device
Version	Firmware version
Serial	Serial number of the device
COM Port	Communication port to which the device is connected
Hardware ID	Hardware identification number of the device
Work Order	Work order number, work order name, and time remaining to complete the work
Model	Model number of the device
Uptime	Length of time that the device has been up

Tasks

Device Manager displays the main page (see Figure 6: Device Manager Common Page Elements and Controls (IR500), on page 12) after securely connecting to the IR500. From the Menu tabs on the main page, you can perform the tasks listed in the following table.

Table 6: Device Manager Tasks (IR500)

Task	Example of When to Perform Task
Use the Dashboard to check the status of the IR500 hardware, such as power and device ports. (See User Interface, on page 11 and Viewing Settings and Status.)	• You need to monitor the IR500 status, activity, and performance.
Use the Ethernet and Serial interface popup menus to view interface details. (See Viewing Interface Details.)	• You need to check statistics for the Ethernet and Serial ports.
Use the Ethernet interface popup menu to manage the interface. (See Managing the Ethernet Interface.)	• You need to bring up, shutdown, or reset the Ethernet interface.
View details about IR500 settings and status. (See Viewing Settings and Status.)	• You need to view details for MAP-T, TCP raw socket, WPAN, RPL, and other protocols used by the IR500 to verify performance of the Cisco Resilient Mesh network and troubleshoot issues.

Task	Example of When to Perform Task
Configure or modify general, MAP-T, and serial interface settings. (See Changing the Configuration.)	• The IR500 needs to transfer serial data between RTUs and a utility management system across an IP network. Use the Config page to configure TCP raw socket session settings for the serial interface.
Upload, install, and back up a copy of a software image. (See Updating the Firmware Image.)	• A firmware image update must be uploaded and installed on the IR500. Use the Firmware page to upload the new image file, and then update the device with the new image.
Verify access to a device (IPv6 address) from the IR500 by using the Ping option to check link connectivity and quality. (See Testing Connectivity.)	• Devices connected to an IR500 over the Ethernet or 6LoWPAN interface cannot be reached. Connect to the IR500 and then check connectivity to the device.

Certificates

A valid X.509 certificate is required for Device Manager to connect to the routers and DA gateways.

You can import certificates through the Device Manager opening page. (See Importing Certificates.)

Work Orders

When you first start Device Manager, it displays the Device Manager opening page, which lists available work orders. On this page, you can view and select work orders for the CGR 1000 routers and IR500 DA gateways, and synchronize with Cisco IoT-FND to download work orders. (See Managing Work Orders.) Device Manager needs to be connected to IoT-FND only to download and update the work orders.

User Accounts

The IoT-FND administrator creates user accounts for the field technicians who use Device Manager to download work orders from IoT-FND. For more information, see *Cisco Connected Grid Network Management System User Guide, Release 2.1*.

The user privilege level configured on the CGR 1000 also authorizes the user to perform tasks on the CGR 1000 using Device Manager. The default configuration for Cisco IOS software-based networking devices uses privilege level 1 for user EXEC mode and privilege level 15 for privileged EXEC. The commands that you can run in user EXEC mode at privilege level 1 are a subset of the commands that you can run in privileged EXEC mode at privilege 15. (See Configuring Security with Passwords Privileges and Logins for more information.)

The following user accounts are provisioned at the factory:

- username cgdm-viewer-t privilege 2 token
- username cgdm-admin-t privilege 15 token

- username cgdm-viewer privilege 2
- username cgdm-admin privilege 15

The following table shows the required privilege level for the listed tasks.

Table 7: Privilege Levels for Device Manager Tasks

Task	Privilege Level
View interfaces, run ping/traceroute, view logs, view directory contents.	2
Bring up or shut down a CGR 1000 interface, upload files, add or remove modules, and execute commands.	15

Additional Information

For more information about Connected Grid devices and features, refer to the documents listed in the table below.

Device or Feature	Related Documents
Cisco 1000 Series Connected Grid Routers	Configuration and Installation Guides: http://www.cisco.com/go/cgr1000-docs
Cisco 800 Series Industrial Integrated Services Routers (IR800)	http://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-hon
IR500	Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide
IoT-FND	Cisco IoT Field Network Director User Guide North Bound API User Guide for the Cisco IoT Field Network Director 3.0
WPAN and Cisco Resilient Mesh	Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Config Guide (Cisco IOS)

Device or Feature	Related Documents
Raw Socket	Raw Socket Transport Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco I Configuring Raw Socket Protocol on the CGR 2010 Router

Feature History

Platform	Release	Feature Information
Cisco IoT Device Manager (DM) for Cisco IOS	Cisco IoT Device Manager Release 5.1.0	• Support for Windows 10. • Supports for TLS v1.2 - IoTDM can connect to FnD running TLS v1.2. • Support for IR809 and IR829 routers and IR510 gateways. Minimum Cisco IOS release 15.6(3)M2. • Support for Get TLVs and Post TLVs operations on the IR509 and IR510 routers. • Modulation support on IR510.
Cisco IoT Device Manager (DM) for Cisco IOS	Cisco IoT Device Manager Release 5.0.0.16	• Support for 4G LTE module for CGR 1000. Minimum Cisco IOS release 15.5(3)M. • Compatible with IoT Field Network Director 3.0 and Industrial Operations Kit 2.0. Minimum Cisco IOS Release 15.5(3)M.

CHAPTER 2

Installation

This chapter explains how to install the Device Manager software.

Required Expertise

This guide is intended for Field Technicians who have basic experience operating a computer laptop.

System Requirements

This section lists the system requirements for Device Manager Release 5.1.

Laptop

The laptop running Device Manager must have the following:

- Microsoft Windows 10, Microsoft Windows 7 Enterprise, or Microsoft Windows Professional.
- 2 GHz or faster processor recommended
- 2 GB RAM minimum (for potential large log file processing)
- WiFi or Ethernet interface
- 4 GB disk storage space
- Windows login enabled
- Utility-signed Certificate Authority (CA) and Client Certificate for router authentication (obtained from your IT department)
- Customer-specific IT security hardening to keep the Device Manager laptop secure

CGR 1000

See Feature History, on page 16 for CGR 1000 software requirements.

IR809

See Feature History, on page 16 for IR800 firmware requirements.

IR500

See Feature History, on page 16 for IR500 firmware requirements.

IoT-FND

To work with Device Manager, IoT-FND must be Release 4.0 or greater.

Device Manager Installation

Note **Note:** You must uninstall any instance of CG-DM 4.x or earlier, before you install IoT-DM on your laptop. The installer will not recognize the older installation given that the product name has changed from Cisco Connected Grid Device Manager (CG-DM) to Cisco IoT Device Manager (IoT-DM).

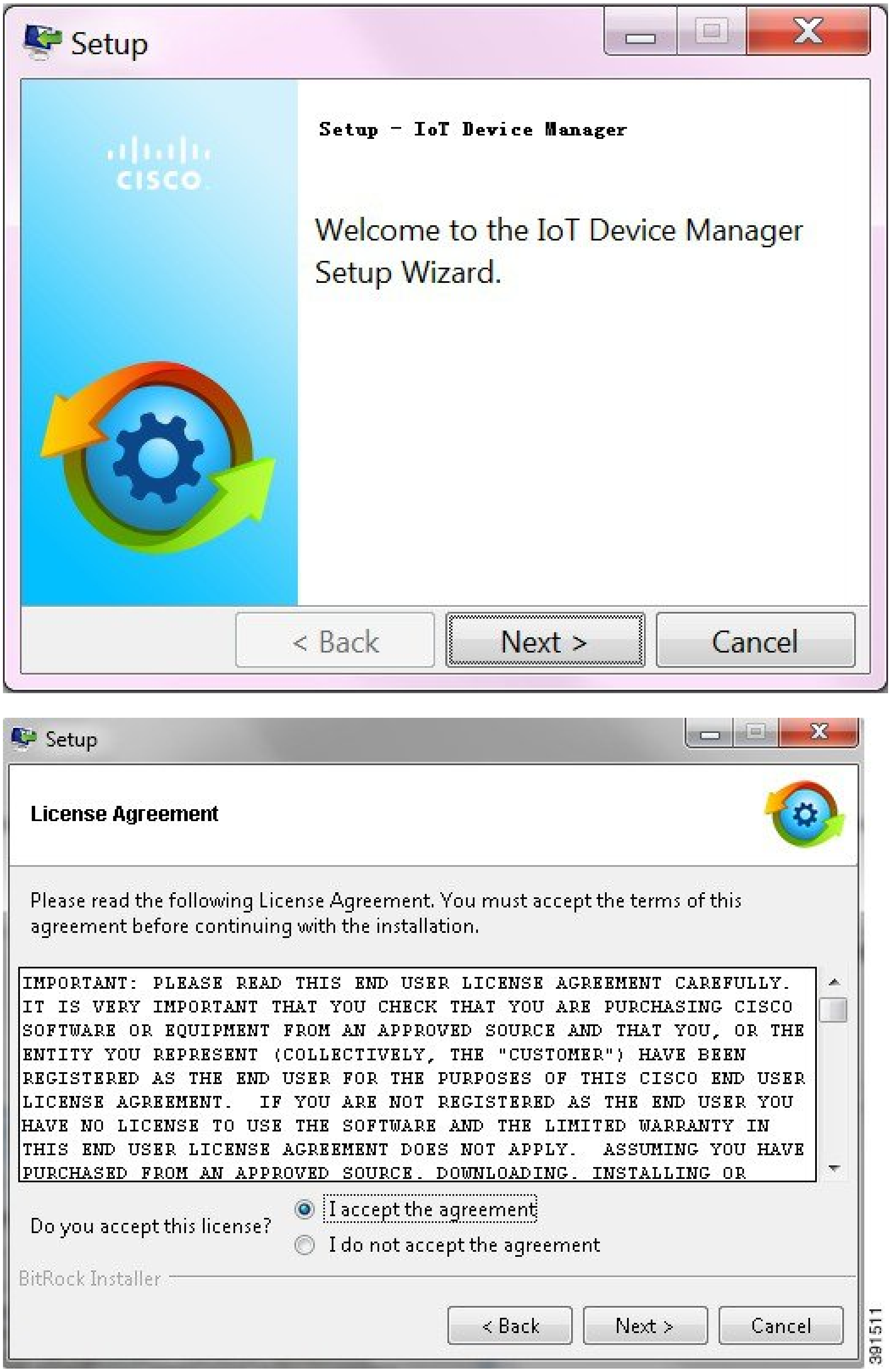
To install the Device Manager:

SUMMARY STEPS

1. Double-click the Device Manager installer executable to start installation.

DETAILED STEPS

Double-click the Device Manager installer executable to start installation.



Welcome to the IoT Device Manager Setup Wizard.

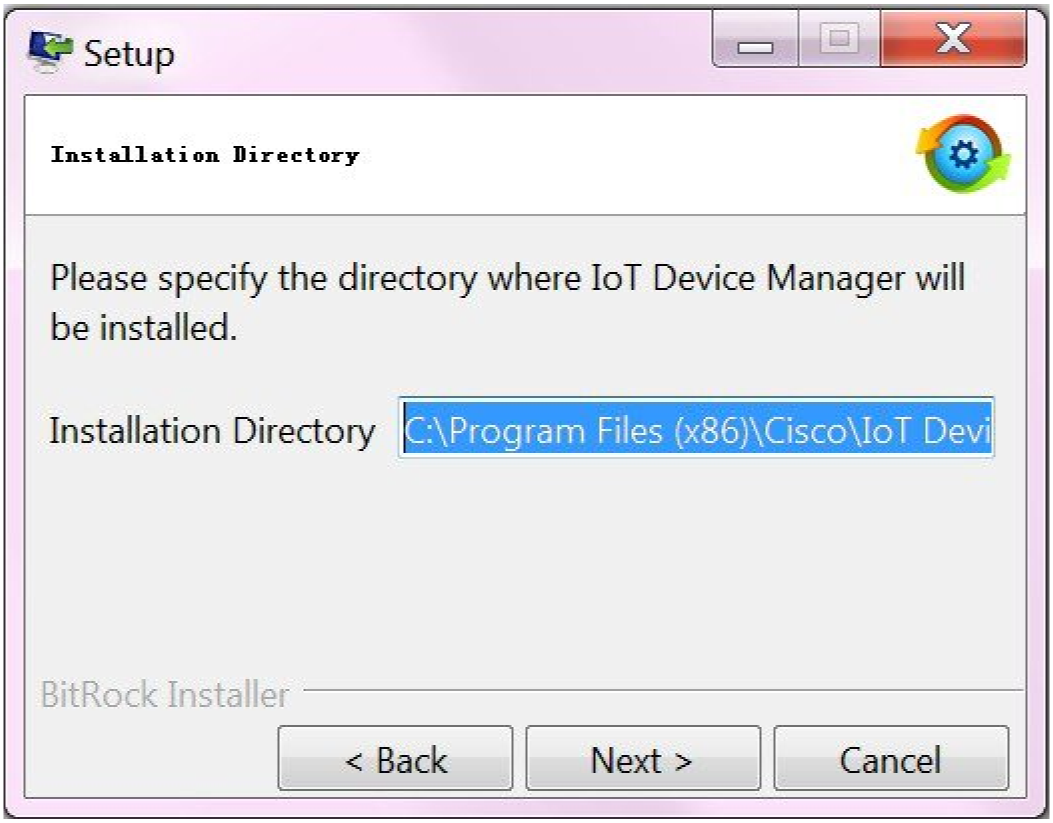
License Agreement

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

```
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY.
IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO
SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE
ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN
REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER
LICENSE AGREEMENT.  IF YOU ARE NOT REGISTERED AS THE END USER YOU
HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN
THIS END USER LICENSE AGREEMENT DOES NOT APPLY.  ASSUMING YOU HAVE
PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR
```

Do you accept this license?

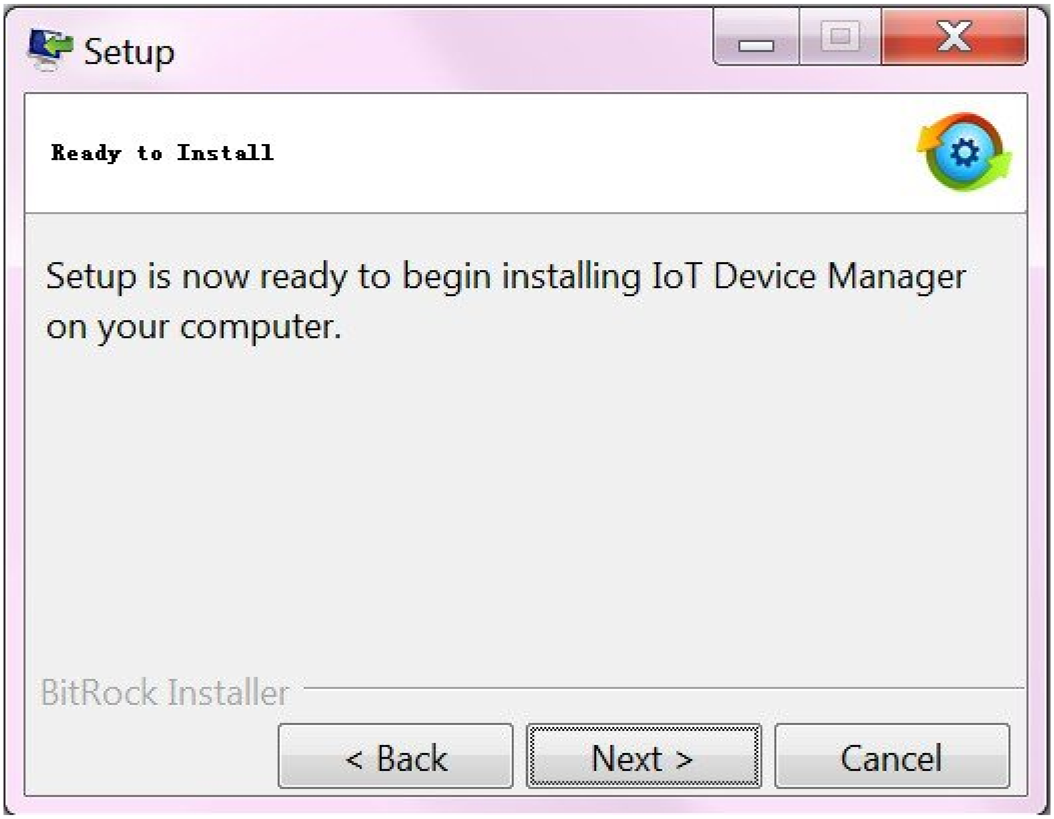
● I accept the agreement
○ I do not accept the agreement



Installation Directory

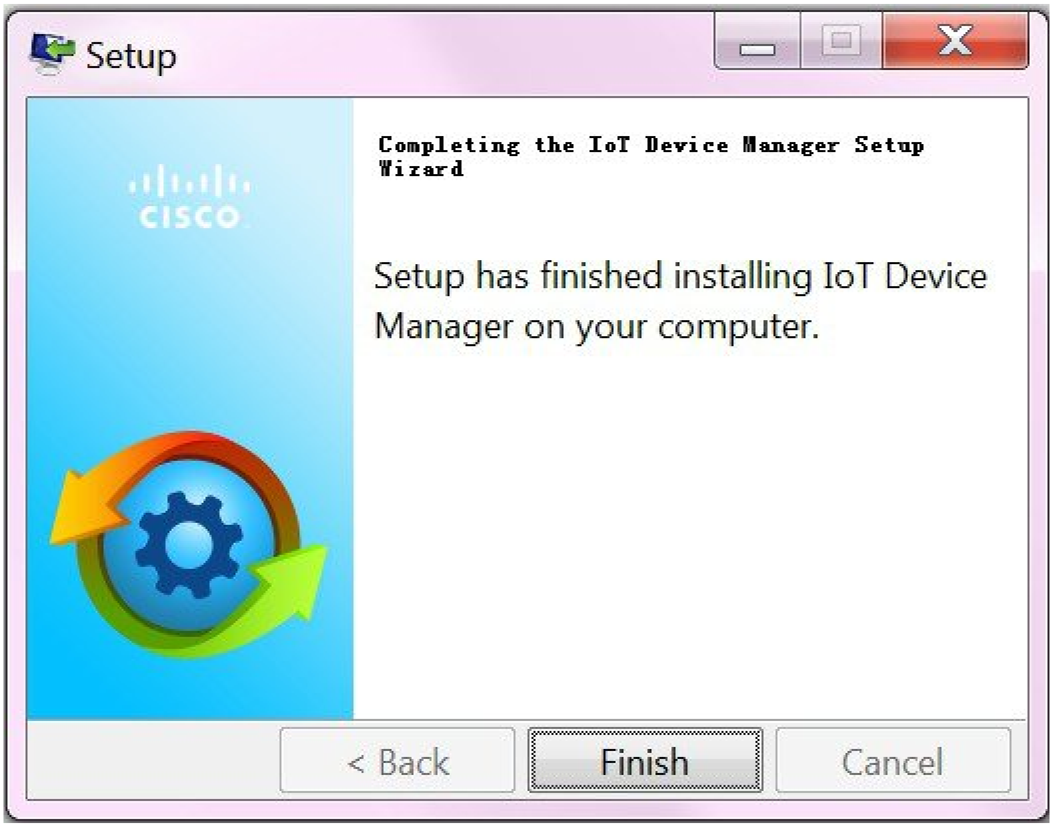
Please specify the directory where IoT Device Manager will be installed.

Installation Directory C:\Program Files (x86)\Cisco\IoT Devi



Ready to Install

Setup is now ready to begin installing IoT Device Manager on your computer.



Completing the IoT Device Manager Setup Wizard

Setup has finished installing IoT Device Manager on your computer.

Device Manager Removal

To remove the Device Manager application, click **Start** > **All Programs** > **Cisco IoT Device Manager** > **Uninstall Cisco IoT Device Manager**, or use **Uninstall or change a program** from **Control Panel** > **Programs and Features**.

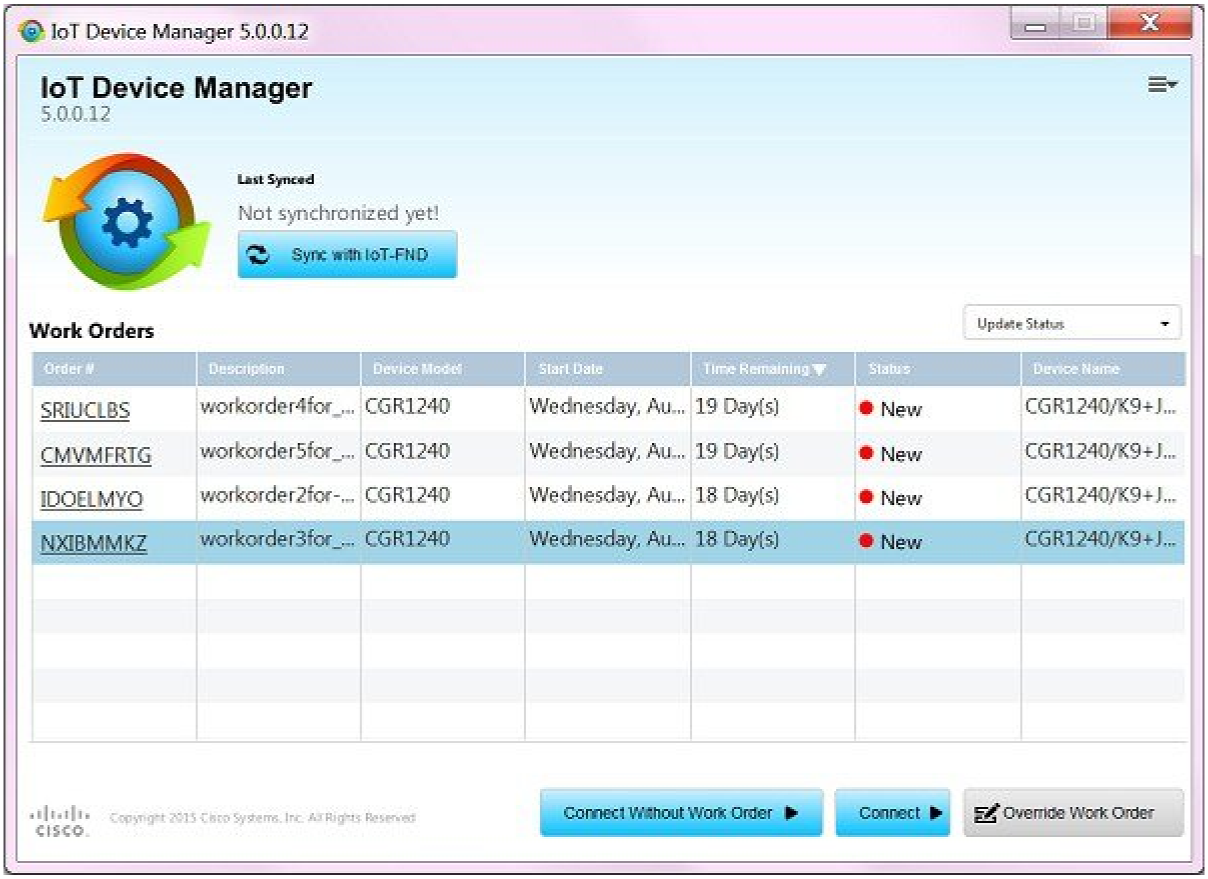
CHAPTER 3

Managing Work Orders

The chapter describes using the Device Manager opening page with the CGR 1000, IR800, or IR500 to connect to IoT-FND and manage work orders.

Work Orders

When you first start Device Manager, the opening page displays a list of work orders, if any are available.



IoT Device Manager
5.0.0.12

Last Synced

Not synchronized yet!

Work Orders

Order #	Description	Device Model	Start Date	Time Remaining	Status	Device Name
SRIUCLBS	workorder4for_...	CGR1240	Wednesday, Au...	19 Day(s)	● New	CGR1240/K9+J...
CMVMFRTG	workorder5for_...	CGR1240	Wednesday, Au...	19 Day(s)	● New	CGR1240/K9+J...
IDOELMYO	workorder2for-...	CGR1240	Wednesday, Au...	18 Day(s)	● New	CGR1240/K9+J...
NXIBMMKZ	workorder3for_...	CGR1240	Wednesday, Au...	18 Day(s)	● New	CGR1240/K9+J...

Copyright 2015 Cisco Systems, Inc. All Rights Reserved

Whenever work or direct inspection of a CGR 1000 or IR500 is necessary by a field technician, an administrator generates a work order in IoT-FND. Work orders include the encrypted credentials necessary for the technician to connect to the router.

You must synchronize Device Manager with IoT-FND to download the latest work orders from IoT-FND and upload status of the work orders to IoT-FND. See Synchronizing With IoT-FND, on page 28.

Each work order shows the following information:

- Work order number
- Description
- Device model
- Start date
- Time remaining on the work order

Note When no time remains on the work order, Time Remaining displays “Expired”. If you attempt to connect to the router with an Expired work order, Device Manager displays an error message.

- Status of the work order: New, In Service, Completed, or Incomplete

- Device name

Importing Certificates

IoT-DM can connect with FND by FND's web UI cert SHA256 fingerprint or CA certificate and connect with IOS devices by CA certificate.

As admin, you can import certificates through the Device Manager opening page. You need to know the path to the certificate (.pfx). Generally, the admin downloads the .pfx file and password to the Device Manager laptop. All these certificates will be verified when being imported to IoT-DM.

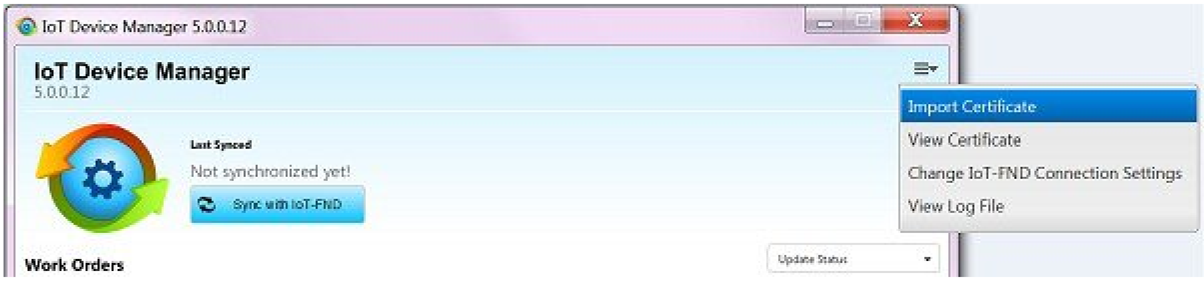
To import a certificate:

SUMMARY STEPS

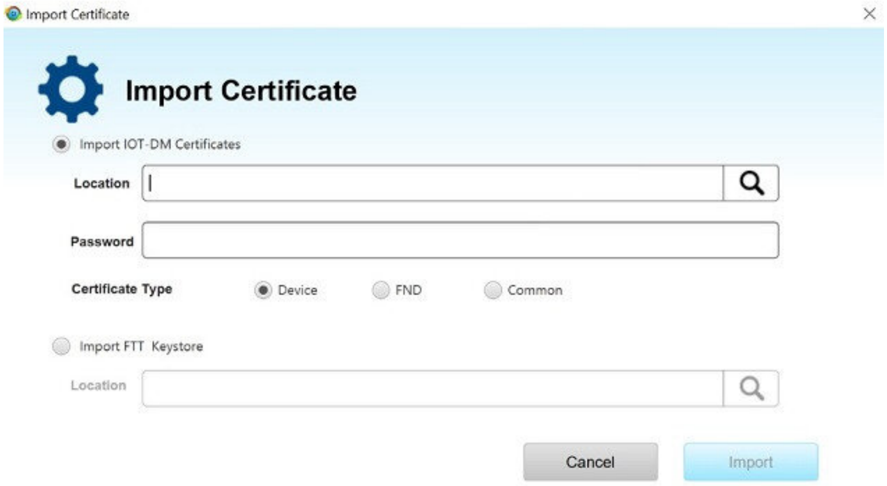
1. On the Device Manager opening page, select **Import Certificate** from the drop-down menu on the upper right.
2. In the Import Certificate dialog box, browse to the location of the certificate file on your laptop and enter the password for the pfx certificate file.
3. Choose the certificate type.
    - If FND and device are using the CA certificates issued from different CA, choose **FND** while importing certificate to communicate with FND, and choose **Device** while importing certificate for device.
    - If FND and Device are both using the CA certificate issued from the same CA, choose **Common**. The certificate will be available for the verification for both FND and Device certificate.
4. Click **Import**. A dialog box displays a success message and informs you to restart Device Manager.
5. Restart Device Manager.
6. To view the certificate details, select **View Certificate** from the Device Manager opening page drop-down menu on the upper right.
7. Click the tab for the certificate details you want to view.

DETAILED STEPS

Step 1 On the Device Manager opening page, select **Import Certificate** from the drop-down menu on the upper right.



Step 2 In the Import Certificate dialog box, browse to the location of the certificate file on your laptop and enter the password for the pfx certificate file.



Import Certificate

● Import IOT-DM Certificates

Location

Password

Certificate Type ● Device ○ FND ○ Common

○ Import FTT Keystore

Location

Step 3 Choose the certificate type.

- If FND and device are using the CA certificates issued from different CA, choose **FND** while importing certificate to communicate with FND, and choose **Device** while importing certificate for device.
- If FND and Device are both using the CA certificate issued from the same CA, choose **Common**. The certificate will be available for the verification for both FND and Device certificate.

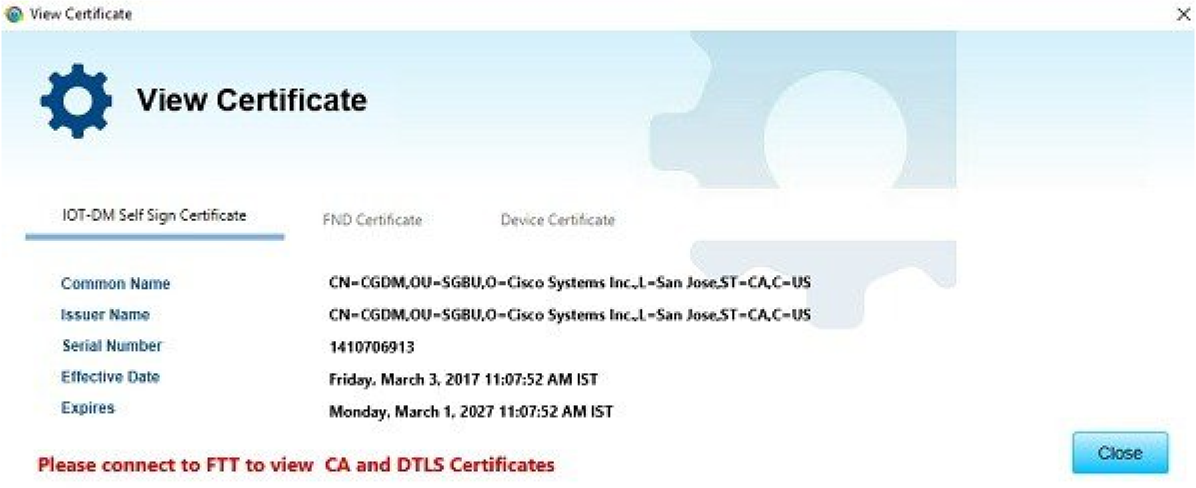
Note If you choose the FND option and import a device certificate instead of an FND certificate, the FND certificate will be replace with the device certificate. In that case, 2 copies of device certificates will be present, and you cannot connect to FND and will get an error. To connect with FND again, you need to properly choose the FND option and import the FND certificate.

If you upload a new certificate, the old certificate will be replaced, for both FND and devices.

Step 4 Click **Import**. A dialog box displays a success message and informs you to restart Device Manager.

Step 5 Restart Device Manager.

Step 6 To view the certificate details, select **View Certificate** from the Device Manager opening page drop-down menu on the upper right.



Common Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Issuer Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Serial Number	1410706913
Effective Date	Friday, March 3, 2017 11:07:52 AM IST
Expires	Monday, March 1, 2027 11:07:52 AM IST

Please connect to FTT to view CA and DTLS Certificates

Step 7 Click the tab for the certificate details you want to view.

Setting Up the IoT-FND Connection

Before synchronizing with IoT-FND for the first time, configure Device Manager to connect to the IoT-FND application server.

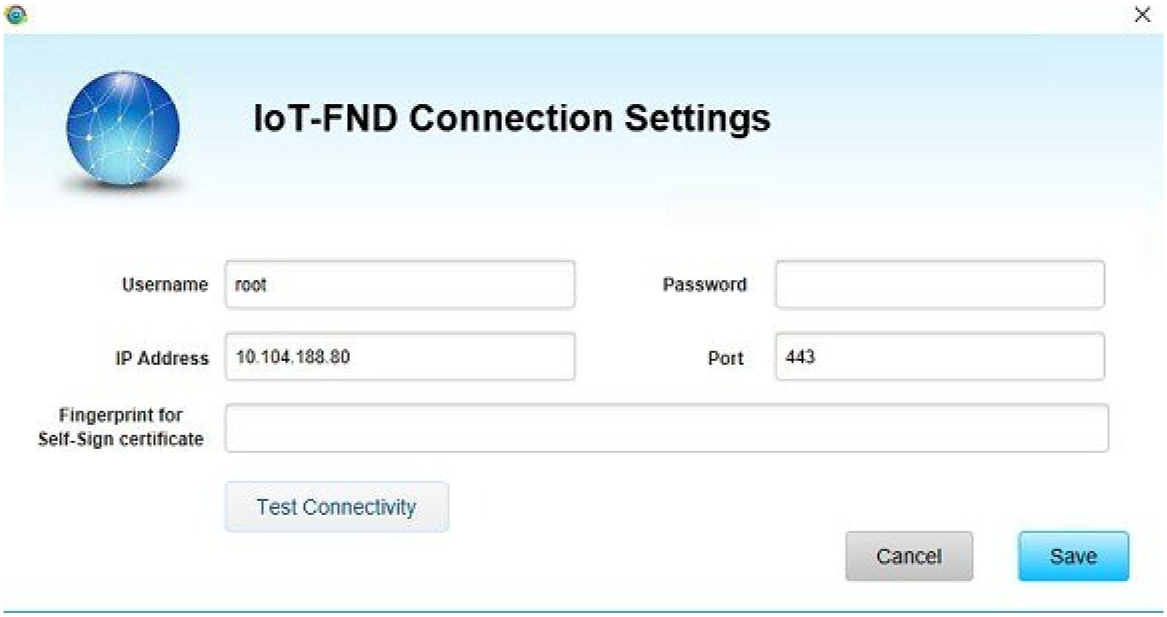
SUMMARY STEPS

1. On the Device Manager opening page, click **Sync with IoT-FND**, or select **Change IoT-FND Connection Settings** from the drop-down menu on the upper right of the page.
2. In the IoT-FND Connection Settings dialog box, enter the username, password, and IP address for connecting to the IoT-FND application server.
3. Confirm or change the server port number.
4. Click **Save**.
5. Click **Test Connectivity** to test connecting to the IoT-FND server.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Sync with IoT-FND**, or select **Change IoT-FND Connection Settings** from the drop-down menu on the upper right of the page.

Step 2 In the IoT-FND Connection Settings dialog box, enter the username, password, and IP address for connecting to the IoT-FND application server.



IoT-FND Connection Settings

Username: root

Password:

IP Address: 10.104.188.80

Port: 443

Fingerprint for Self-Sign certificate:

Step 3 Confirm or change the server port number.

Step 4 Click **Save**.

Step 5 Click **Test Connectivity** to test connecting to the IoT-FND server.

Synchronizing With IoT-FND

Synchronizing with IoT-FND is a two-way operation. All assigned work orders are downloaded from IoT-FND to CG-DM, and CG-DM updates IoT-FND with the status of complete and incomplete work orders.

Note You can only download assigned work orders from IoT-FND.

To download the latest work orders from IoT-FND and upload the status of the work orders to IoT-FND:

SUMMARY STEPS

1. On the Device Manager opening page, click **Sync with IoT-FND**. Device Manager verifies the authorization for connecting to the IoT-FND application server. If the connection is successful, a dialog box displays the message *Sync Successful* and the number of downloaded work orders.
2. Click **Close** to close the dialog box and display the list of work orders. Proceed to Connecting to the Router with a Work Order or Connecting to the IR500 with a Work Order.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Sync with IoT-FND**. Device Manager verifies the authorization for connecting to the IoT-FND application server. If the connection is successful, a dialog box displays the message *Sync Successful* and the number of downloaded work orders.

Step 2 Click **Close** to close the dialog box and display the list of work orders. Proceed to Connecting to the Router with a Work Order or Connecting to the IR500 with a Work Order.

Updating Work Order Status

The work order number on the left of the Device Manager opening page corresponds to an existing work order within a utility management or operations system that the technician can access to get additional details on the work order.

Generally, a technician synchronizes with IoT-FND at the beginning of the day to download work orders before heading to the field and then again at the end of the day when back at the office to update IoT-FND with the changes.

The work order status can be New, Complete, or Incomplete.

To update the status of a work order:

SUMMARY STEPS

1. Using the Order number that appears on the left of the Device Manager opening page, locate the specific work details from the appropriate system and then do one of the following:
2. Click **Sync with IoT-FND** to update IoT-FND.

DETAILED STEPS

Step 1 Using the Order number that appears on the left of the Device Manager opening page, locate the specific work details from the appropriate system and then do one of the following:

- When you complete the work order, select **Complete** from the Status drop-down menu.
- If you are not able to complete the work order, select **Incomplete** from the Status drop-down menu.

The work order reflects the status change.

Step 2 Click **Sync with IoT-FND** to update IoT-FND.

After synchronization with IoT-FND, all Complete, Incomplete, and Expired work orders are removed from the Device Manager display.

Override Work Order

Use the Override Work Order option when you need to use different login information than that provided in the work order.

For example, for connecting to the CGR 1000, the SSID or passphrase for a WiFi connection might have changed since the work order was first created, but a new work order was not issued. In this case, the field technician might call the administrator for that information and use Override Work Order to enter that new information to log in to the router. Optionally, the field technician can directly connect to the router over Ethernet with the Auto Discover IP address option.

To change the login information:

SUMMARY STEPS

1. On the Device Manager opening page, click **Override Work Order**.
2. Follow the steps in Manually Connecting to the Router for the CGR 1000 or Connecting to the IR500 Without a Work Order for the IR500.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Override Work Order**.

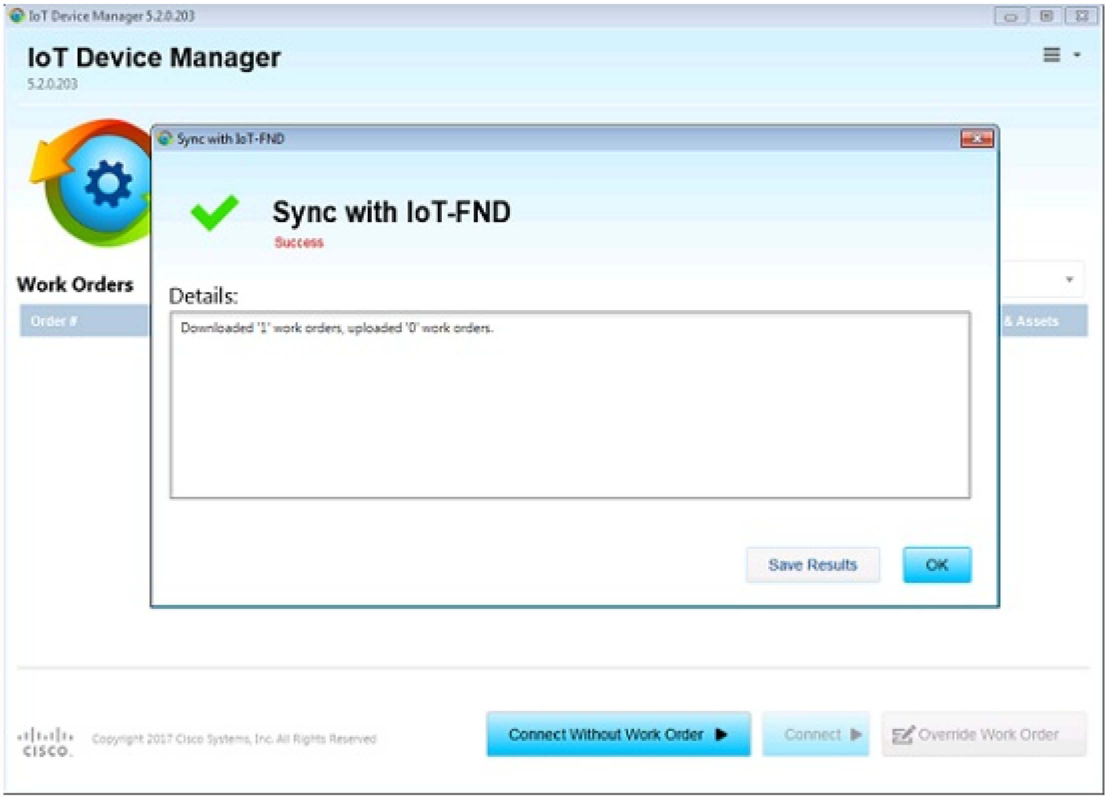
Step 2 Follow the steps in Manually Connecting to the Router for the CGR 1000 or Connecting to the IR500 Without a Work Order for the IR500.

Managing Notes and Assets of Work Order

From IoT Device Manager Release 5.2, you can display the assets and notes created in FND in IoT-DM, and add new notes to the work order. The added notes will be updated in FND via NB API. The assets created in FND cannot be modified in IoT-DM.

Follow these steps to add notes to the work order.

Step 1 Click the **Sync with IoT-FND** button to download work orders from FND.


IoT Device Manager 5.2.0.203
IoT Device Manager
5.2.0.203
Work Orders
Order #
& Assets
Sync with IoT-FND
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2017 Cisco Systems, Inc. All Rights Reserved

Sync with IoT-FND

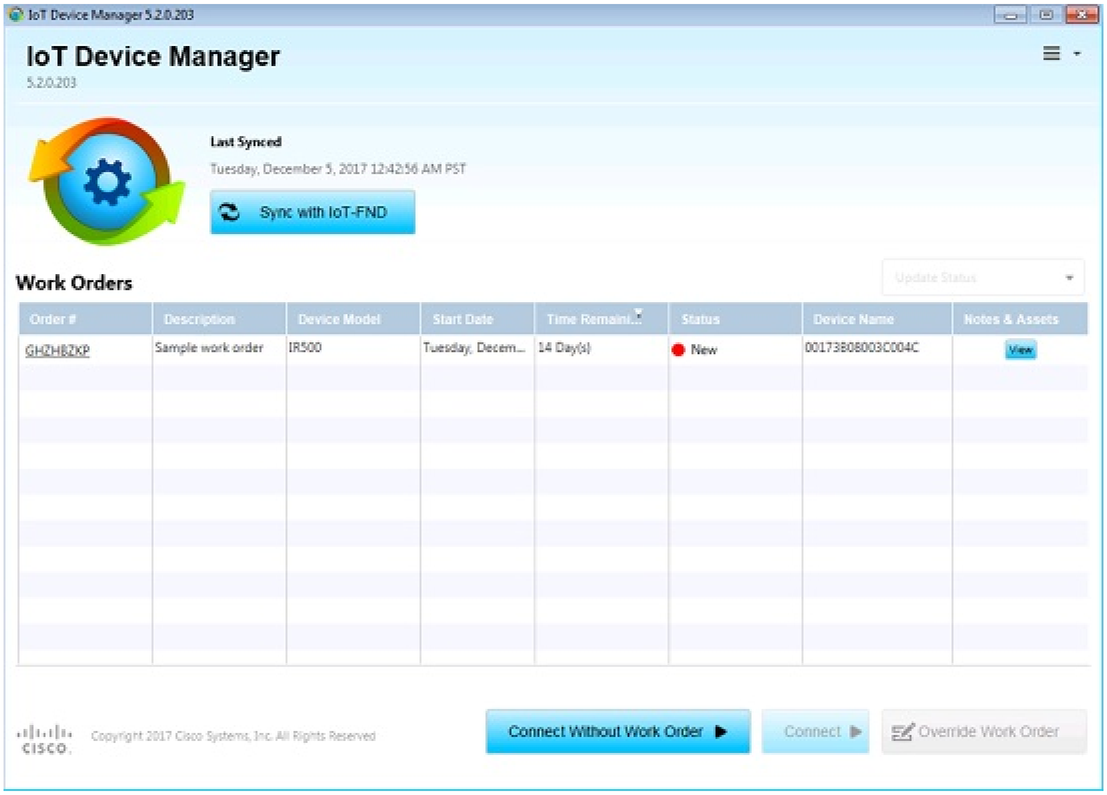
Success

Details:

Downloaded '1' work orders, uploaded '0' work orders.

Save Results OK

Step 2 When the work orders are displayed, click the **View** buttonn in the Notes & Assets column.


IoT Device Manager 5.2.0.203
IoT Device Manager
5.2.0.203
Sync with IoT-FND
Update Status
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2017 Cisco Systems, Inc. All Rights Reserved

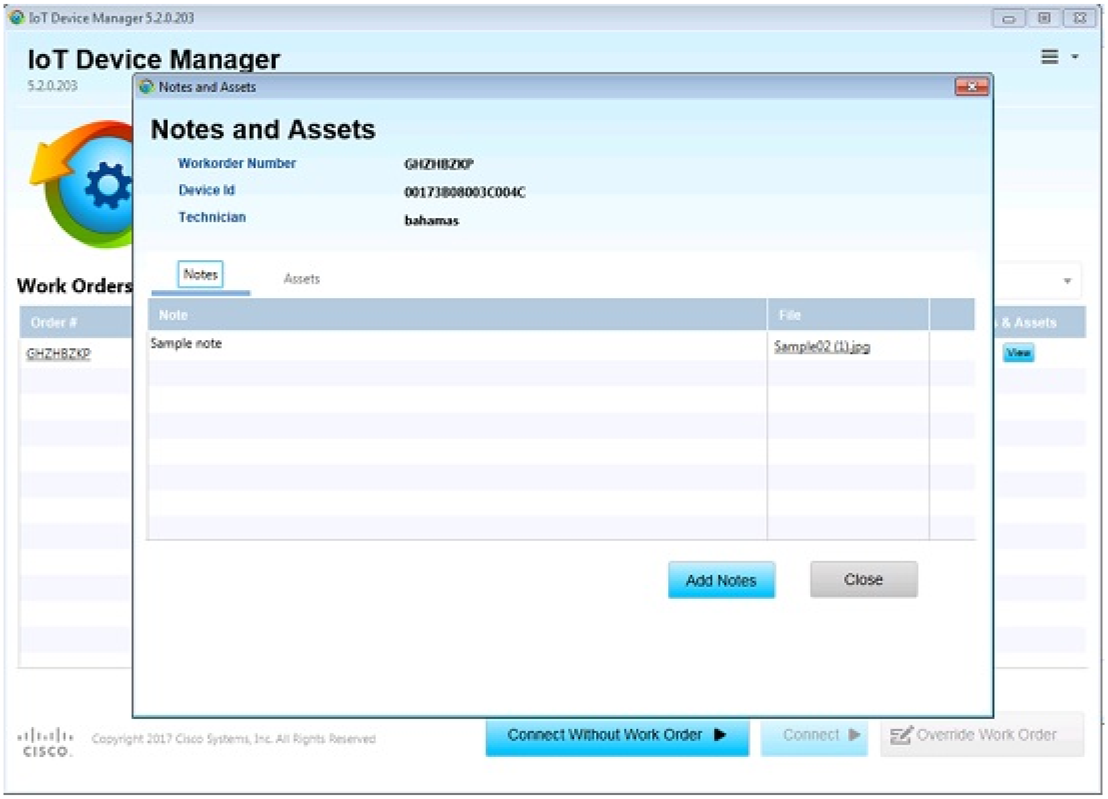
Last Synced

Tuesday, December 5, 2017 12:42:56 AM PST

Work Orders

Order #	Description	Device Model	Start Date	Time Remaini...	Status	Device Name	Notes & Assets
GHZHBZKP	Sample work order	IR500	Tuesday, Decem...	14 Day(s)	● New	00173B08003C004C	View

Step 3 The Notes and Assets window displays, which contains two tabs: **Notes** and **Assets**.



Notes and Assets

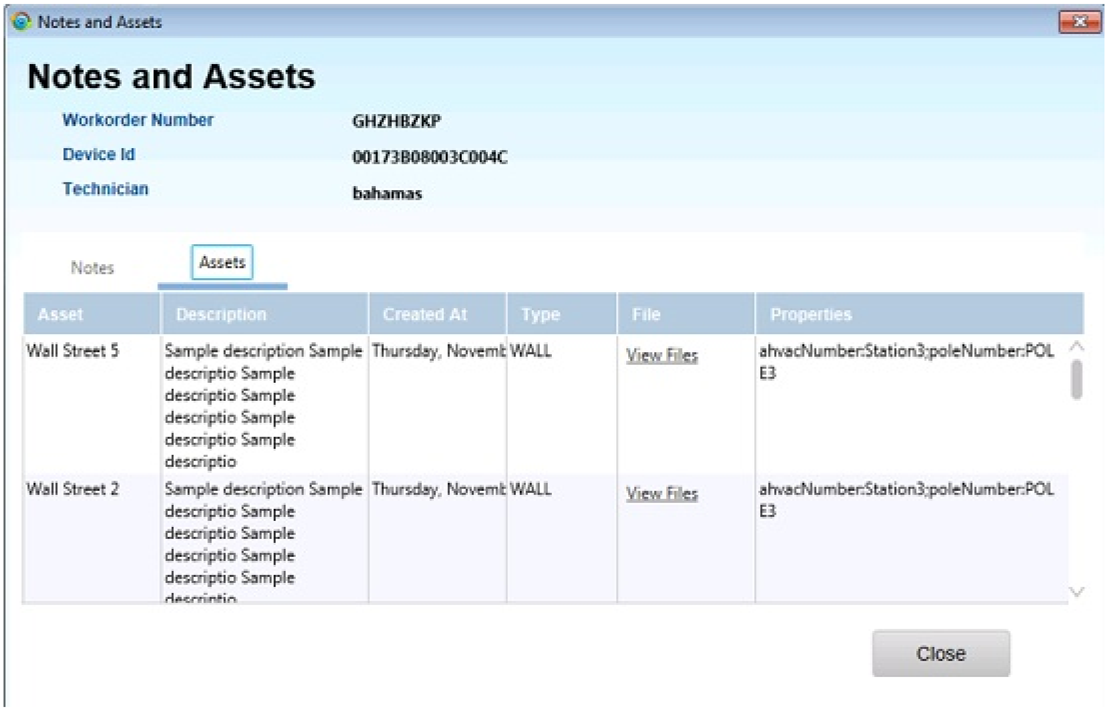
Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technician bahamas

Order #
GHZHBZKP

Note	File
Sample note	Sample02 (1).jpg



Notes and Assets

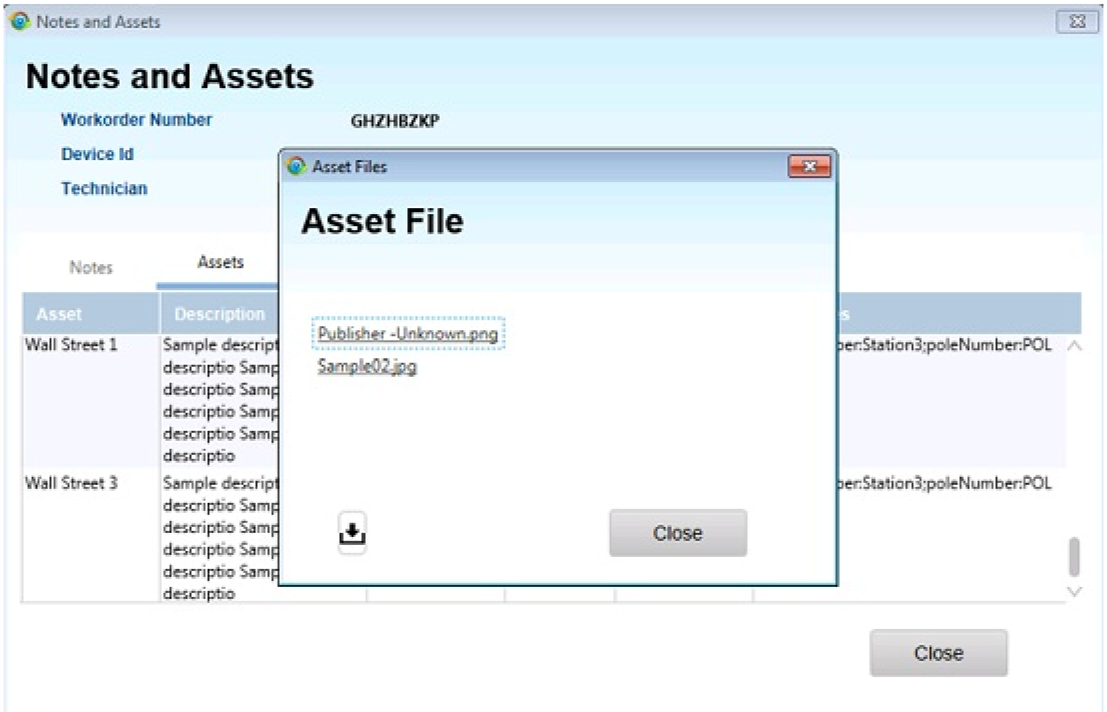
Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technician bahamas

Asset	Description	Created At	Type	File	Properties
Wall Street 5	Sample description Sample descriptio Sample descriptio Sample descriptio Sample descriptio Sample descriptio	Thursday, Novemb	WALL	View Files	ahvacNumber:Station3;poleNumber:POLE3
Wall Street 2	Sample description Sample descriptio Sample descriptio Sample descriptio Sample descriptio Sample descriptio	Thursday, Novemb	WALL	View Files	ahvacNumber:Station3;poleNumber:POLE3

Step 4 On the **Assets** tab,click **View Files** to display the files for the assets. Files can be downloaded either by clicking on the file or clicking the download button.


Notes and Assets

Workorder Number GHZHBZKP

Device Id

Technician

Asset	Description
Wall Street 1	Sample descript descriptio Samp descriptio Samp descriptio Samp descriptio Samp descriptio
Wall Street 3	Sample descript descriptio Samp descriptio Samp descriptio Samp descriptio Samp descriptio

per:Station3;poleNumber:POL

per:Station3;poleNumber:POL

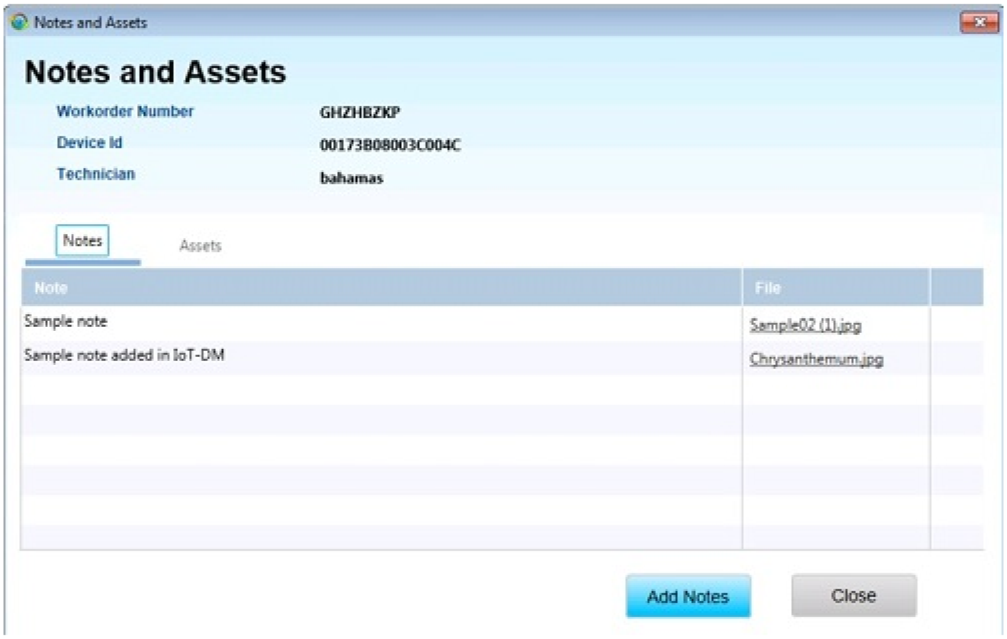
Asset Files

Asset File

Publisher -Unknown.png

Sample02.jpg

Step 5 On the **Notes** tab, click the file name to download the notes.


Notes and Assets

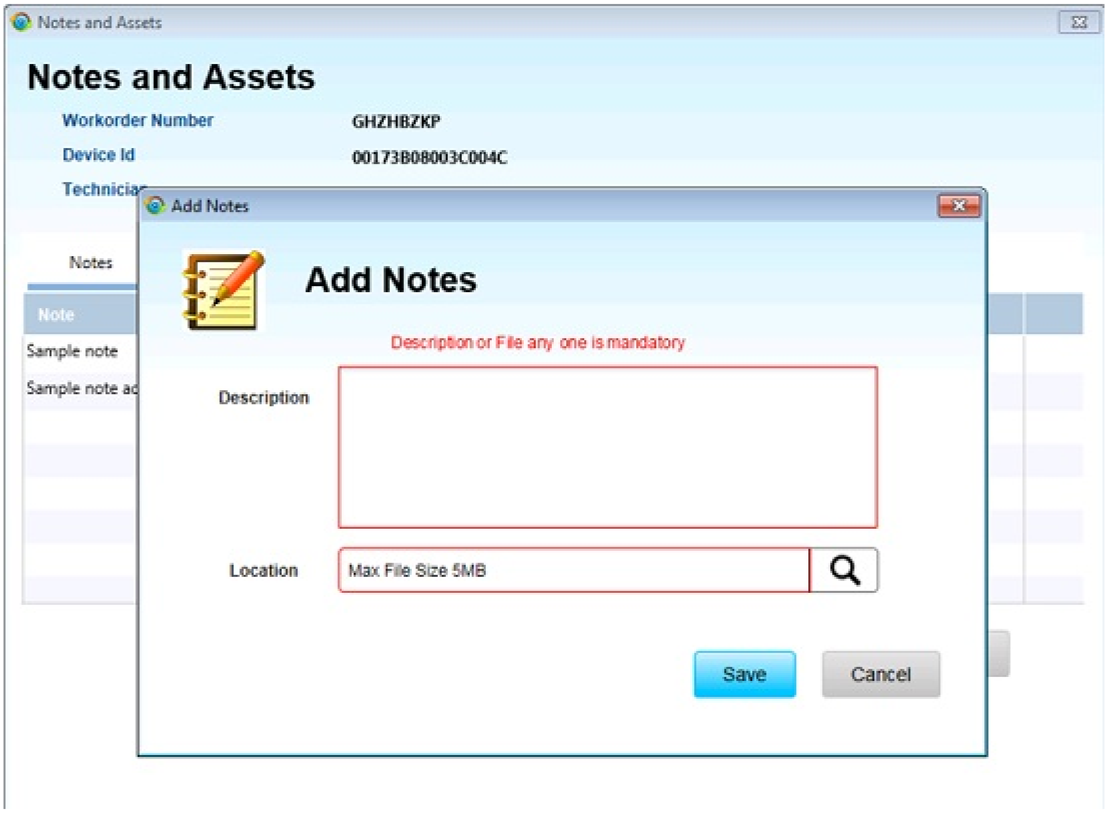
Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technician bahamas

Note	File
Sample note	Sample02 (1).jpg
Sample note added in IoT-DM	Chrysanthemum.jpg

Step 6 Click **Add Notes** on the **Notes** tab. The **Add Notes** pop-up window appears. Add note description and upload a file, then click the **Save** button. Either Description or File is mandatory. The notes added on IoT-DM can be deleted before the sync with IoT FND, by clicking the Recycle Bin icon.



Notes and Assets

Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technicia

Sample note

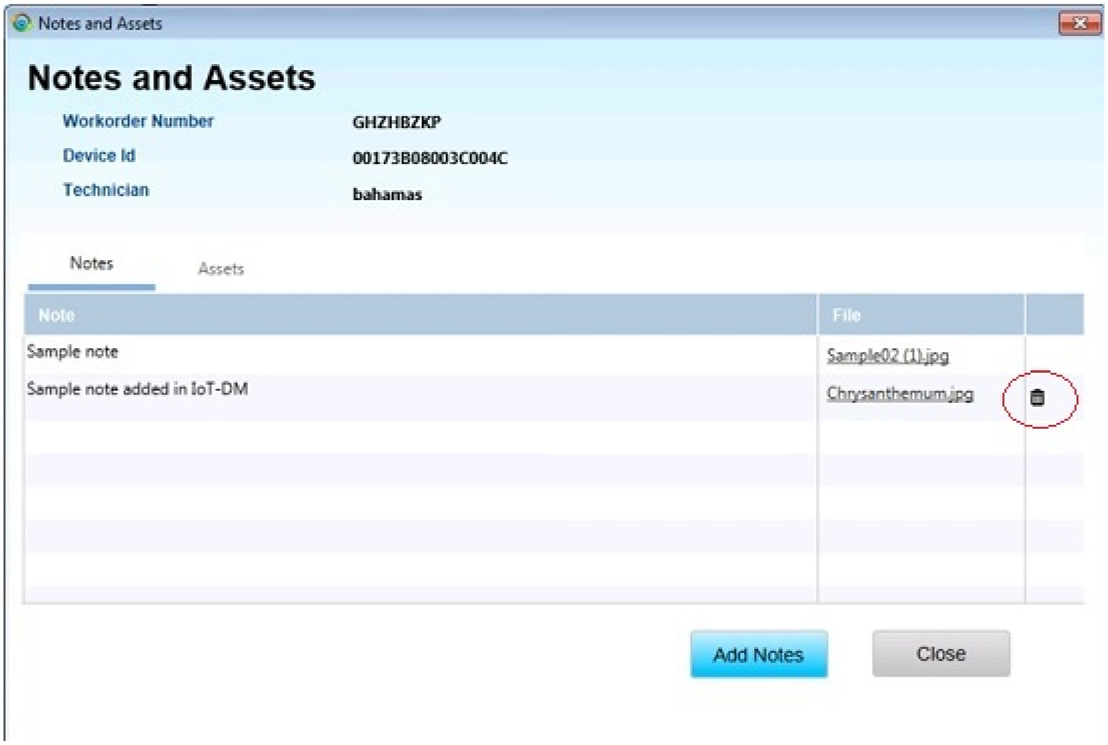
Sample note ad

Add Notes

Description or File any one is mandatory

Description

Location Max File Size 5MB



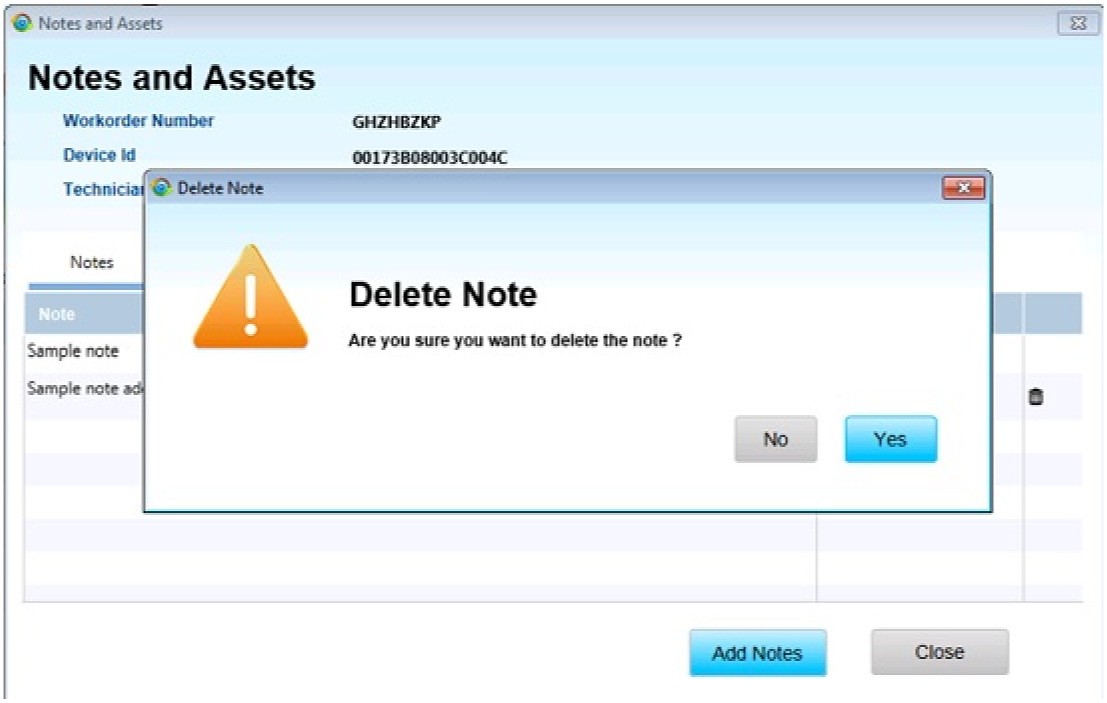
Notes and Assets

Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technician bahamas

Note	File	
Sample note	Sample02 (1).jpg	
Sample note added in IoT-DM	Chrysanthemum.jpg	🗑



Workorder Number GHZHBZKP

Device Id 00173B08003C004C

Technicia

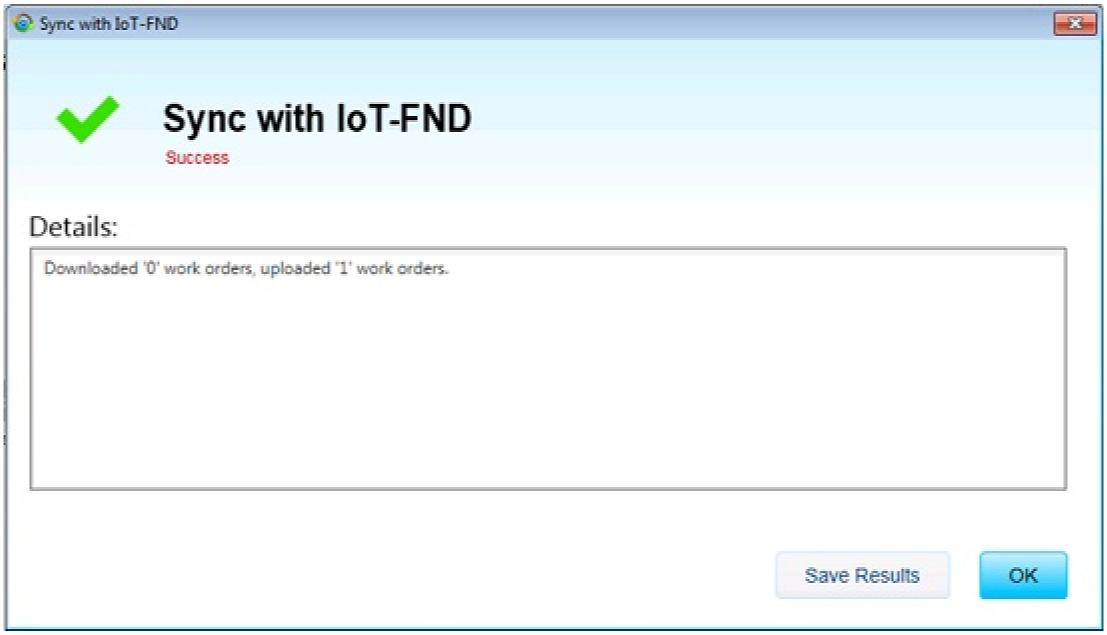
Sample note

Sample note ad

Delete Note

Are you sure you want to delete the note ?

Step 7 Click **Sync with IoT FND** to sync work orders with IoT-FND.



Success

Downloaded '0' work orders, uploaded '1' work orders.

CHAPTER 4

Performing Tasks on the CGR 1000

The chapter explains how to use the Device Manager to perform tasks on the CGR 1000.

Connecting to the CGR 1000

You can use Device Manager in the following ways:

- Operating with IoT-FND——When you have IoT-FND operating in the network, you can connect to that system with Device Manager to download and update work orders. Work orders allow Device Manager to view status and perform tasks on the CGR 1000. To operate in conjunction with IoT-FND, follow the steps in Setting Up the IoT-FND Connection.

- Operating without IoT-FND—When you do not have IoT-FND operating in the network or do not want to connect to that system, use Device Manager to connect directly to a CGR 1000 by either WiFi (with valid SSID and passphrase) or Ethernet to view status and perform tasks on the CGR 1000.

Connecting to the Router with a Work Order

Before connecting to the router with a work order, you should be familiar with the information in Managing Work Orders.

To connect to the router with a work order, select a work order from the list on the Device Manager opening page and click **Connect**.

Note The IR809 must have IPv6 option enabled to connect with work order.

Manually Connecting to the Router

You can connect to a CGR 1000 by either Ethernet or WiFi. WiFi connectivity ensures WPA Layer 2 security on data traffic between Device Manager and the router, after association and the key handshake complete. The Ethernet connection is secured by HTTPS only.

Connect to the Device Manager by employing one of the following methods:

- Auto Discovered IPv6 address (preferred method for the field)
- IPv4 address (such as 128.128.128.128)
- IPv6 address (such as fe80::d81f:6402:2ae4:4ea8)

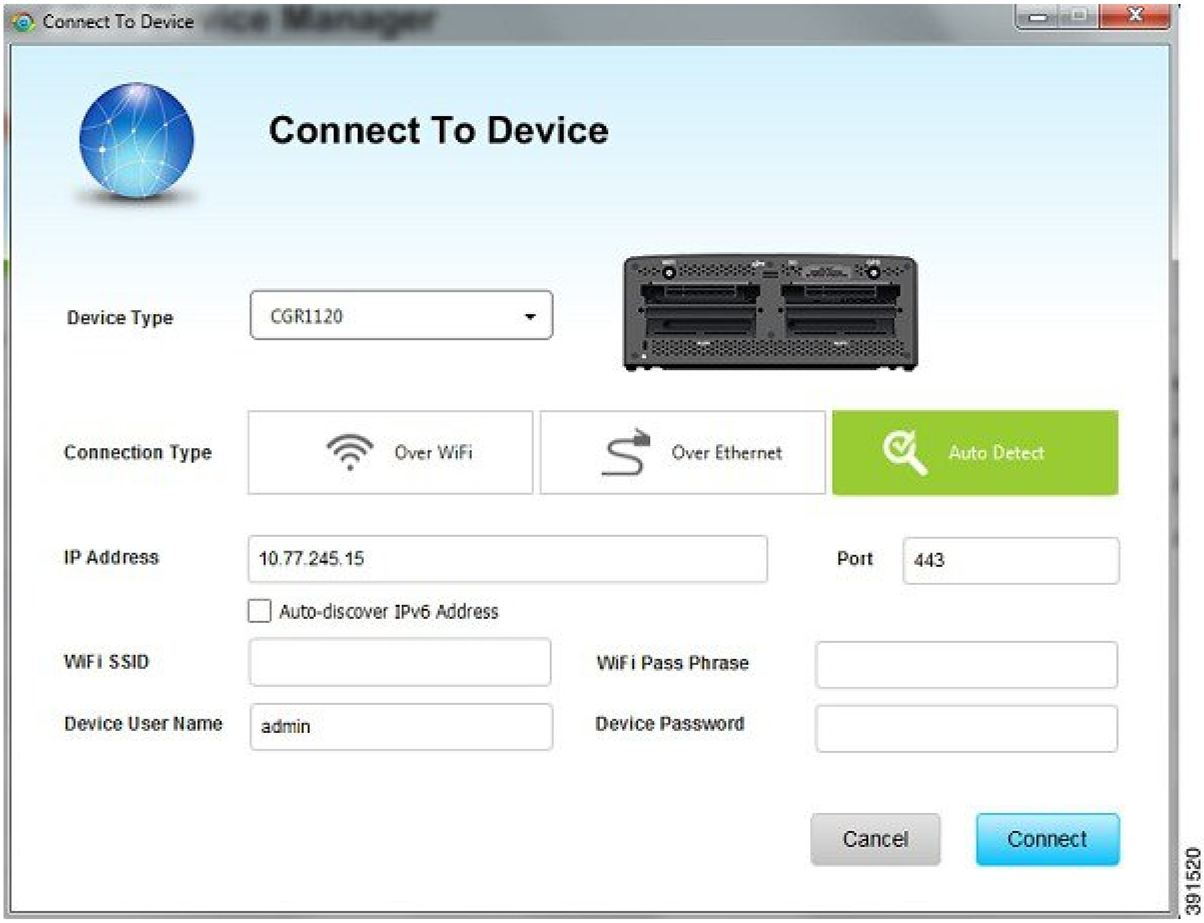
To connect to the Device Manager manually:

SUMMARY STEPS

1. On the Device Manager opening page, click **Connect Without Work Order**.
2. In the Connect to Device dialog box, select the Device Type: **CGR1120** or **CGR1240**.
3. Select the Connection Type: **Over WiFi**, **Over Ethernet**, or **Auto Detect**.
4. Enter the router IP address and port, or select the check box to auto-discover the IP address.
5. (WiFi only) Enter the SSID and pass phrase.
6. Enter the user name and password.
7. Click **Connect**. The Device Manager main page appears.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Connect Without Work Order**.



Connect To Device

Device Type: CGR1120

Connection Type: Over WiFi | Over Ethernet | [✓ Auto Detect]

IP Address: 10.77.245.15

Port: 443

□ Auto-discover IPv6 Address

WiFi SSID:

WiFi Pass Phrase:

Device User Name: admin

Device Password:

Step 2 In the Connect to Device dialog box, select the Device Type: **CGR1120** or **CGR1240**.

Step 3 Select the Connection Type: **Over WiFi**, **Over Ethernet**, or **Auto Detect**.

Step 4 Enter the router IP address and port, or select the check box to auto-discover the IP address.

Note To Auto Discover an IPv6 address, the laptop running Device Manager must be directly connected to the CGR 1000 via Ethernet or WiFi. By design, the Auto Discover function works when there is only one active router within the same network.

Step 5 (WiFi only) Enter the SSID and pass phrase.

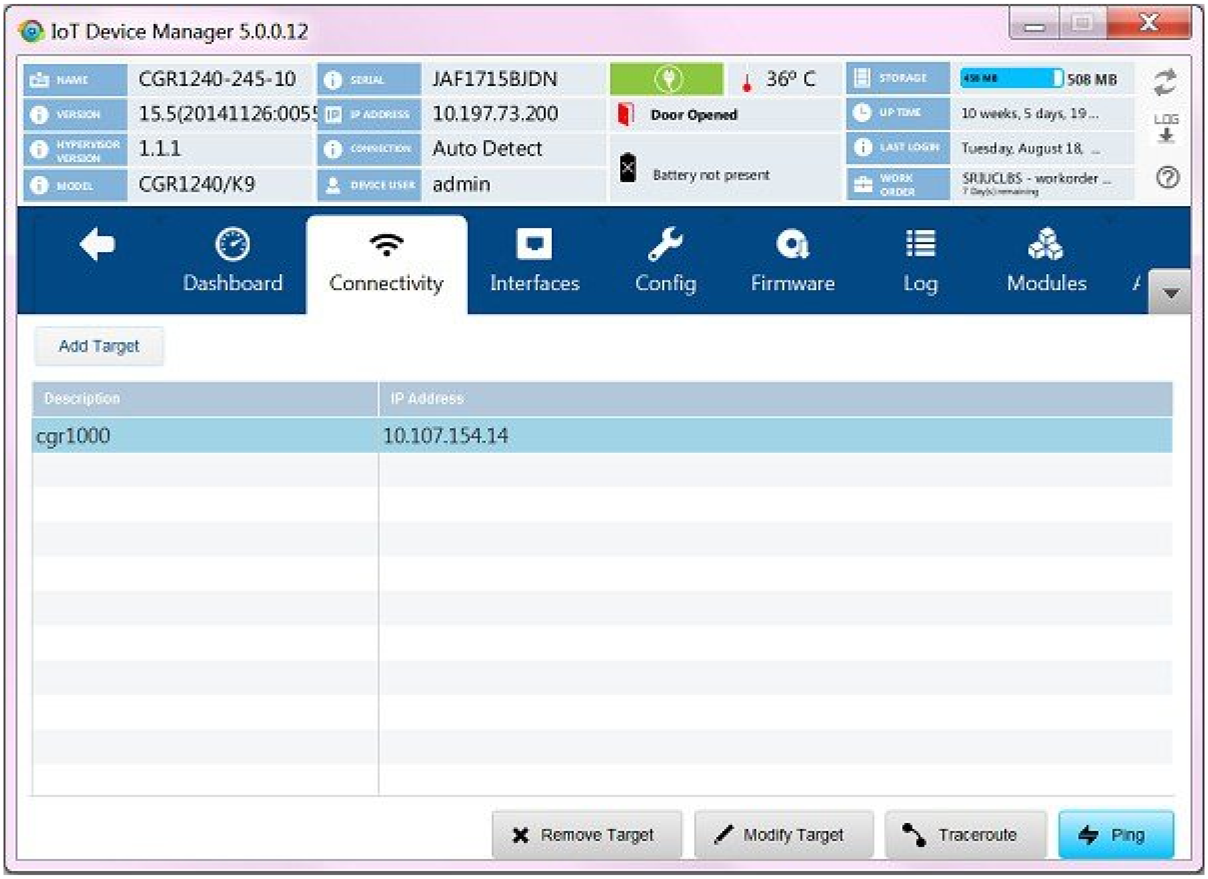
Step 6 Enter the user name and password.

Step 7 Click **Connect**. The Device Manager main page appears.

Testing Connectivity

You can confirm connectivity to a device from the CGR 1000 through the Connectivity page.

Before you can check a device connection or route to a CGR 1000, you must add the IPv4 or IPv6 address or hostname of the device (connection target) to Device Manager. All work orders have connection targets.



NAME	CGR1240-245-10	SERIAL	JAF1715BJDN
VERSION	15.5(20141126:0055	IP ADDRESS	10.197.73.200
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect
MODEL	CGR1240/K9	DEVICE USER	admin

36° C
Door Opened
Battery not present

STORAGE	508 MB
UP TIME	10 weeks, 5 days, 19 ...
LAST LOGIN	Tuesday, August 18, ...
WORK ORDER	SRJUCLBS - workorder ...

Description	IP Address
cgr1000	10.107.154.14

Adding a Device IP Address

To add a device IP address:

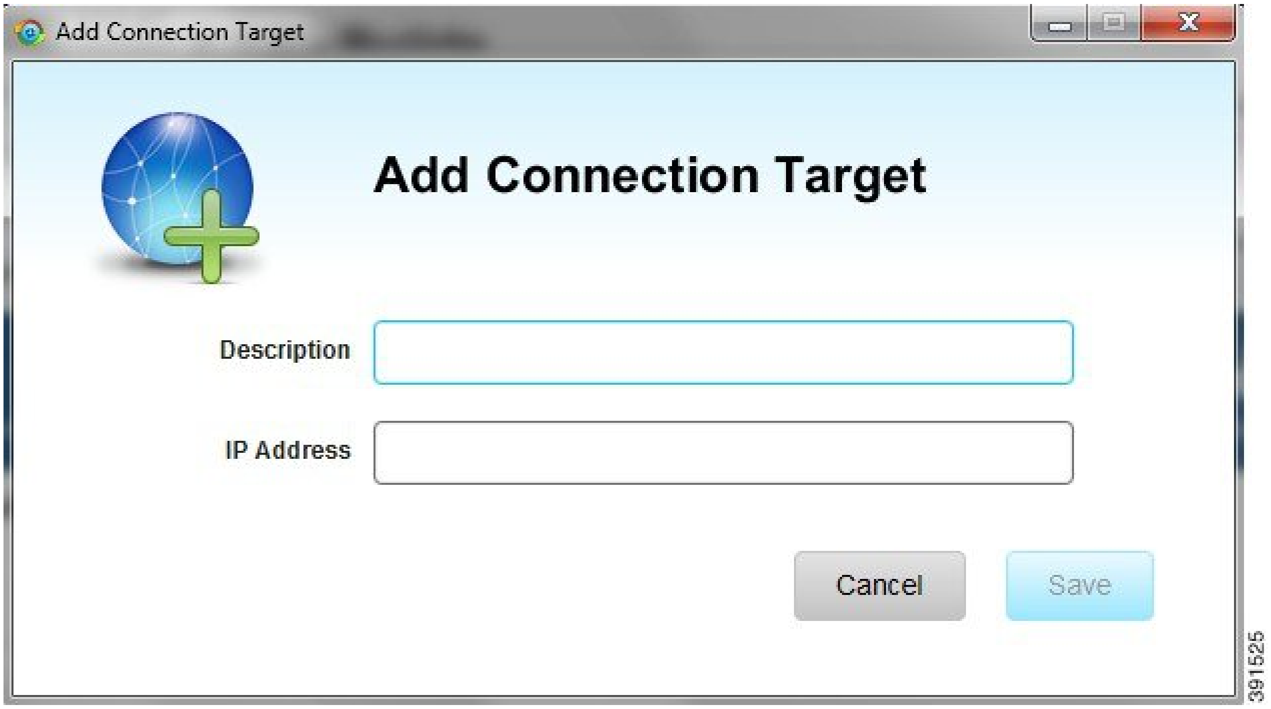
SUMMARY STEPS

1. On the Device Manager main page, click the **Connectivity** tab.
2. On the Connectivity page, click **Add Target** to create a new target.
3. In the Description field, enter a description for the device.
4. In the IP Address field, enter the IP address (IPv4 or IPv6) of the device.
5. Click **Save**. You can now test the connectivity to the device you just added to the Device Manager.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Connectivity** tab.

Step 2 On the Connectivity page, click **Add Target** to create a new target.



Step 3 In the Description field, enter a description for the device.

Step 4 In the IP Address field, enter the IP address (IPv4 or IPv6) of the device.

Step 5 Click **Save**. You can now test the connectivity to the device you just added to the Device Manager.

Pinging a Device IP Address

The Ping feature allows you to verify connectivity to a device by querying the target IP address.

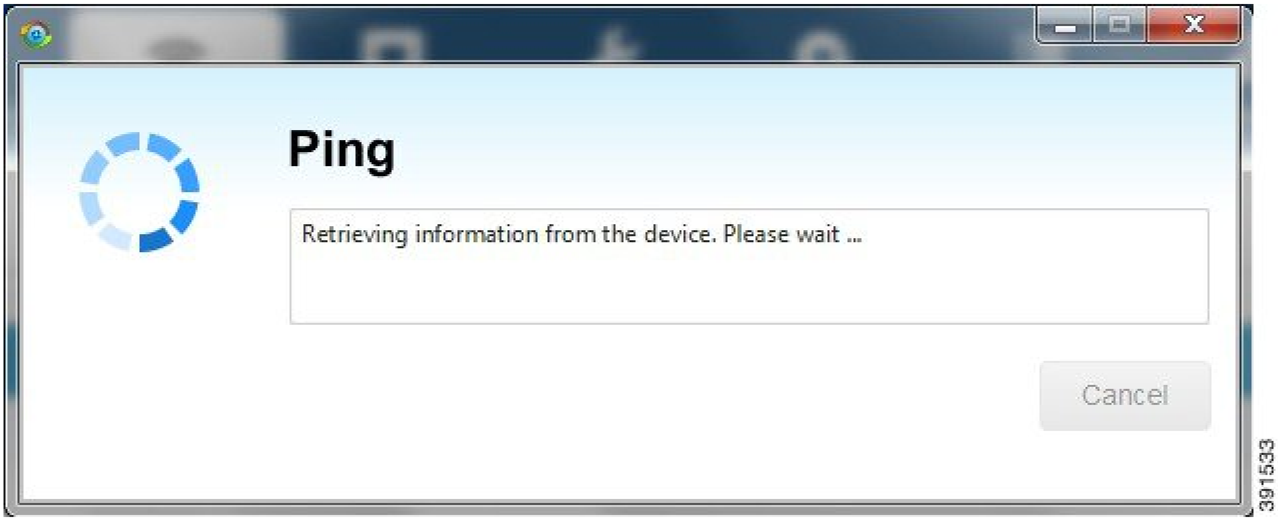
To test connectivity between the router and the device:

SUMMARY STEPS

1. On the Connectivity page, select the connection target and click **Ping**. A dialog box appears indicating that the router is attempting to ping the target IP address.
2. Click **OK** to close the Ping dialog box.

DETAILED STEPS

Step 1 On the Connectivity page, select the connection target and click **Ping**. A dialog box appears indicating that the router is attempting to ping the target IP address.



Ping

Retrieving information from the device. Please wait ...

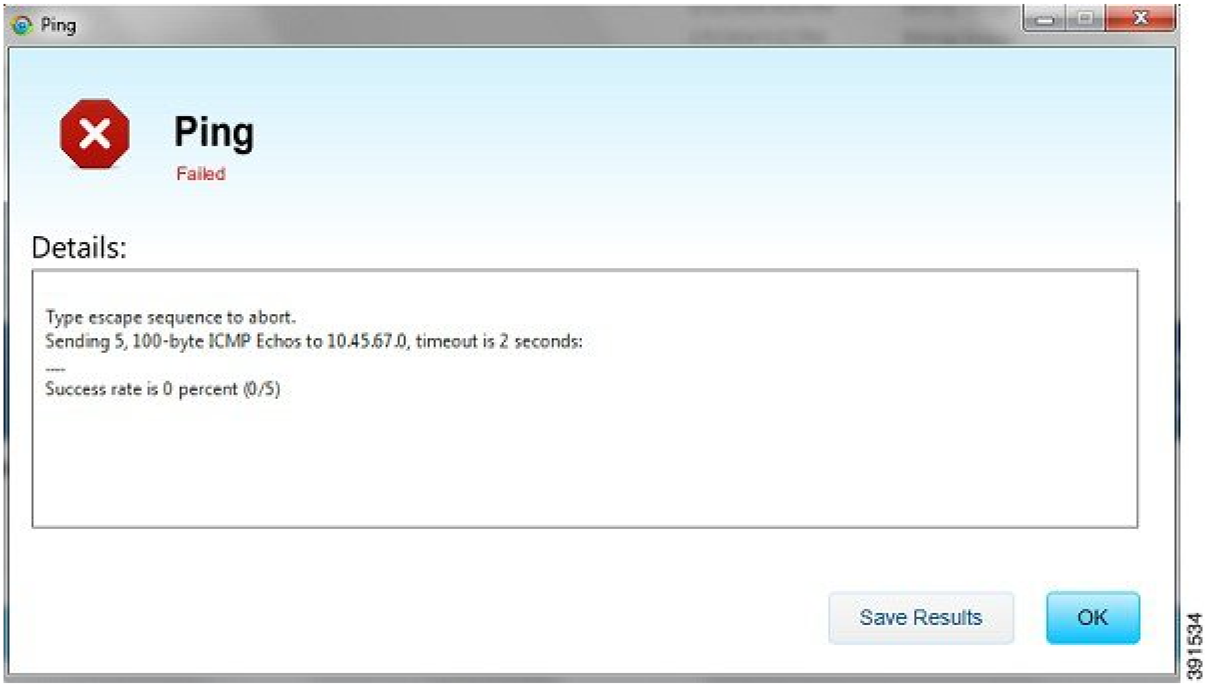
When the system successfully pings the device, a dialog box appears indicating that the ping was successful.

If the system does not successfully ping a device, refer to Failed Ping, on page 42.

Step 2 Click **OK** to close the Ping dialog box.

Failed Ping

If the system does not successfully ping a device, a message appears showing the details of the failed ping attempt.



Ping

Failed

Details:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.45.67.0, timeout is 2 seconds:
-----
Success rate is 0 percent (0/5)
```

SUMMARY STEPS

1. In the Ping error dialog box, review the reason for the error, then click **OK** or **Save Results** to save the output to a file on the laptop.
2. Proceed to Tracing the Route of a Device IP Address, on page 43.

DETAILED STEPS

Step 1 In the Ping error dialog box, review the reason for the error, then click **OK** or **Save Results** to save the output to a file on the laptop.

Step 2 Proceed to Tracing the Route of a Device IP Address, on page 43.

Tracing the Route of a Device IP Address

When an IP address cannot be reached using Ping, you can use the Trace Route feature to check the route taken to reach the device IP address.

To trace the route of the IP address:

SUMMARY STEPS

1. On the Connectivity page, click **Trace Route** for the listed connection target.
2. If the trace route is successful, review the details and click **Save Results** or **OK** in the Trace Route dialog box.
3. If the trace route is unsuccessful, proceed to Deleting or Editing a Device IP Address, on page 43.

DETAILED STEPS

Step 1 On the Connectivity page, click **Trace Route** for the listed connection target.

Step 2 If the trace route is successful, review the details and click **Save Results** or **OK** in the Trace Route dialog box.

Step 3 If the trace route is unsuccessful, proceed to Deleting or Editing a Device IP Address, on page 43.

Deleting or Editing a Device IP Address

After you have tested a target IP address and verified its connectivity, you can delete the device entry from the Device Manager. You can also delete or edit an IP address that the application identifies as incorrect during failed pings and trace route attempts.

To delete or edit a target IP address:

SUMMARY STEPS

1. On the Connectivity page, select the listed connection target, and click **Delete** to remove the device from the list.
2. To edit the device’s IP address, click **Modify Target**.

3. In the Modify Connection Target dialog box, edit the IP address and click **Save**.

DETAILED STEPS

Step 1 On the Connectivity page, select the listed connection target, and click **Delete** to remove the device from the list.

Step 2 To edit the device's IP address, click **Modify Target**.

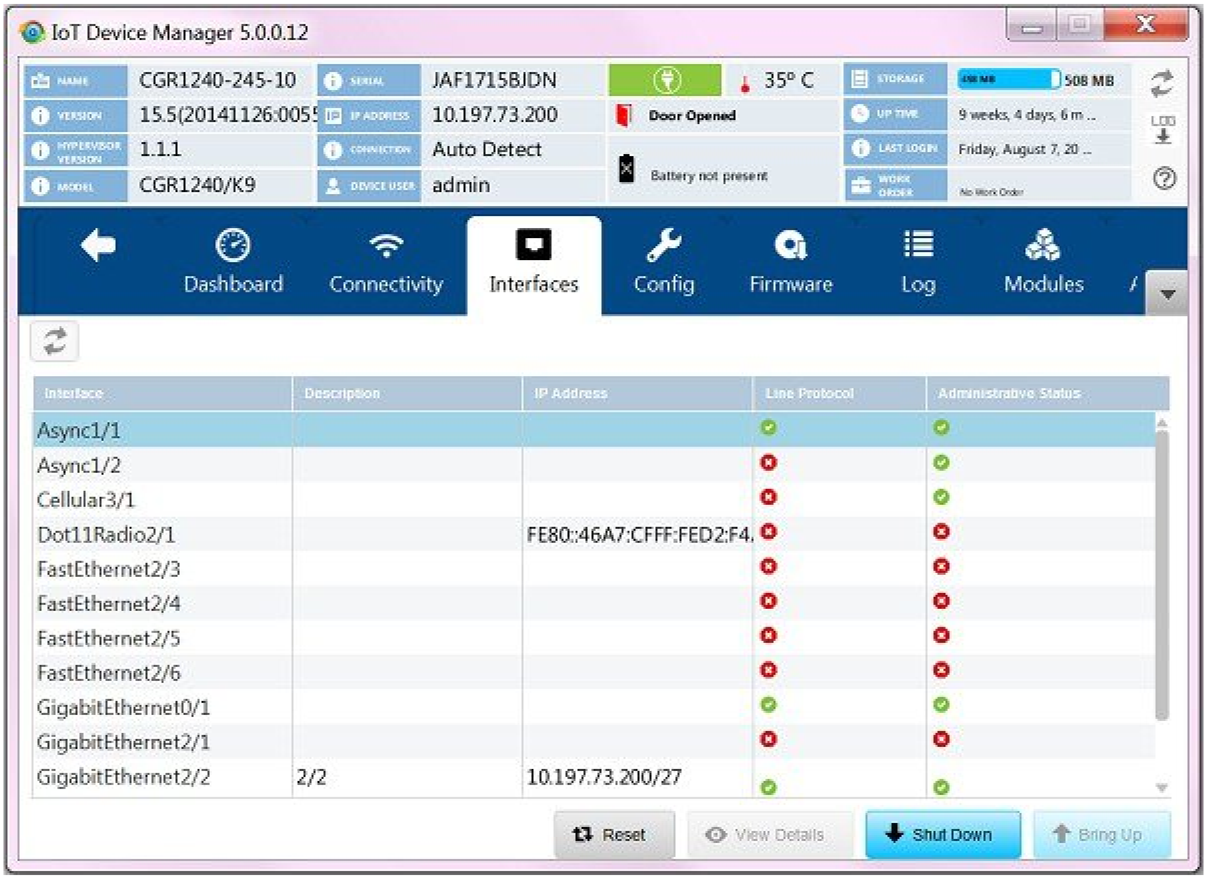
Step 3 In the Modify Connection Target dialog box, edit the IP address and click **Save**.

Managing Interfaces

You can bring up or shut down an interface on the Interfaces page. You can also reset an interface and view interface details.

- When the line protocol for an interface is *up* (a green check mark), the line protocol is currently active. When the line protocol for an interface is *down* (a red cross), it means the line protocol is not active.
- When the administrative status for an interface is *up* (a green check mark), the administrator brought up the interface. When the administrative status for an interface is *down* (a red cross), the administrator took down the interface.

All interfaces installed within the CGR 1000 display automatically.



IoT Device Manager 5.0.0.12

NAME	CGR1240-245-10	SERIAL	JAF1715BJDN		35° C	STORAGE	508 MB
VERSION	15.5(20141126:005	IP ADDRESS	10.197.73.200	Door Opened		UP TIME	9 weeks, 4 days, 6 m ...
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect	Battery not present		LAST LOGIN	Friday, August 7, 20 ...
MODEL	CGR1240/K9	DEVICE USER	admin			WORK ORDER	No Work Order

Interface	Description	IP Address	Line Protocol	Administrative Status
Async1/1			✓	✓
Async1/2			✗	✓
Cellular3/1			✗	✓
Dot11Radio2/1		FE80::46A7:CFFF:FED2:F4,	✗	✗
FastEthernet2/3			✗	✗
FastEthernet2/4			✗	✗
FastEthernet2/5			✗	✗
FastEthernet2/6			✗	✗
GigabitEthernet0/1			✓	✓
GigabitEthernet2/1			✗	✗
GigabitEthernet2/2	2/2	10.197.73.200/27	✓	✓

Resetting an Interface

Resetting an interface shuts it down and then brings it up. To reset an interface:

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Reset**.
3. In the Reset Interface dialog box, click **Yes** to confirm the reset.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Reset**.

Step 3 In the Reset Interface dialog box, click **Yes** to confirm the reset.

Viewing Details for an Interface

Select an interface and click **View Details** to display information including interface status, settings, and dynamic statistics. Information is updated every 5 seconds.

Note In this release, details are available for the 3G (cellular*x* /1), 4G LTE (cellular*x* /1), and WiMAX (Dot16Radio*x* /1) interfaces.

The following details are available for the cellular interface:

- Received Signal Strength Indicator (RSSI) (chart)
- Modem status
- Settings (IMSI, IMEI, Cell ID, and APN)

The following details are available for the WiMAX interface:

- RSSI (chart)
- Carrier to Interference-plus-Noise Ratio (CINR) (chart)
- Settings (Hardware Address, Hardware Version, Microcode Version, Firmware Version, Device Name, Link State, Frequency, and Bandwidth)

To view details for an interface:

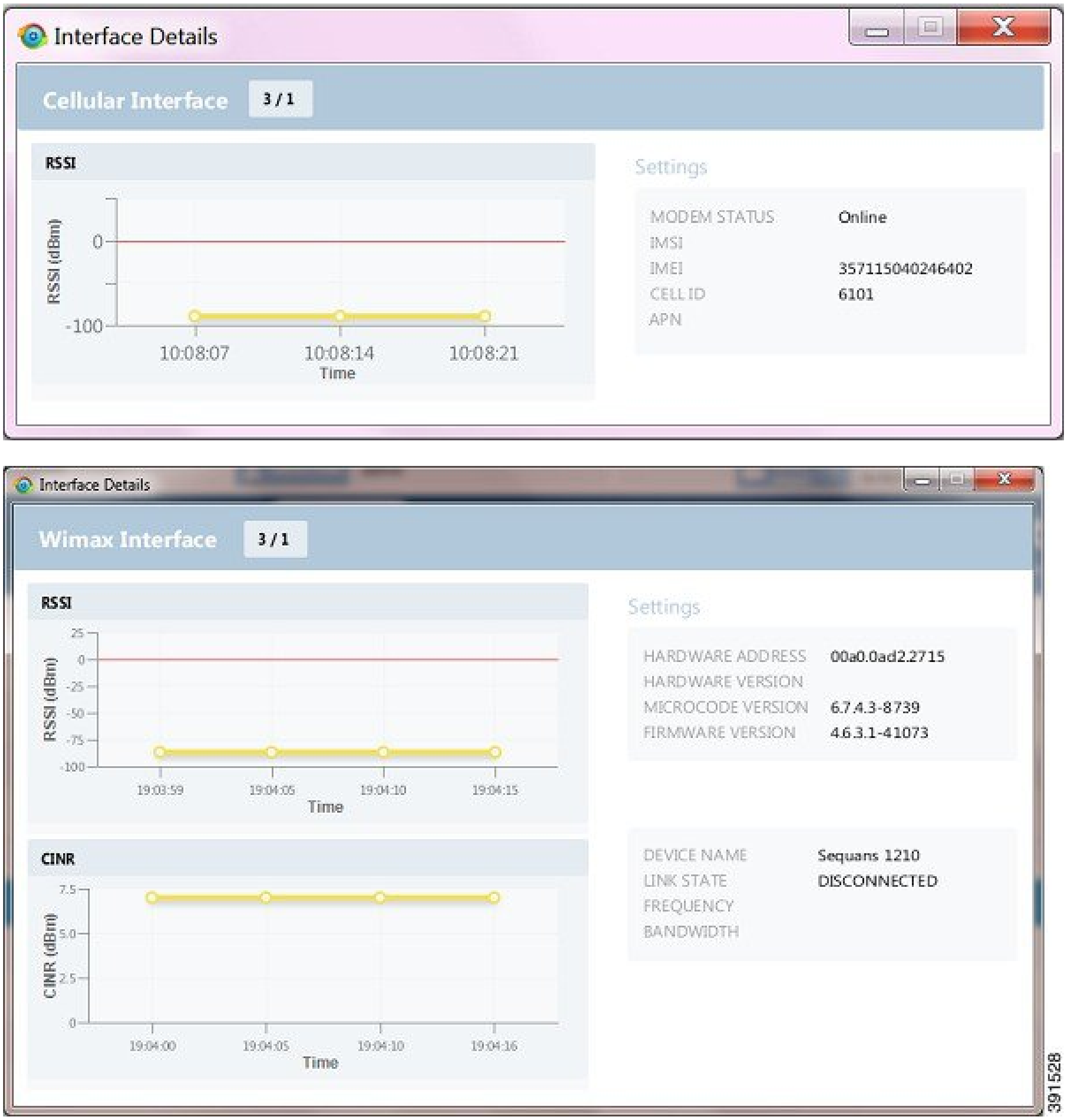
SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **View Details**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **View Details**.



Cellular Interface 3 / 1

Settings

MODEM STATUS	Online
IMSI	
IMEI	357115040246402
CELL ID	6101
APN	

Wimax Interface 3 / 1

Settings

HARDWARE ADDRESS	00a0.0ad2.2715
HARDWARE VERSION	
MICROCODE VERSION	6.7.4.3-8739
FIRMWARE VERSION	4.6.3.1-41073

DEVICE NAME	Sequans 1210
LINK STATE	DISCONNECTED
FREQUENCY	
BANDWIDTH	

Bringing Up an Interface

When an interface is shut down for any reason, you can attempt to bring up the interface.

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Bring Up**.

3. In the Bring Up interface dialog box, click **Yes** to confirm bringing up the interface.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Bring Up**.

Step 3 In the Bring Up interface dialog box, click **Yes** to confirm bringing up the interface.

Shutting Down an Interface

Note You cannot shut down the interface on which the Device Manager communicates with the CGR 1000 because the connection would be lost.

To shut down an interface:

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Shut Down**.
3. In the Shut Down interface dialog box, click **Yes** to confirm shutting down the interface.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Shut Down**.

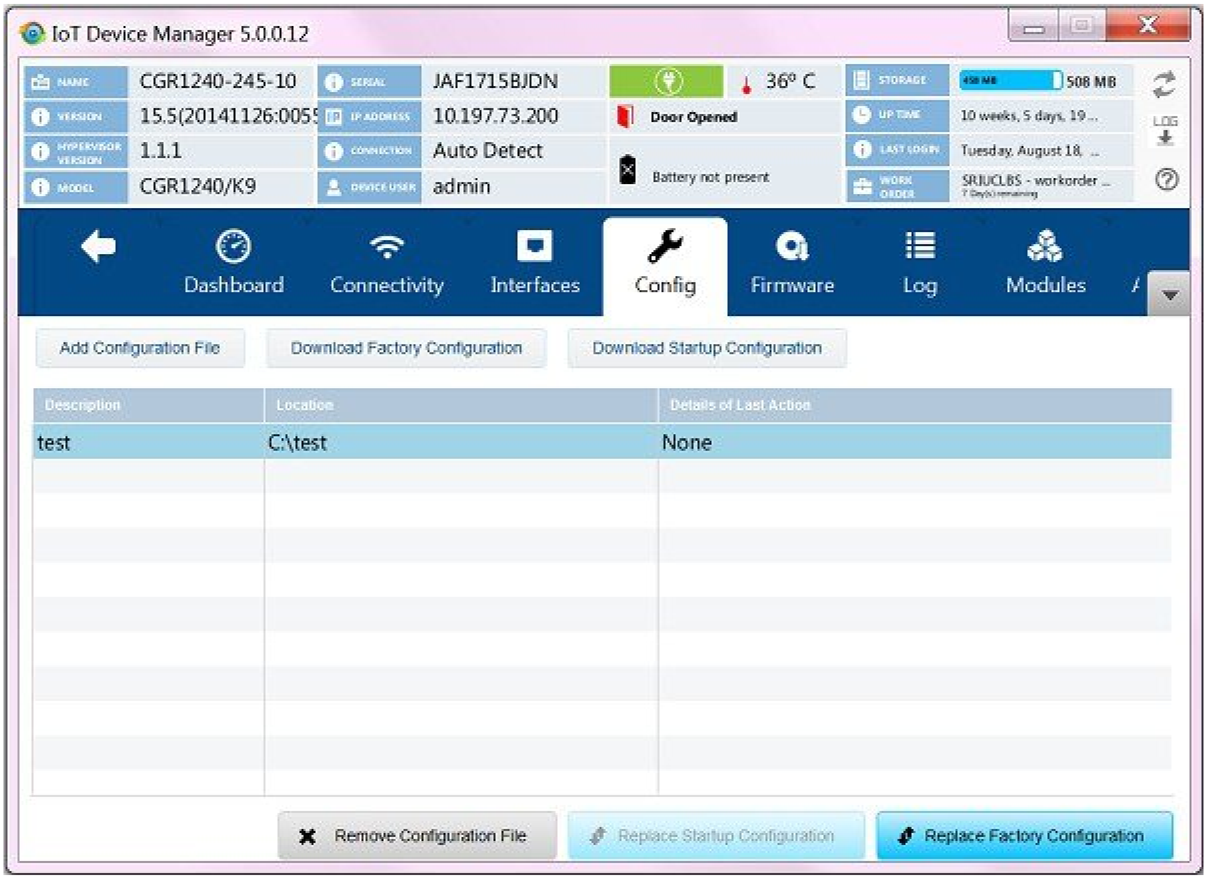
Step 3 In the Shut Down interface dialog box, click **Yes** to confirm shutting down the interface.

Changing the Configuration

You can upload a router configuration file to the Device Manager and then use that file to replace the startup configuration or the express setup (factory configuration) of the CGR 1000. (For more information about the configuration file, see Managing Configuration Files Configuration Guide, Cisco IOS Release 15M&T .)

Note In NMS mode, you can replace only the factory configuration. In non-NMS mode, you can replace both the startup and factory configuration.

You can also download the factory or startup configuration file from the router to your laptop.



IoT Device Manager 5.0.0.12

NAME	CGR1240-245-10	SERIAL	JAF1715BJDN
VERSION	15.5(20141126:0055	IP ADDRESS	10.197.73.200
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect
MODEL	CGR1240/K9	DEVICE USER	admin

36° C
Door Opened
Battery not present

STORAGE	458 MB 508 MB
UP TIME	10 weeks, 5 days, 19 ...
LAST LOGIN	Tuesday, August 18, ...
WORK ORDER	SRJUCLBS - workorder ...

Description	Location	Details of Last Action
test	C:\test	None

LOG
Dashboard
Connectivity
Interfaces
Config
Firmware
Log
Modules
Add Configuration File
Download Factory Configuration
Download Startup Configuration
Remove Configuration File
Replace Startup Configuration
Replace Factory Configuration

Adding a Configuration File

To add a configuration file to Device Manager:

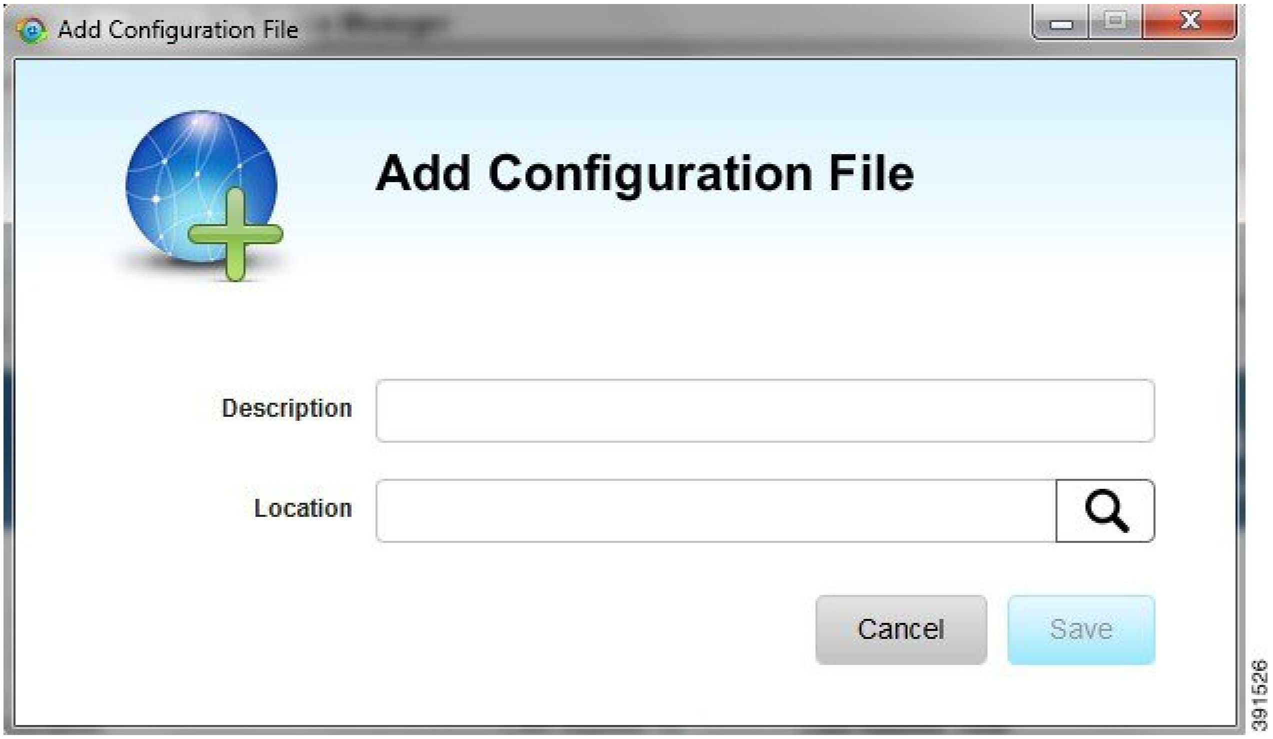
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Add Configuration File**.
3. In the Add Configuration File dialog box:

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click **Add Configuration File**.



Step 3 In the Add Configuration File dialog box:

a) Enter a description for the configuration file that you are going to upload.

b) Click **Search** to navigate to the configuration file location and select the file.

c) Click **Save**.

The file you selected is listed on the Config page.

Downloading a Configuration File

To download the factory configuration file or the startup configuration file to the Device Manager laptop:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Download Factory Configuration** or **Download Startup Configuration**.
3. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click **Download Factory Configuration** or **Download Startup Configuration**.

Step 3 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Replacing a Configuration File

After you add a configuration file to Device Manager (see Adding a Configuration File, on page 49), you can find the file name listed on the Config page. You can use the file to update the startup configuration or the express setup (factory configuration).

⚠ **Caution** Replacing the configuration file causes the router to reboot. All connections to the router are lost during the update. After this task starts, there is no way to cancel the event. Be careful when using this feature.

To replace the configuration file on the router:

SUMMARY STEPS

1. On the Config page, select the configuration file that you want to install and click **Replace Startup Configuration** or **Replace Factory Configuration**.
2. In the confirmation dialog box, click **Yes** to begin installing the router configuration file.

DETAILED STEPS

Step 1 On the Config page, select the configuration file that you want to install and click **Replace Startup Configuration** or **Replace Factory Configuration**.

Step 2 In the confirmation dialog box, click **Yes** to begin installing the router configuration file.

If an error message appears, the file did not upload to the router. Proceed to Removing a Configuration File, on page 51.

Removing a Configuration File

After you update the router with the new configuration file, you can remove the file from Device Manager. You can also use this function to remove unwanted or duplicate configuration files.

To remove a configuration file:

SUMMARY STEPS

1. On the Config page, select the configuration file you want to remove from the list.
2. Click **Remove Configuration File**.
3. In the dialog box that appears, click **Yes** to remove the file.

DETAILED STEPS

Step 1 On the Config page, select the configuration file you want to remove from the list.

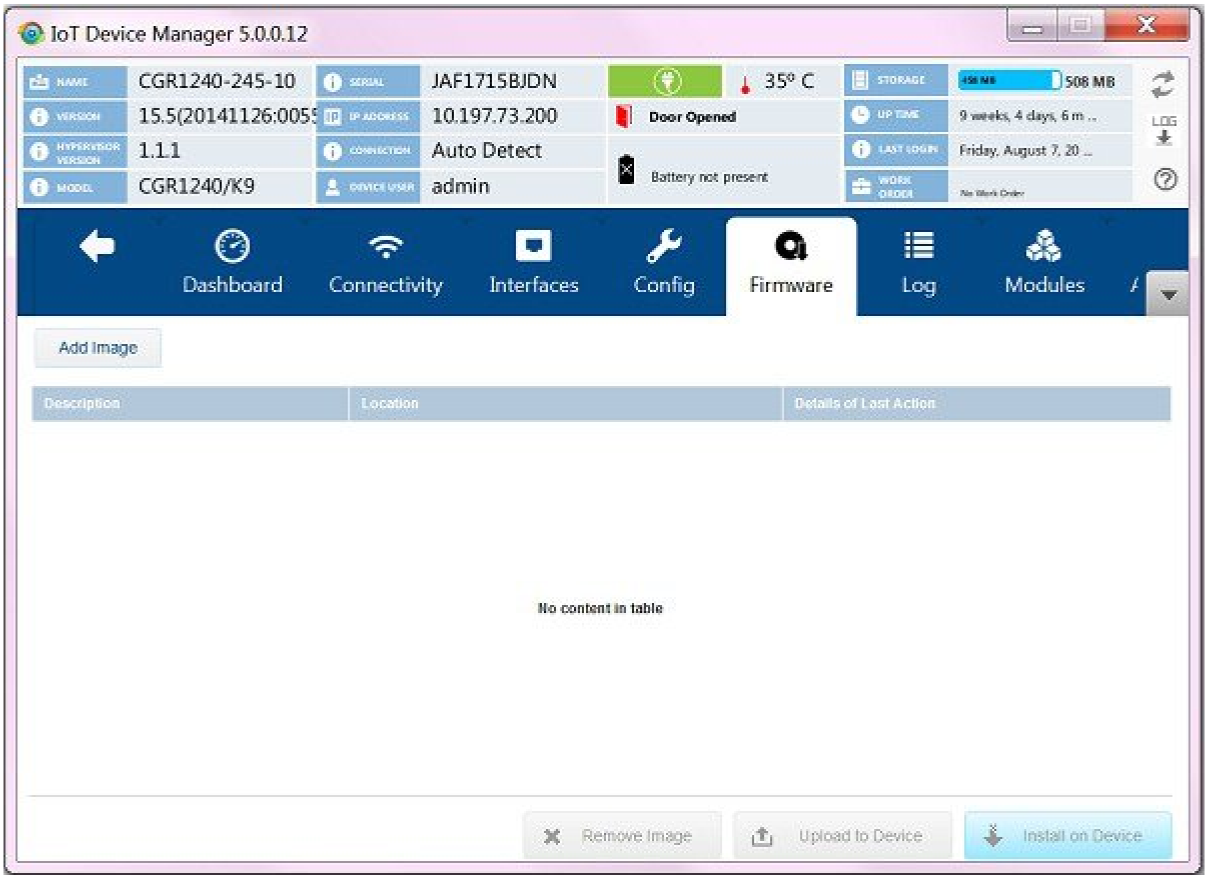
Step 2 Click **Remove Configuration File**.

Step 3 In the dialog box that appears, click **Yes** to remove the file.

Updating the Firmware Image

The CGR 1000 image bundle contains information that the router uses when starting up and operating. The information in the image contains information on FPGA, 3G, 4G LTE, wireless drivers, and so on. The only acceptable file format for the Cisco CGR 1000 image file is a zip bundle, which contains a manifest file with information on versioning and files. Any missing files in the zip bundle cancels the update. You can find the official Cisco CGR 1000 zip bundle on Cisco.com:

https://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/tsd-products-support-series-home.html



IoT Device Manager 5.0.0.12

NAME	CGR1240-245-10	SERIAL	JAF1715BJDN		35° C	STORAGE	458 MB 508 MB
VERSION	15.5(20141126:0055	IP ADDRESS	10.197.73.200	Door Opened		UP TIME	9 weeks, 4 days, 6 m ...
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect	Battery not present		LAST LOGIN	Friday, August 7, 20 ...
MODEL	CGR1240/K9	DEVICE USER	admin			WORK ORDER	No Work Order

Adding an Image

To add an image file to Device Manager:

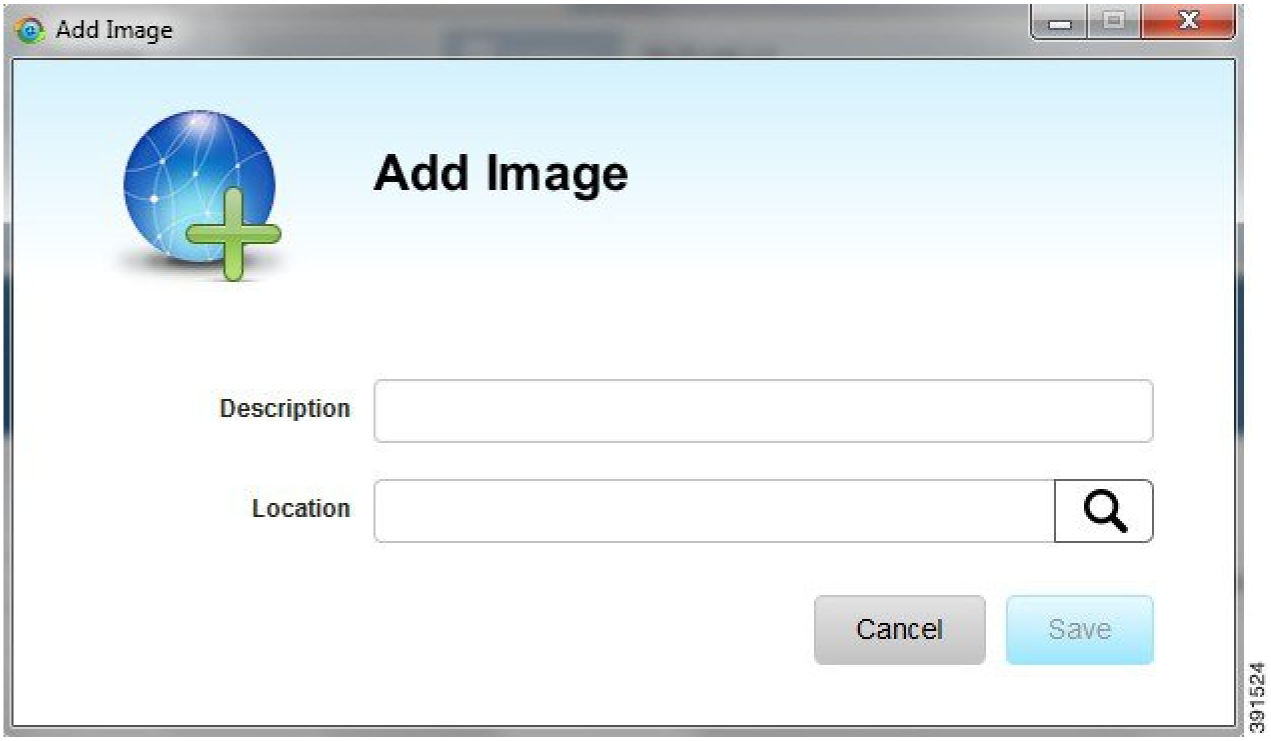
SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. Click **Add Image**.
3. In the Add Image dialog box:

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 Click **Add Image**.



Step 3 In the Add Image dialog box:

a) Enter a description for the image that you are going to upload.
b) Click **Search** to navigate to the image file location and select the file.
c) Click **Save**.

The file you select appears on the Firmware page.

Uploading an Image to the Router

The **Upload to Device** option allows you to upload and store a copy of a firmware image on the router without initiating an immediate image install. This capability allows operations personnel to use IoT-FND or a utility management tool to install and reboot the router when network conditions allow.

To upload an image to the router:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. If the firmware image that you want to install on the router is not listed on the Firmware page, add the image (see Adding an Image, on page 52).
3. On the Firmware page, select the router firmware image that you want to upload and click **Upload to Device**. The new image is stored on the router until you are ready to install the image on the router. (See Installing an Image, on page 54.)

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 If the firmware image that you want to install on the router is not listed on the Firmware page, add the image (see Adding an Image, on page 52).

Step 3 On the Firmware page, select the router firmware image that you want to upload and click **Upload to Device**. The new image is stored on the router until you are ready to install the image on the router. (See Installing an Image, on page 54.)

Installing an Image

⚠

Caution Be careful when using this feature. After this tasks starts, there is no way to cancel the event. Updating the router firmware image might take a while to complete and requires a reboot. All connections to the router are unavailable during the image update.

To install an image:

SUMMARY STEPS

1. On the Firmware page, select the image file to install and click **Install on Device**.
2. In the dialog box that appears, click **Yes** to exclude Guest OS from the installation.
3. If you click Yes, Guest OS will not be upgraded.
4. If the firmware image already exists in the router, you are prompted to confirm reinstalling the same image.
5. In the confirmation dialog box, click **Yes** to begin the install process. After the router firmware update completes, the router reboots.

DETAILED STEPS

Step 1 On the Firmware page, select the image file to install and click **Install on Device**.

Step 2 In the dialog box that appears, click **Yes** to exclude Guest OS from the installation.

Step 3 If you click Yes, Guest OS will not be upgraded.

Step 4 If the firmware image already exists in the router, you are prompted to confirm reinstalling the same image.

Step 5 In the confirmation dialog box, click **Yes** to begin the install process. After the router firmware update completes, the router reboots.

Removing an Image

After you install an image, you can remove the image file from the Device Manager. You can also use the Remove image option to remove an image file.

To remove an image file:

SUMMARY STEPS

1. On the Update Image page, select a image.
2. Click **Remove Image**.
3. In the dialog box that appears, click **Yes** to remove the image. A message warns you if the image has not yet been installed on the router.

DETAILED STEPS

Step 1 On the Update Image page, select a image.

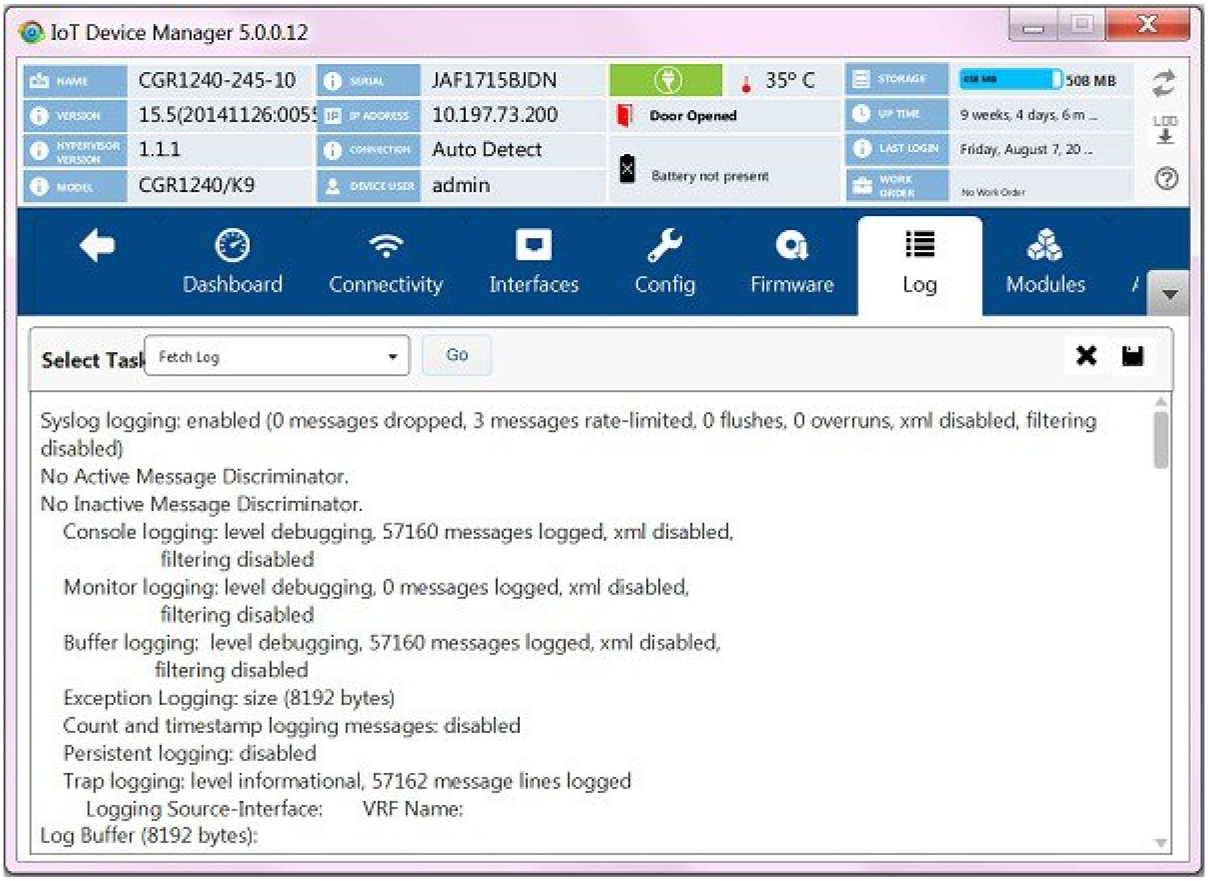
Step 2 Click **Remove Image**.

Step 3 In the dialog box that appears, click **Yes** to remove the image. A message warns you if the image has not yet been installed on the router.

Retrieving Logs

You can retrieve real-time log events from the CGR 1000 and view them on the Log page or save the information to a file.

You can specify either the system log or the tech support log for retrieval.



NAME CGR1240-245-10
VERSION 15.5(20141126:0055
HYPERVISOR VERSION 1.1.1
MODEL CGR1240/K9
SERIAL JAF1715BJDN
IP ADDRESS 10.197.73.200
CONNECTION Auto Detect
DEVICE USER admin
35° C
Door Opened
Battery not present
STORAGE 508 MB
UP TIME 9 weeks, 4 days, 6 m ...
LAST LOGIN Friday, August 7, 20 ...
WORK ORDER No Work Order

Select Task: Fetch Log

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering
disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
   Console logging: level debugging, 57160 messages logged, xml disabled,
                filtering disabled
   Monitor logging: level debugging, 0 messages logged, xml disabled,
                filtering disabled
   Buffer logging:  level debugging, 57160 messages logged, xml disabled,
                filtering disabled
   Exception Logging: size (8192 bytes)
   Count and timestamp logging messages: disabled
   Persistent logging: disabled
   Trap logging: level informational, 57162 message lines logged
      Logging Source-Interface:       VRF Name:
Log Buffer (8192 bytes):
```

Retrieving and Saving Logs

To retrieve real-time log events from the router:

SUMMARY STEPS

1. On the Device Manager main page, click the **Log tab**.
2. On the Log page, select the report retrieval task from the Select Task drop-down menu:
3. To save a copy of the retrieved log events displayed on the page, click Save.
4. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.
5. To clear the output, click the black cross.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Log tab**.

Step 2 On the Log page, select the report retrieval task from the Select Task drop-down menu:

- Fetch Log–Retrieves the output from the **show logging** command.
- Fetch Tech-Support–Retrieves the output from the **show tech-support** command.

Step 3 To save a copy of the retrieved log events displayed on the page, click Save.

Step 4 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Step 5 To clear the output, click the black cross.

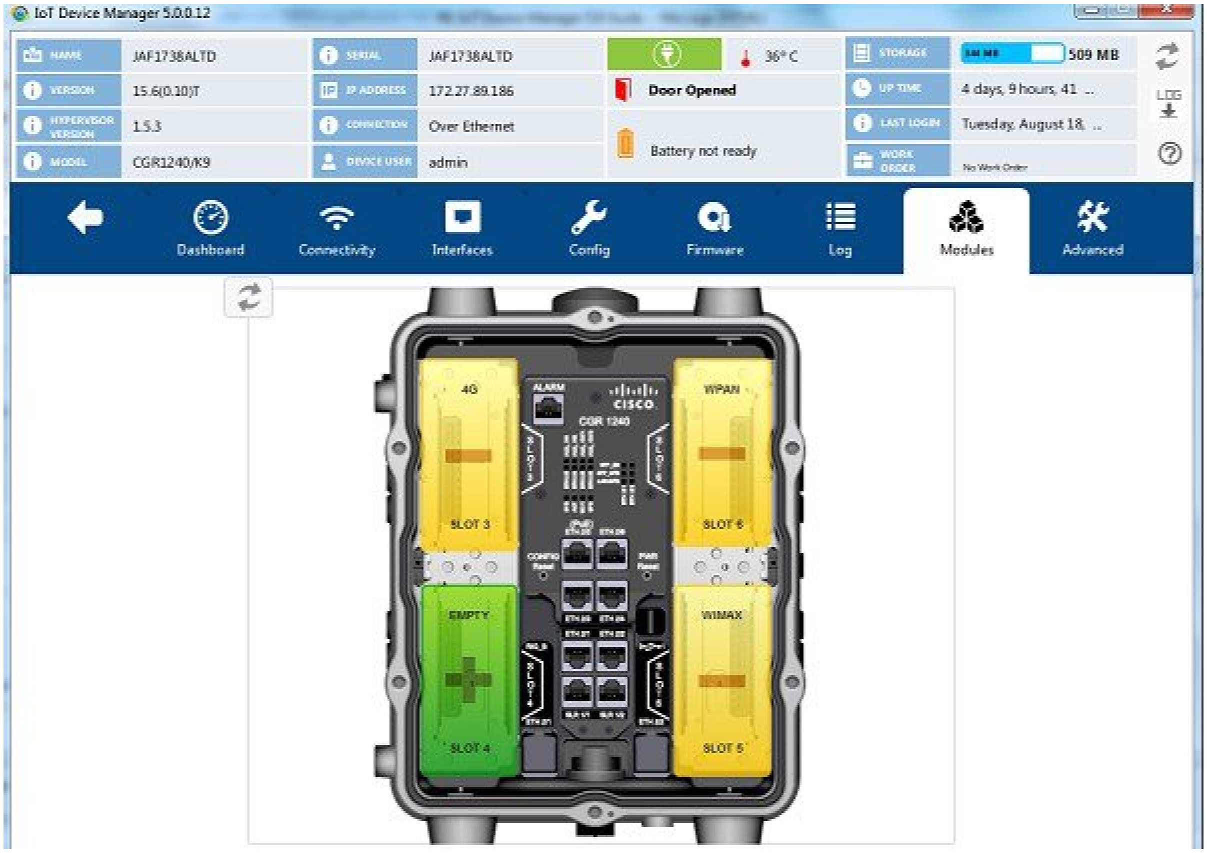
Managing Modules

The Modules page guides you through the process of inserting or removing modules on the CGR 1000.

You can determine the slot availability as follows:

- A green module with the plus sign (+) indicates an available slot.
- A yellow module with the minus sign (-) indicates an occupied slot.
- A gray module with the minus sign (-) indicates that module status is not UP (for example, power down).

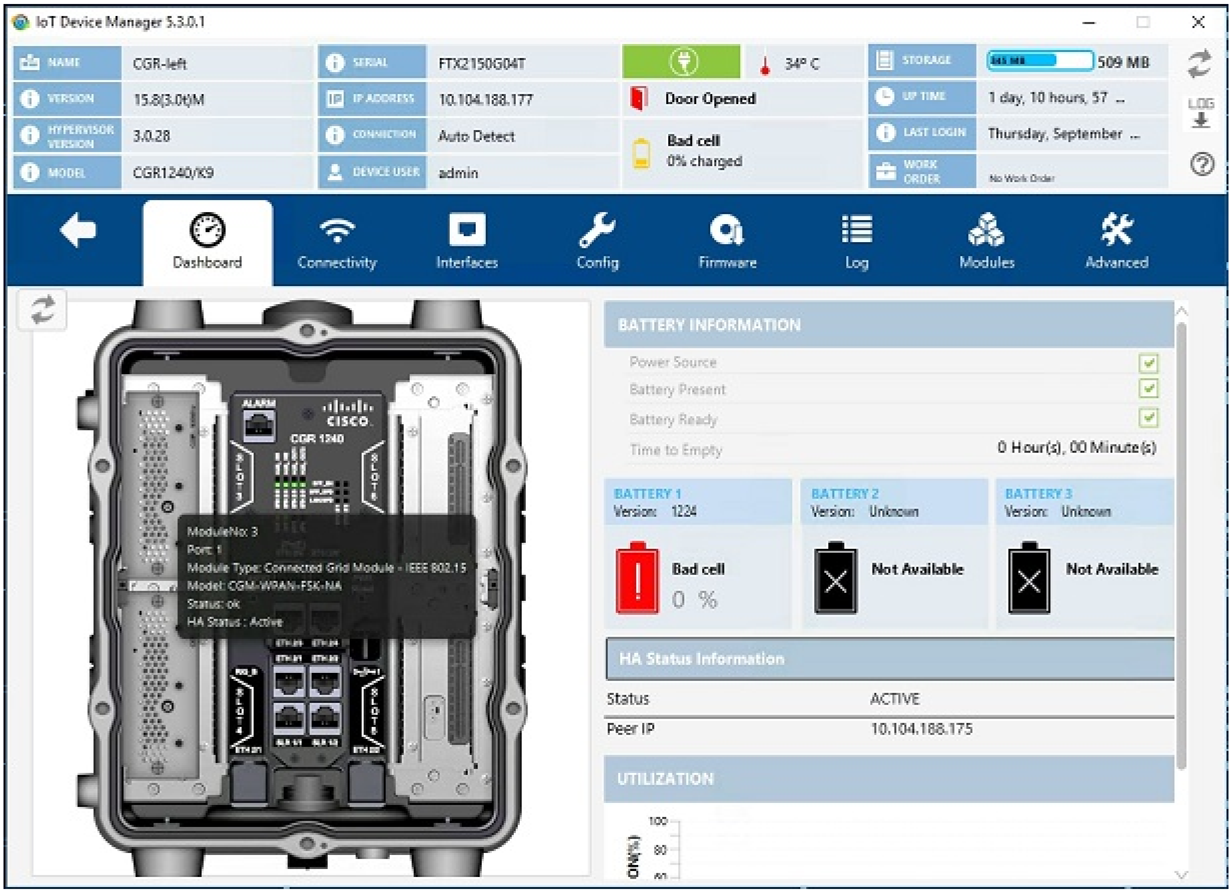
Note Hover the pointer over an occupied slot to display module details.



IoT Device Manager 5.0.0.12

NAME JAF1738ALTD
VERSION 15.6(0.10)T
HYPERVISOR VERSION 1.5.3
MODEL CGR1240/K9
SERIAL JAF1738ALTD
IP ADDRESS 172.27.89.186
CONNECTION Over Ethernet
DEVICE USER admin
36° C
Door Opened
Battery not ready
STORAGE 509 MB
UP TIME 4 days, 9 hours, 41 ...
LAST LOGIN Tuesday, August 18, ...
WORK ORDER No Work Order

For the modules of CGR 1240 series with firmware version 15.8 and above, when High Availability (HA) information is supported, CGR activation status and its peer address will be displayed in the Dashboard tab, as the following figure shows.



IoT Device Manager 5.3.0.1

NAME	CGR-left	SERIAL	FTX2150G04T		34° C	STORAGE	509 MB
VERSION	15.8(3.0t)M	IP ADDRESS	10.104.188.177	Door Opened		UP TIME	1 day, 10 hours, 57 ...
HYPERVISOR VERSION	3.0.28	CONNECTION	Auto Detect	Bad cell 0% charged		LAST LOGIN	Thursday, September ...
MODEL	CGR1240/K9	DEVICE USER	admin			WORK ORDER	No Work Order

ModuleNo: 3
Port: 1
Module Type: Connected Grid Module - IEEE 802.15
Model: CGM-WPAN-FSK-NA
Status: ok
HA Status : Active

BATTERY INFORMATION

Power Source	☑
Battery Present	☑
Battery Ready	☑
Time to Empty	0 Hour(s), 00 Minute(s)

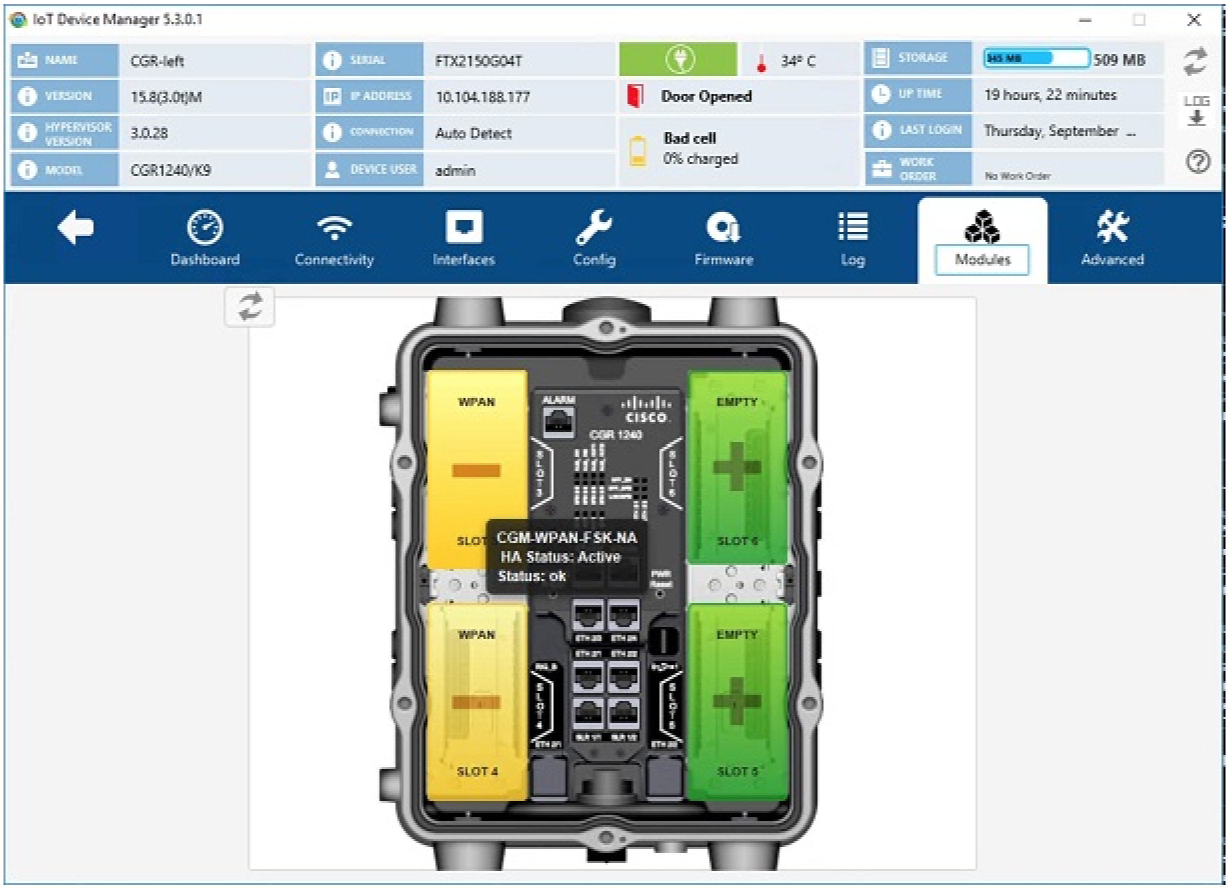
BATTERY 1	BATTERY 2	BATTERY 3
Version: 1224	Version: Unknown	Version: Unknown
Bad cell 0 %	Not Available	Not Available

HA Status Information

Status	ACTIVE
Peer IP	10.104.188.175

UTILIZATION

If you hover the curser on the WPAN slots under Dashboard and Modules tab, HA status will appear in the tooltip, as the following figure shows.



IoT Device Manager 5.3.0.1

NAME	CGR-left	SERIAL	FTX2150G04T		34° C	STORAGE	509 MB
VERSION	15.8(3.0t)M	IP ADDRESS	10.104.188.177	Door Opened		UP TIME	19 hours, 22 minutes
HYPERVISOR VERSION	3.0.28	CONNECTION	Auto Detect	Bad cell 0% charged		LAST LOGIN	Thursday, September ...
MODEL	CGR1240/K9	DEVICE USER	admin			WORK ORDER	No Work Order

CGM-WPAN-FSK-NA
HA Status: Active
Status: ok

Note For details on opening the chassis door of the CGR 1240, please refer to the “Opening the Router Chassis” chapter in the Cisco 1240 Connected Grid Router Hardware Installation Guide . For details on installing a specific module, refer to the Installation and Configuration Guide for that module at: http://www.cisco.com/go/cgr1000-docs .

Inserting a Module

To insert a module:

SUMMARY STEPS

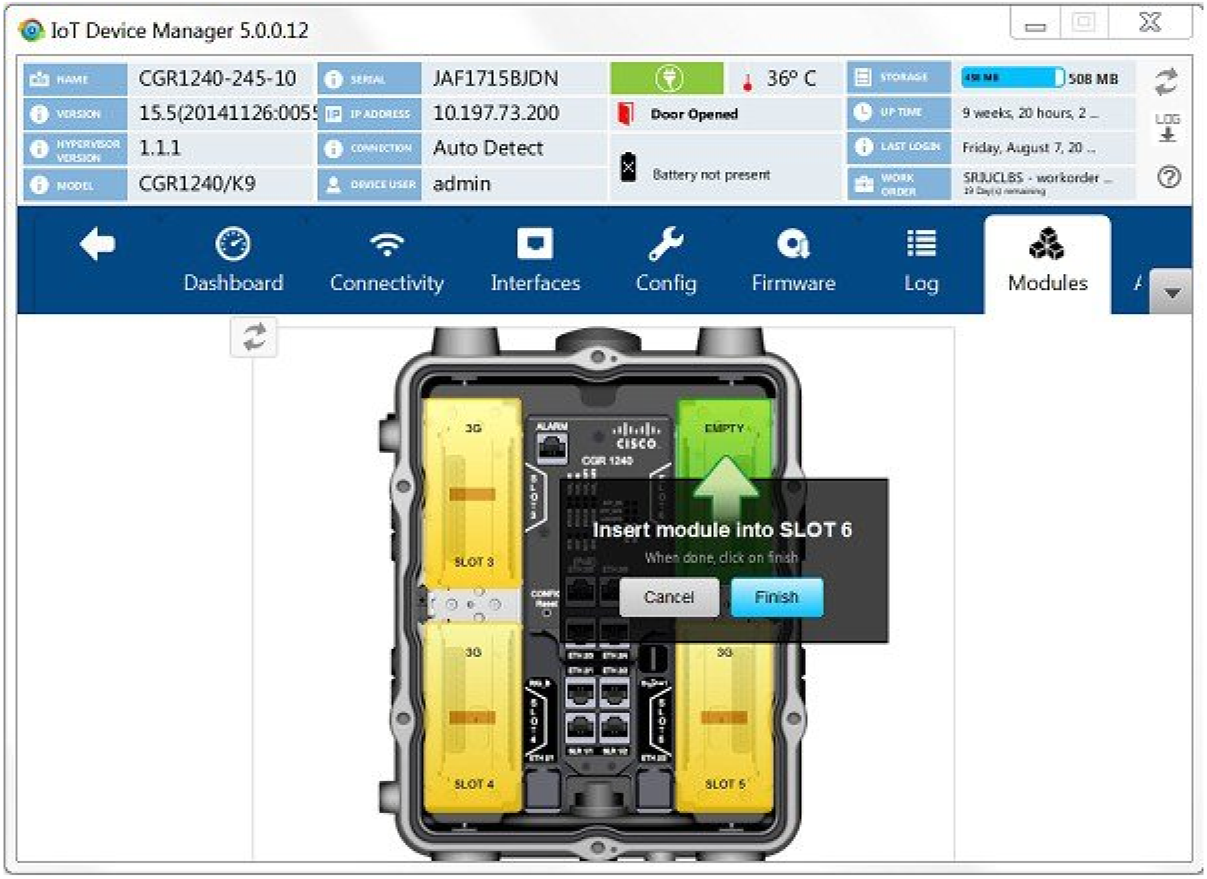
1. On the Modules page, click the module slot that corresponds to the target destination for your module.
2. To continue inserting the module, click **Yes** in the Insert Module confirmation dialog box.
3. When the *Insert module into SLOT* message appears, insert the module in the physical slot of the router.
4. Click **Finish**.
5. In the Insert Module dialog box, click **Save Results** or **OK**. The slot where you physically inserted the module appears in yellow with a minus (-) sign, indicating an occupied slot.

DETAILED STEPS

Step 1 On the Modules page, click the module slot that corresponds to the target destination for your module.

Note Empty slots are in green and display a plus sign.

Step 2 To continue inserting the module, click **Yes** in the Insert Module confirmation dialog box.



IoT Device Manager 5.0.0.12

NAME	CGR1240-245-10	SERIAL	JAF1715BJDN	36° C	STORAGE	508 MB
VERSION	15.5(20141126:005	IP ADDRESS	10.197.73.200	Door Opened	UP TIME	9 weeks, 20 hours, 2 ...
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect		LAST LOGIN	Friday, August 7, 20 ...
MODEL	CGR1240/K9	DEVICE USER	admin	Battery not present	WORK ORDER	SRJUCLBS - workorder ...

Insert module into SLOT 6

When done, click on finish

Cancel Finish

Step 3 When the *Insert module into SLOT* message appears, insert the module in the physical slot of the router.

Step 4 Click **Finish**.

Step 5 In the Insert Module dialog box, click **Save Results** or **OK**. The slot where you physically inserted the module appears in yellow with a minus (-) sign, indicating an occupied slot.

Removing a Module

Note Before starting the removal process, ensure that no traffic is active or destined for the module. You cannot run any other operations when removing a module.

To remove a module:

SUMMARY STEPS

1. On the Modules page, click the module slot corresponding to the location of the module that you want to remove.
2. To continue the removal, click **Yes** in the Remove Module confirmation dialog box.
3. When the *Remove module from SLOT* message appears, remove the module from the physical slot of the router.
4. Click **Finish**.
5. Click **Save Results** or **OK** in the Remove Module dialog box. The slot where you physically removed the module appears in green with a plus (+) sign, indicating an empty slot.

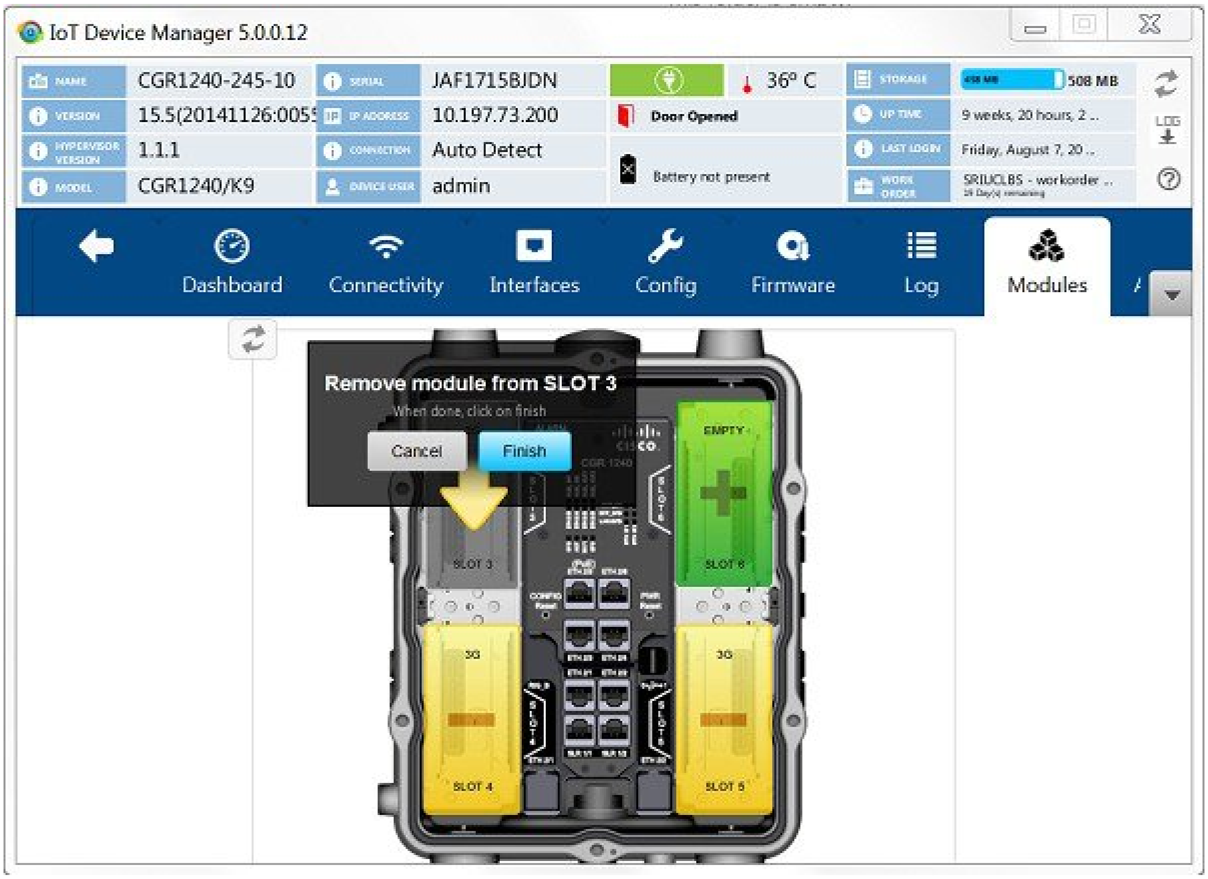
DETAILED STEPS

Step 1 On the Modules page, click the module slot corresponding to the location of the module that you want to remove.

Note Populated slots are in yellow and display a minus sign.

Step 2 To continue the removal, click **Yes** in the Remove Module confirmation dialog box.

Caution Do not physically remove the module until a message prompts you to do so.



IoT Device Manager 5.0.0.12

NAME CGR1240-245-10
VERSION 15.5(20141126:0055
HYPERVISOR VERSION 1.1.1
MODEL CGR1240/K9
SERIAL JAF1715BJDN
IP ADDRESS 10.197.73.200
CONNECTION Auto Detect
DEVICE USER admin
36° C
Door Opened
Battery not present
STORAGE 508 MB
UP TIME 9 weeks, 20 hours, 2 ..
LAST LOGIN Friday, August 7, 20 ..
WORK ORDER SRIUCLBS - workorder ..

Remove module from SLOT 3

When done, click on finish

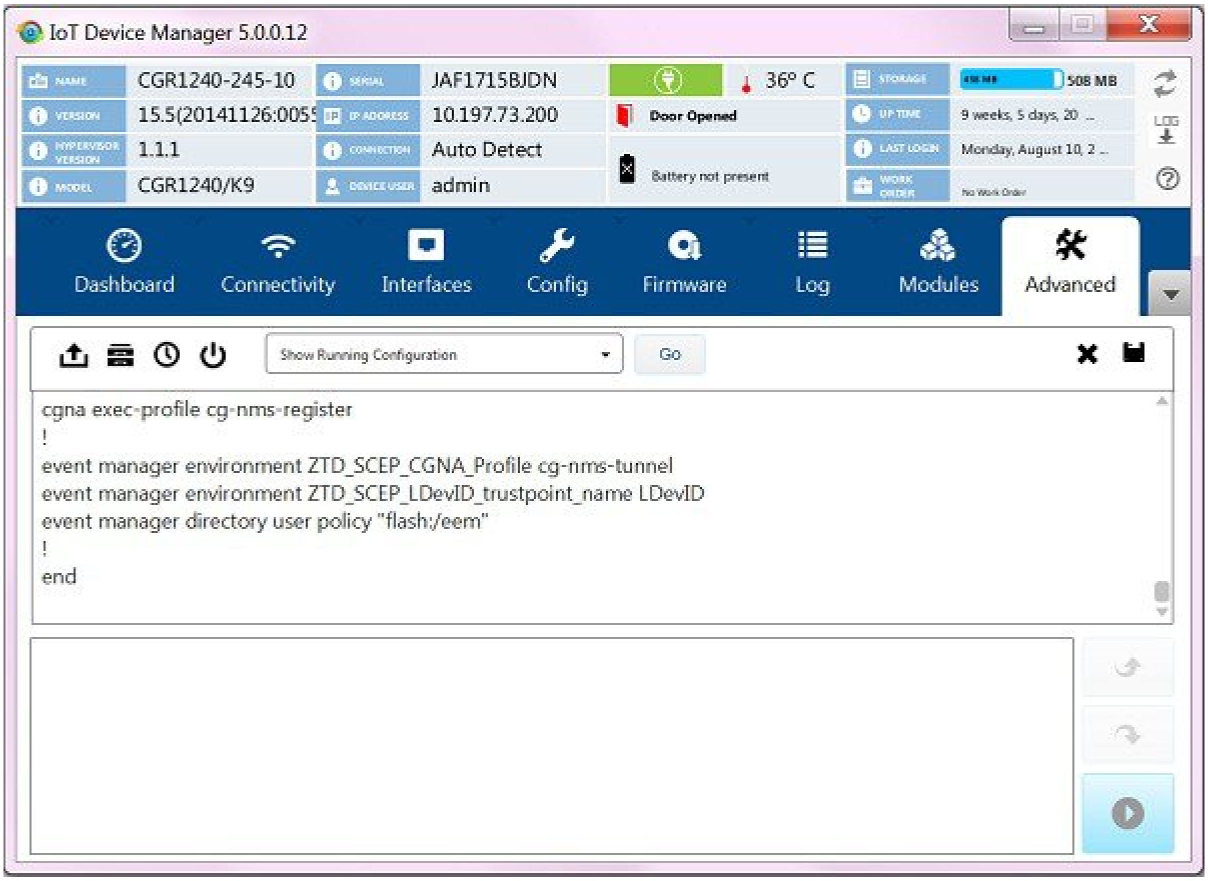
Step 3 When the *Remove module from SLOT* message appears, remove the module from the physical slot of the router.

Step 4 Click **Finish**.

Step 5 Click **Save Results** or **OK** in the Remove Module dialog box. The slot where you physically removed the module appears in green with a plus (+) sign, indicating an empty slot.

Executing Commands

The Advanced page provides access to the CGR 1000 CLI to fine-tune or troubleshoot the router. You must have admin privilege and be familiar with Cisco IOS commands. For details on supported commands, refer to the CGR 1000 software configuration guides at: www.cisco.com/go/cgr1000-docs



IoT Device Manager 5.0.0.12

NAME CGR1240-245-10
VERSION 15.5(20141126:005
HYPERVISOR VERSION 1.1.1
MODEL CGR1240/K9
SERIAL JAF1715BJDN
IP ADDRESS 10.197.73.200
CONNECTION Auto Detect
DEVICE USER admin
36° C
Door Opened
Battery not present
STORAGE 508 MB
UP TIME 9 weeks, 5 days, 20 ...
LAST LOGIN Monday, August 10, 2 ...
WORK ORDER No Work Order

Show Running Configuration

```
cgna exec-profile cg-nms-register
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager directory user policy "flash:/eem"
!
end
```

SUMMARY STEPS

1. On the Device Manager main page, click the **Advanced** tab.
2. Enter Cisco IOS commands in the text input area at the bottom of the page as follows:
3. Use the buttons above the output area for the following common commands:
4. To save a copy of the output, click Save.
5. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

6. To clear the output, click the black cross.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Advanced** tab.

Step 2 Enter Cisco IOS commands in the text input area at the bottom of the page as follows:

- To execute an exec command (for example, **show version**), type the command and click the execute button.
- To execute multiple exec commands, type one command per line and click the execute button.
- Use the up arrow to display the previous command.
- Use the down arrow to display the next command.
- To execute config commands, enclose all of the config commands between **configure terminal** and **end** commands, and click the execute button, for example:

Example:

```
configure terminal
interface gigabitethernet 2/1
description management interface
interface gigabitethernet 2/2
description not used
end
```

Command output appears in the output area above the text input area.

Step 3 Use the buttons above the output area for the following common commands:

- **Upload File**

  —Upload a new image file to the router.
- **File Directory**—Display the router file directory.
- **System Time**—Display the current setting of the system clock for the router.
- **Reboot**—Reboot the router.

You can also select a command from the **More Actions** drop-down menu, then click **Go**. The following commands are available:

- Show Running Configuration
- Show Startup Configuration
- Save Running to Startup
- Reset to Factory Configuration
- Show Factory Configuration
- Show Before Tunnel Configuration
- Show Before Registration Configuration
- Show All CGNA Profiles

- Trigger Registration Request to IoT-FND
- Trigger Tunnel Provisioning Request to IoT-FND

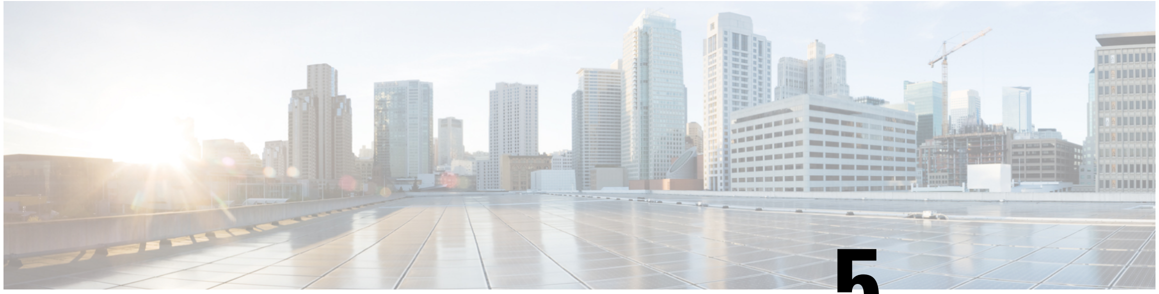
Step 4 To save a copy of the output, click Save.

Step 5 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Step 6 To clear the output, click the black cross.

Disconnecting from the CGR 1000

After finishing your work on the CGR 1000, click the left arrow on the left side of the menu tabs area on the main page to disconnect Device Manager from the router. Click **Yes** to confirm that you want to disconnect from the device. Device Manager disconnects and displays the Device Manager opening page.



CHAPTER 5

Performing Tasks on the IR800

The chapter explains how to use the Device Manager to perform tasks on the IR800.

Connecting to the IR800

You can use Device Manager in the following ways:

- Operating with IoT-FND——When you have IoT-FND operating in the network, you can connect to that system with Device Manager to download and update work orders. Work orders allow Device Manager to view status and perform tasks on the IR800. To operate in conjunction with IoT-FND, follow the steps in Setting Up the IoT-FND Connection.

- Operating without IoT-FND—When you do not have IoT-FND operating in the network or do not want to connect to that system, use Device Manager to connect directly to a IR800 by either WiFi (with valid SSID and passphrase) or Ethernet to view status and perform tasks on the IR800.

Connecting to the Router with a Work Order

Before connecting to the router with a work order, you should be familiar with the information in Managing Work Orders.

To connect to the router with a work order, select a work order from the list on the Device Manager opening page and click **Connect**.

Note The IR809 must have IPv6 option enabled to connect with work order.

Manually Connecting to the Router

You can connect to an IR809 by Ethernet, and connect to an IR829 by Ethernet or WiFi.

Connect to the Device Manager by employing one of the following methods:

- Auto Discovered IPv6 address (preferred method for the field)
- IPv4 address (such as 128.128.128.128)
- IPv6 address (such as fe80::d81f:6402:2ae4:4ea8)

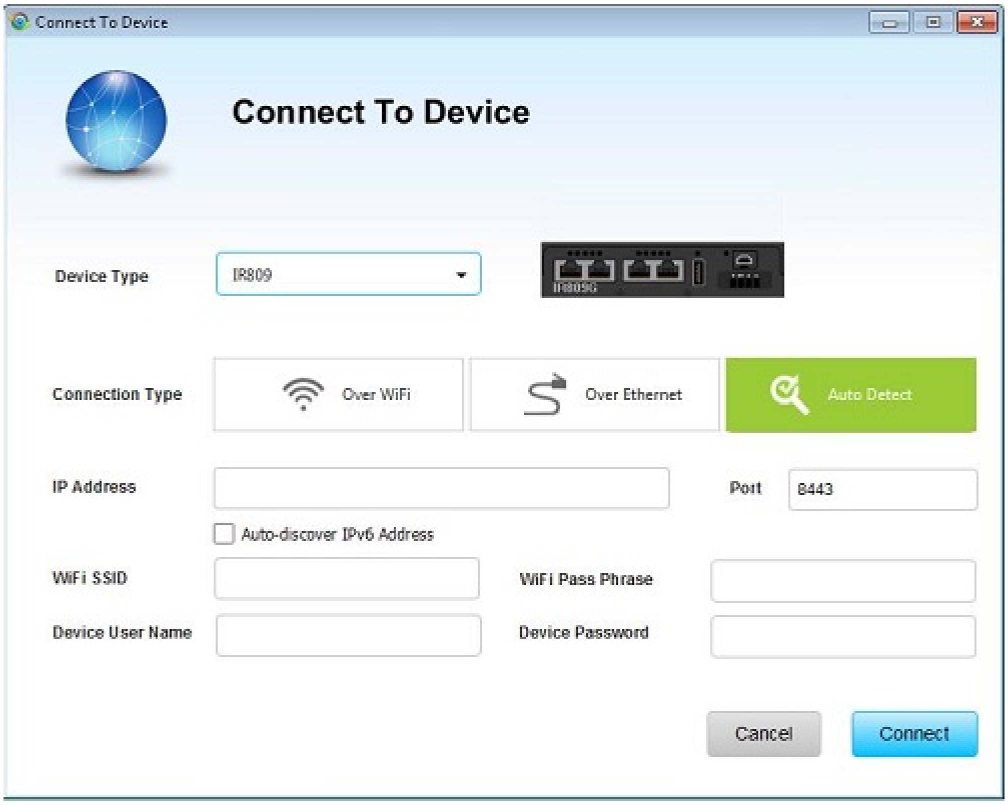
To connect to the Device Manager manually:

SUMMARY STEPS

1. On the Device Manager opening page, click **Connect Without Work Order**.
2. In the Connect to Device dialog box, select the Device Type: **IR809** or **IR829**.
3. Select the Connection Type: **Over WiFi**, **Over Ethernet**, or **Auto Detect**.
4. Enter the router IP address and port, or select the check box to auto-discover the IP address.
5. (WiFi only) Enter the SSID and pass phrase.
6. Enter the user name and password.
7. Click **Connect**. The Device Manager main page appears.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Connect Without Work Order**.



Device Type: IR809

Connection Type

IP Address

Port: 8443

□ Auto-discover IPv6 Address

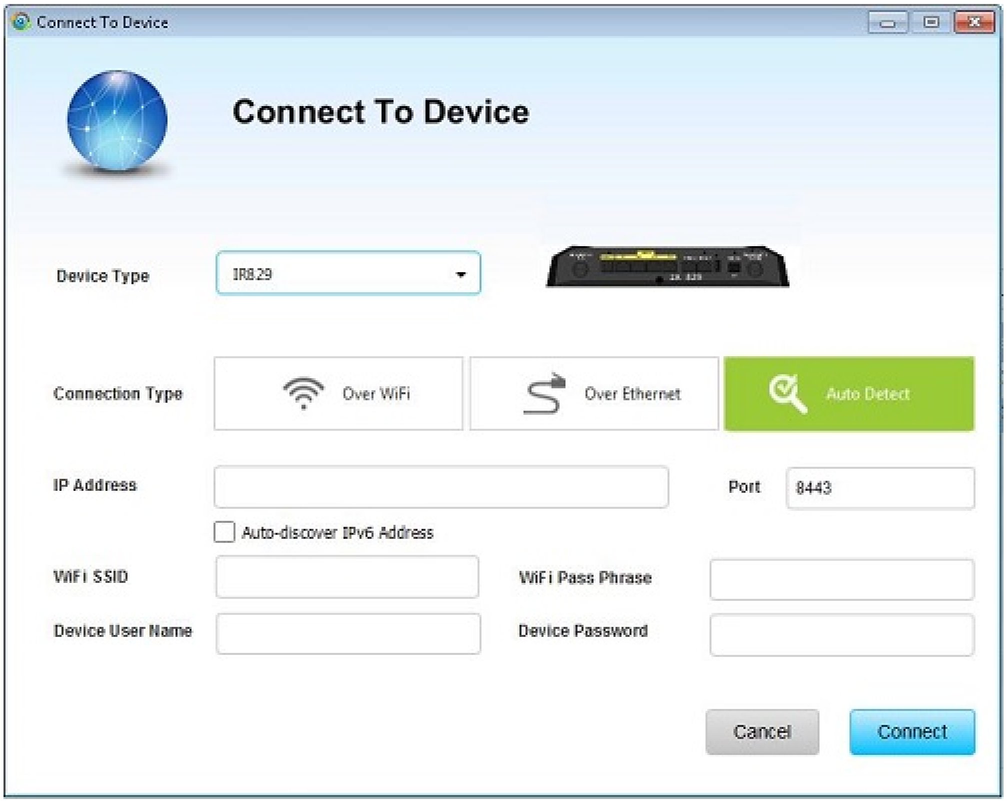
WiFi SSID

WiFi Pass Phrase

Device User Name

Device Password

Step 2 In the Connect to Device dialog box, select the Device Type: **IR809** or **IR829**.



Device Type: IR829

Port: 8443

Step 3 Select the Connection Type: **Over WiFi**, **Over Ethernet**, or **Auto Detect**.

Step 4 Enter the router IP address and port, or select the check box to auto-discover the IP address.

Step 5 (WiFi only) Enter the SSID and pass phrase.

Step 6 Enter the user name and password.

Step 7 Click **Connect**. The Device Manager main page appears.

Testing Connectivity

You can confirm connectivity to a device from the IR800 through the Connectivity page.

Before you can check a device connection or route to a IR800, you must add the IPv4 or IPv6 address or hostname of the device (connection target) to Device Manager. All work orders have connection targets.

Adding a Device IP Address

To add a device IP address:

SUMMARY STEPS

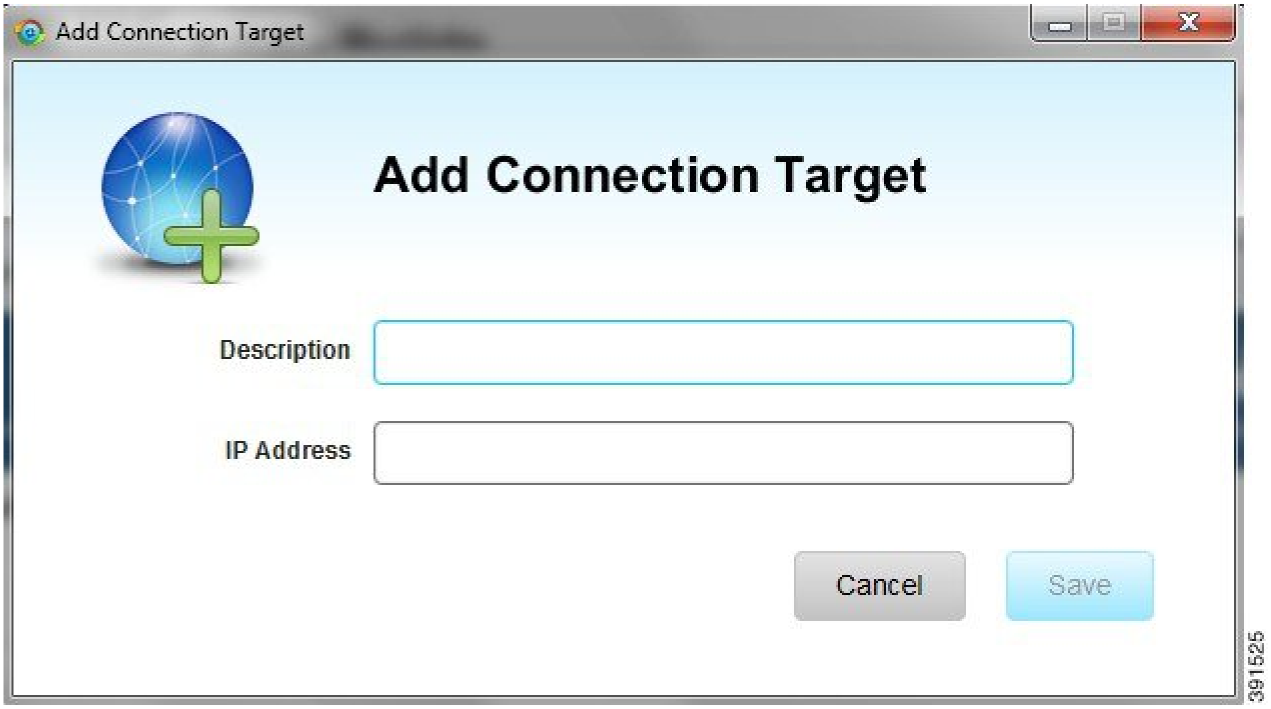
1. On the Device Manager main page, click the **Connectivity** tab.
2. On the Connectivity page, click **Add Target** to create a new target.

3. In the Description field, enter a description for the device.
4. In the IP Address field, enter the IP address (IPv4 or IPv6) of the device.
5. Click **Save**. You can now test the connectivity to the device you just added to the Device Manager.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Connectivity** tab.

Step 2 On the Connectivity page, click **Add Target** to create a new target.



Step 3 In the Description field, enter a description for the device.

Step 4 In the IP Address field, enter the IP address (IPv4 or IPv6) of the device.

Step 5 Click **Save**. You can now test the connectivity to the device you just added to the Device Manager.

Pinging a Device IP Address

The Ping feature allows you to verify connectivity to a device by querying the target IP address.

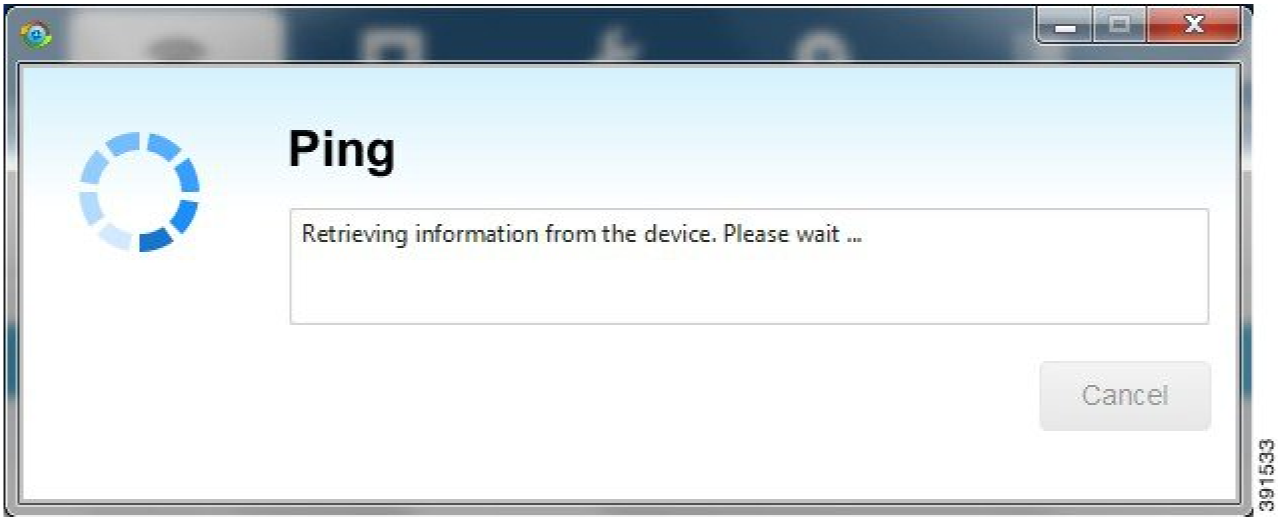
To test connectivity between the router and the device:

SUMMARY STEPS

1. On the Connectivity page, select the connection target and click **Ping**. A dialog box appears indicating that the router is attempting to ping the target IP address.
2. Click **OK** to close the Ping dialog box.

DETAILED STEPS

Step 1 On the Connectivity page, select the connection target and click **Ping**. A dialog box appears indicating that the router is attempting to ping the target IP address.



Ping

Retrieving information from the device. Please wait ...

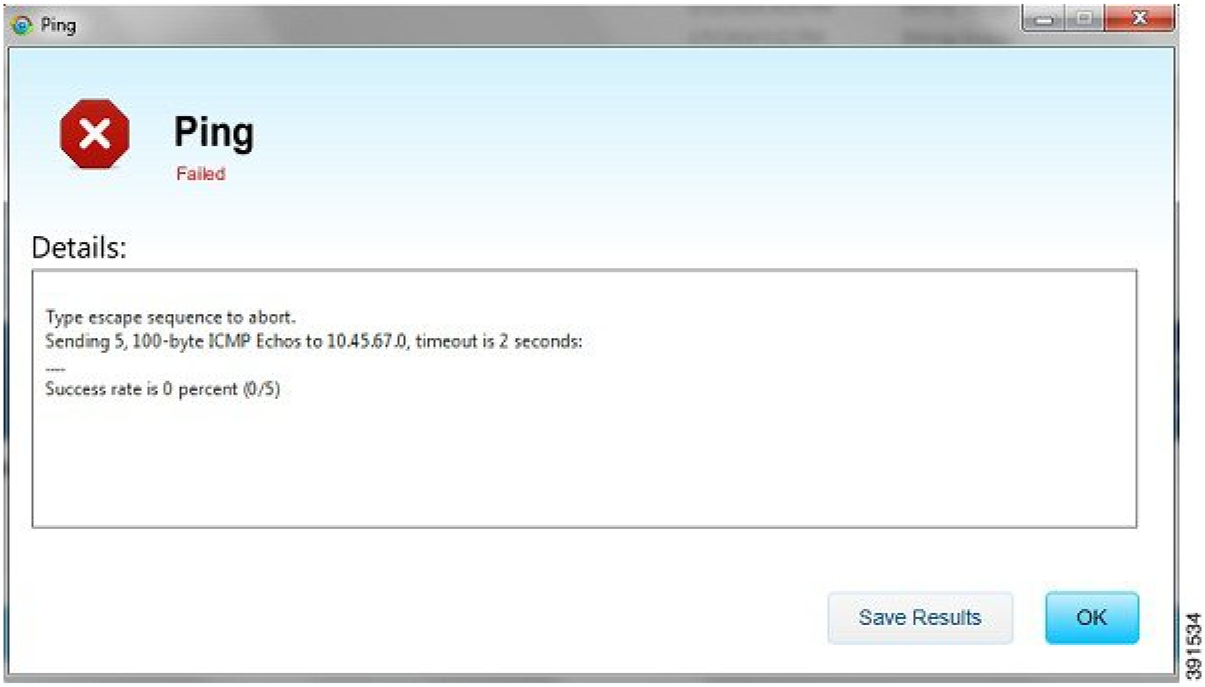
When the system successfully pings the device, a dialog box appears indicating that the ping was successful.

If the system does not successfully ping a device, refer to Failed Ping, on page 42.

Step 2 Click **OK** to close the Ping dialog box.

Failed Ping

If the system does not successfully ping a device, a message appears showing the details of the failed ping attempt.



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.45.67.0, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

SUMMARY STEPS

1. In the Ping error dialog box, review the reason for the error, then click **OK** or **Save Results** to save the output to a file on the laptop.
2. Proceed to Tracing the Route of a Device IP Address, on page 43.

DETAILED STEPS

Step 1 In the Ping error dialog box, review the reason for the error, then click **OK** or **Save Results** to save the output to a file on the laptop.

Step 2 Proceed to Tracing the Route of a Device IP Address, on page 43.

Tracing the Route of a Device IP Address

When an IP address cannot be reached using Ping, you can use the Trace Route feature to check the route taken to reach the device IP address.

To trace the route of the IP address:

SUMMARY STEPS

1. On the Connectivity page, click **Trace Route** for the listed connection target.
2. If the trace route is successful, review the details and click **Save Results** or **OK** in the Trace Route dialog box.
3. If the trace route is unsuccessful, proceed to Deleting or Editing a Device IP Address, on page 43.

DETAILED STEPS

Step 1 On the Connectivity page, click **Trace Route** for the listed connection target.

Step 2 If the trace route is successful, review the details and click **Save Results** or **OK** in the Trace Route dialog box.

Step 3 If the trace route is unsuccessful, proceed to Deleting or Editing a Device IP Address, on page 43.

Deleting or Editing a Device IP Address

After you have tested a target IP address and verified its connectivity, you can delete the device entry from the Device Manager. You can also delete or edit an IP address that the application identifies as incorrect during failed pings and trace route attempts.

To delete or edit a target IP address:

SUMMARY STEPS

1. On the Connectivity page, select the listed connection target, and click **Delete** to remove the device from the list.
2. To edit the device’s IP address, click **Modify Target**.
3. In the Modify Connection Target dialog box, edit the IP address and click **Save**.

DETAILED STEPS

Step 1 On the Connectivity page, select the listed connection target, and click **Delete** to remove the device from the list.

Step 2 To edit the device’s IP address, click **Modify Target**.

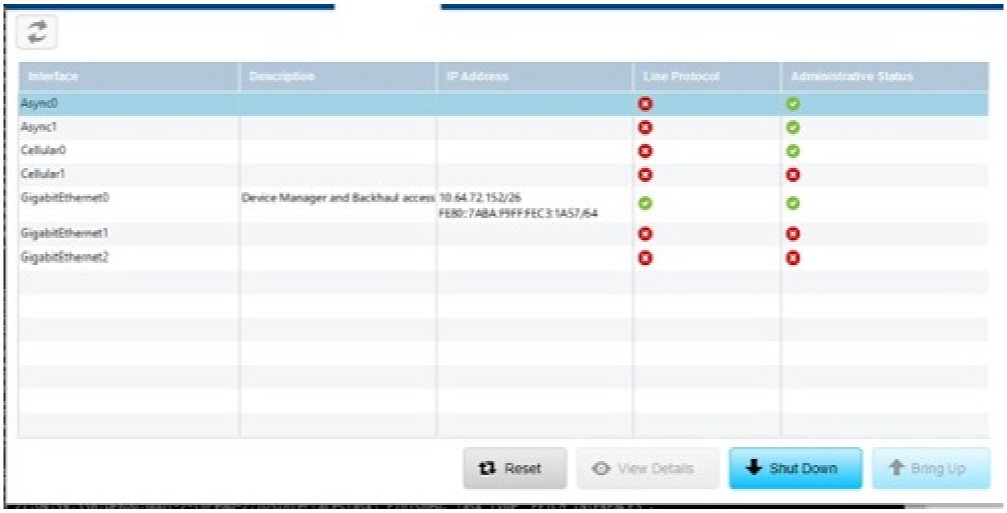
Step 3 In the Modify Connection Target dialog box, edit the IP address and click **Save**.

Managing Interfaces

You can bring up or shut down an interface on the Interfaces page. You can also reset an interface and view interface details.

- When the line protocol for an interface is *up* (a green check mark), the line protocol is currently active. When the line protocol for an interface is *down* (a red cross), it means the line protocol is not active.
- When the administrative status for an interface is *up* (a green check mark), the administrator brought up the interface. When the administrative status for an interface is *down* (a red cross), the administrator took down the interface.

All interfaces installed within the IR800 display automatically.



Interface	Description	IP Address	Line Protocol	Administrative Status
Async0			✗	✓
Async1			✗	✓
Cellular0			✗	✓
Cellular1			✗	✗
GigabitEthernet0	Device Manager and Backhaul access	10.64.72.152/26 FE80::7ABA:F9FF:FEC3:1A57/64	✓	✓
GigabitEthernet1			✗	✗
GigabitEthernet2			✗	✗

Resetting an Interface

Resetting an interface shuts it down and then brings it up. To reset an interface:

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Reset**.
3. In the Reset Interface dialog box, click **Yes** to confirm the reset.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Reset**.

Step 3 In the Reset Interface dialog box, click **Yes** to confirm the reset.

Viewing Details for an Interface

Select an interface and click **View Details** to display information including interface status, settings, and dynamic statistics. Information is updated every 5 seconds.

To view details for an interface:

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **View Details**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **View Details**.

Bringing Up an Interface

When an interface is shut down for any reason, you can attempt to bring up the interface.

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Bring Up**.
3. In the Bring Up interface dialog box, click **Yes** to confirm bringing up the interface.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Bring Up**.

Step 3 In the Bring Up interface dialog box, click **Yes** to confirm bringing up the interface.

Shutting Down an Interface

Note You cannot shut down the interface on which the Device Manager communicates with the CGR 1000 because the connection would be lost.

To shut down an interface:

SUMMARY STEPS

1. On the Device Manager main page, click the **Interfaces** tab.
2. On the Interfaces page, select an interface and click **Shut Down**.
3. In the Shut Down interface dialog box, click **Yes** to confirm shutting down the interface.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Interfaces** tab.

Step 2 On the Interfaces page, select an interface and click **Shut Down**.

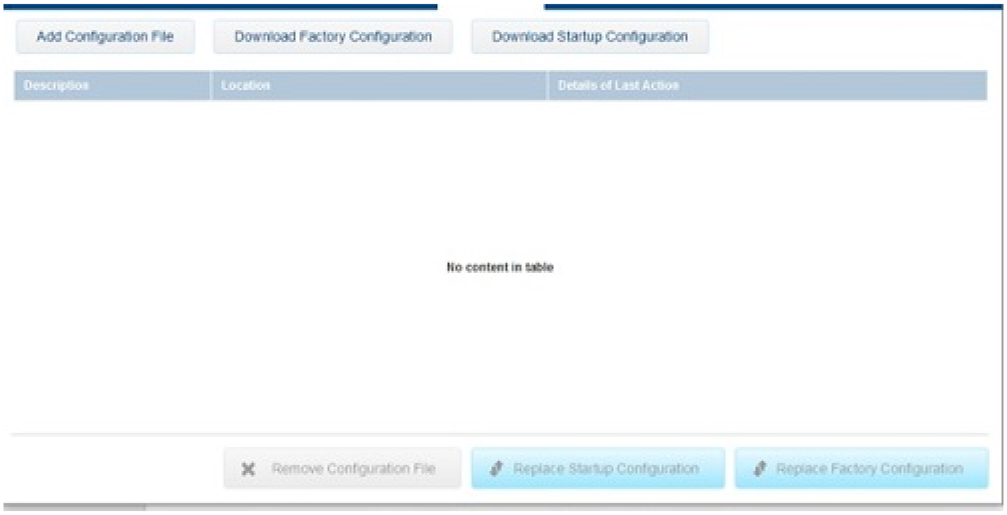
Step 3 In the Shut Down interface dialog box, click **Yes** to confirm shutting down the interface.

Changing the Configuration

You can upload a router configuration file to the Device Manager and then use that file to replace the startup configuration or the express setup (factory configuration) of the IR800.

Note In NMS mode, you can replace only the factory configuration. In non-NMS mode, you can replace both the startup and factory configuration.

You can also download the factory or startup configuration file from the router to your laptop.


Add Configuration File
Download Factory Configuration
Download Startup Configuration
Description
Location
Details of Last Action
No content in table
Remove Configuration File
Replace Startup Configuration
Replace Factory Configuration

Adding a Configuration File

To add a configuration file to Device Manager:

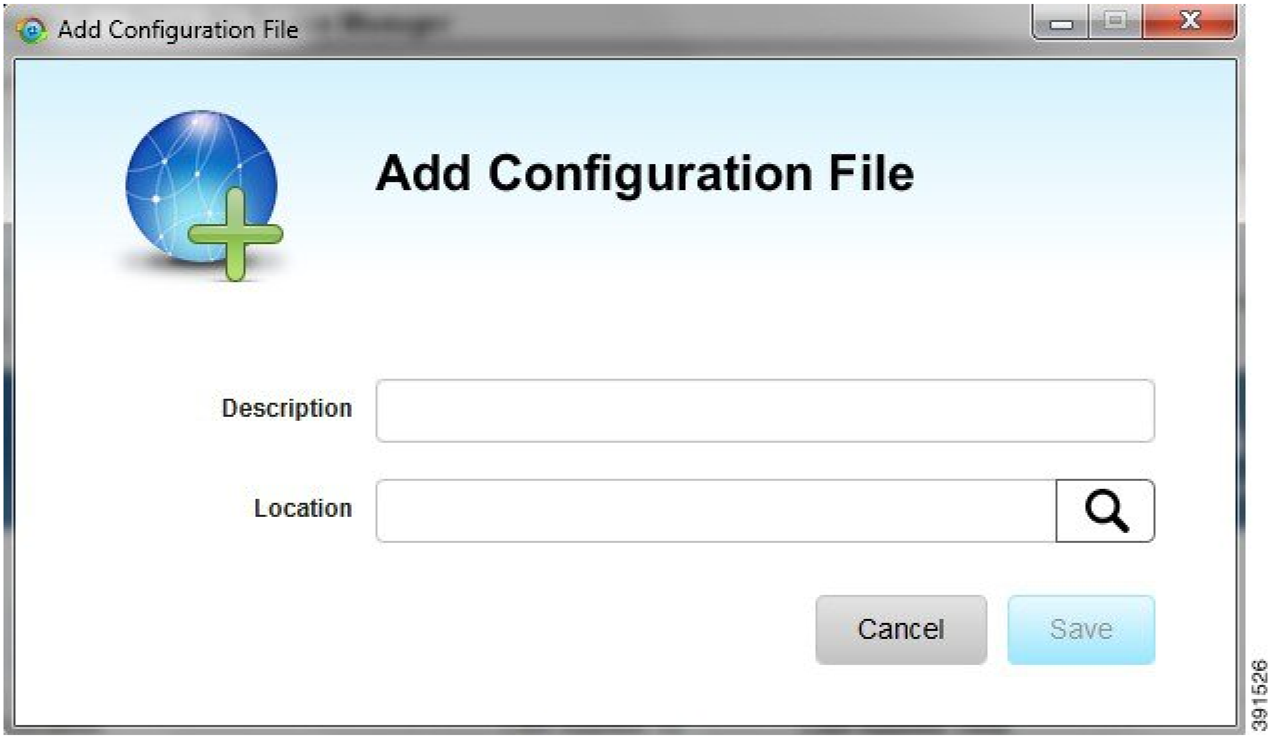
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Add Configuration File**.
3. In the Add Configuration File dialog box:

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click **Add Configuration File**.



Step 3 In the Add Configuration File dialog box:

a) Enter a description for the configuration file that you are going to upload.

b) Click **Search** to navigate to the configuration file location and select the file.

c) Click **Save**.

The file you selected is listed on the Config page.

Downloading a Configuration File

To download the factory configuration file or the startup configuration file to the Device Manager laptop:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Download Factory Configuration** or **Download Startup Configuration**.
3. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click **Download Factory Configuration** or **Download Startup Configuration**.

Step 3 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Replacing a Configuration File

After you add a configuration file to Device Manager (see Adding a Configuration File, on page 49), you can find the file name listed on the Config page. You can use the file to update the startup configuration or the express setup (factory configuration).

⚠ **Caution** Replacing the configuration file causes the router to reboot. All connections to the router are lost during the update. After this task starts, there is no way to cancel the event. Be careful when using this feature.

To replace the configuration file on the router:

SUMMARY STEPS

1. On the Config page, select the configuration file that you want to install and click **Replace Startup Configuration** or **Replace Factory Configuration**.
2. In the confirmation dialog box, click **Yes** to begin installing the router configuration file.

DETAILED STEPS

Step 1 On the Config page, select the configuration file that you want to install and click **Replace Startup Configuration** or **Replace Factory Configuration**.

Step 2 In the confirmation dialog box, click **Yes** to begin installing the router configuration file.

If an error message appears, the file did not upload to the router. Proceed to Removing a Configuration File, on page 51.

Removing a Configuration File

After you update the router with the new configuration file, you can remove the file from Device Manager. You can also use this function to remove unwanted or duplicate configuration files.

To remove a configuration file:

SUMMARY STEPS

1. On the Config page, select the configuration file you want to remove from the list.
2. Click **Remove Configuration File**.
3. In the dialog box that appears, click **Yes** to remove the file.

DETAILED STEPS

Step 1 On the Config page, select the configuration file you want to remove from the list.

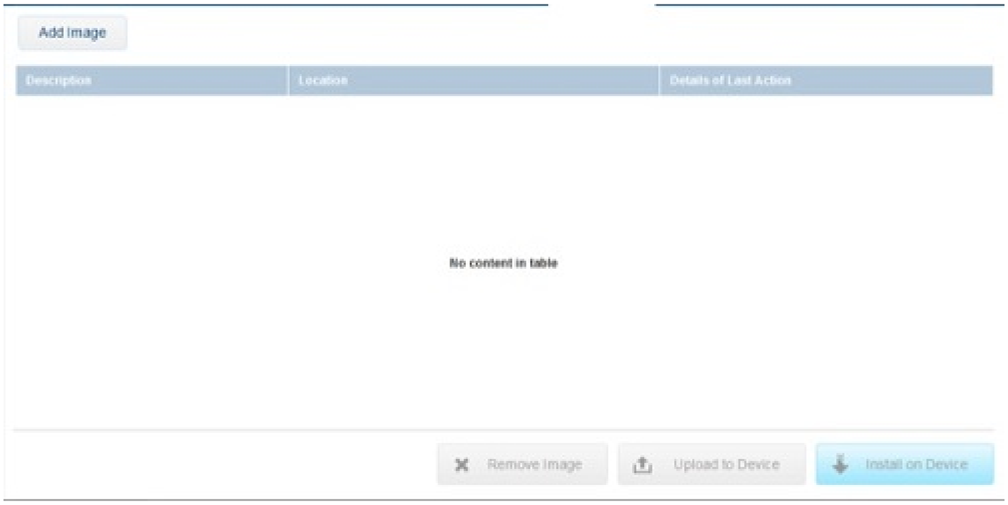
Step 2 Click **Remove Configuration File**.

Step 3 In the dialog box that appears, click **Yes** to remove the file.

Updating the Firmware Image

The IR800 image bundle contains information that the router uses when starting up and operating. The only acceptable file format for the Cisco IR800 image file is a zip bundle, which contains a manifest file with information on versioning and files. Any missing files in the zip bundle cancels the update. You can find the official Cisco IR800 zip bundle on Cisco.com:

https://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-home.html



Adding an Image

To add an image file to Device Manager:

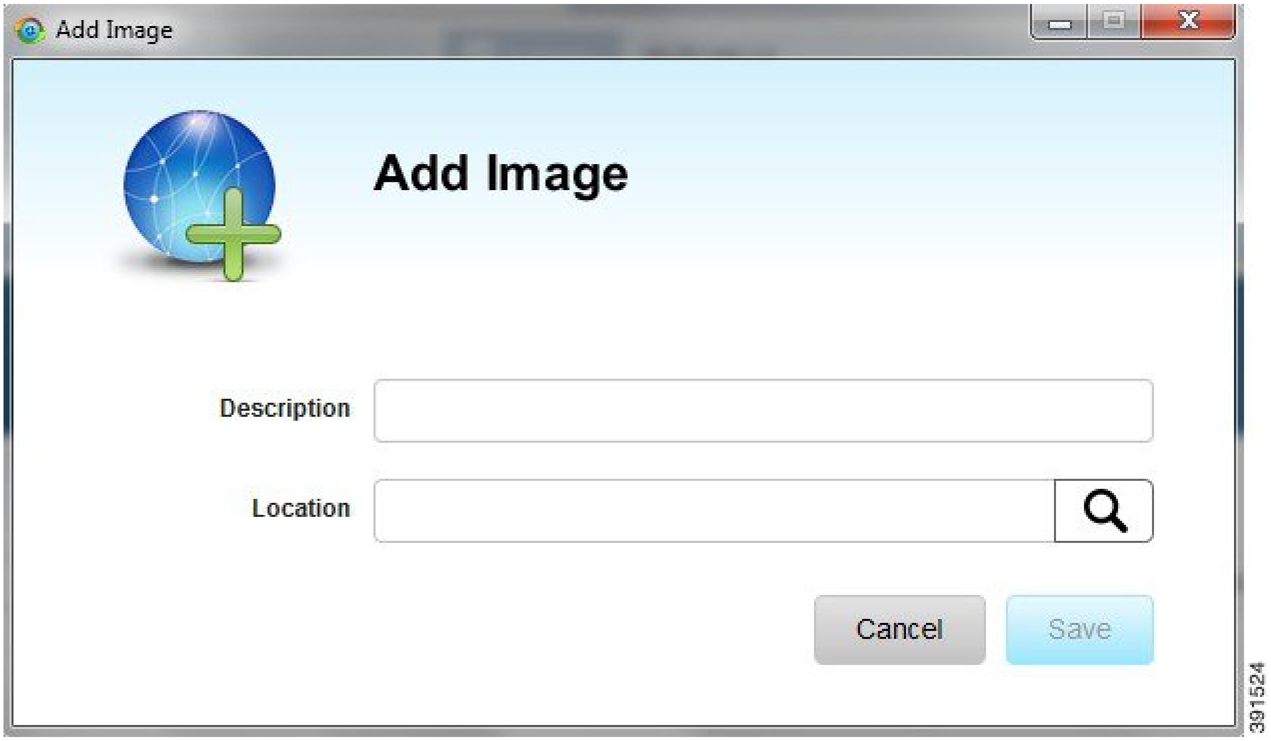
SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. Click **Add Image**.
3. In the Add Image dialog box:

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 Click **Add Image**.



Step 3 In the Add Image dialog box:

a) Enter a description for the image that you are going to upload.
b) Click **Search** to navigate to the image file location and select the file.
c) Click **Save**.

The file you select appears on the Firmware page.

Uploading an Image to the Router

The **Upload to Device** option allows you to upload and store a copy of a firmware image on the router without initiating an immediate image install. This capability allows operations personnel to use IoT-FND or a utility management tool to install and reboot the router when network conditions allow.

To upload an image to the router:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. If the firmware image that you want to install on the router is not listed on the Firmware page, add the image (see Adding an Image, on page 52).
3. On the Firmware page, select the router firmware image that you want to upload and click **Upload to Device**. The new image is stored on the router until you are ready to install the image on the router. (See Installing an Image, on page 54.)

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 If the firmware image that you want to install on the router is not listed on the Firmware page, add the image (see Adding an Image, on page 52).

Step 3 On the Firmware page, select the router firmware image that you want to upload and click **Upload to Device**. The new image is stored on the router until you are ready to install the image on the router. (See Installing an Image, on page 54.)

Installing an Image

⚠ **Caution** Be careful when using this feature. After this tasks starts, there is no way to cancel the event. Updating the router firmware image might take a while to complete and requires a reboot. All connections to the router are unavailable during the image update.

To install an image:

SUMMARY STEPS

1. On the Firmware page, select the image file to install and click **Install on Device**.
2. In the dialog box that appears, click **Yes** to exclude Guest OS from the installation.
3. If you click Yes, Guest OS will not be upgraded.
4. If the firmware image already exists in the router, you are prompted to confirm reinstalling the same image.
5. In the confirmation dialog box, click **Yes** to begin the install process. After the router firmware update completes, the router reboots.

DETAILED STEPS

Step 1 On the Firmware page, select the image file to install and click **Install on Device**.

Step 2 In the dialog box that appears, click **Yes** to exclude Guest OS from the installation.

Step 3 If you click Yes, Guest OS will not be upgraded.

Step 4 If the firmware image already exists in the router, you are prompted to confirm reinstalling the same image.

Step 5 In the confirmation dialog box, click **Yes** to begin the install process. After the router firmware update completes, the router reboots.

Removing an Image

After you install an image, you can remove the image file from the Device Manager. You can also use the Remove image option to remove an image file.

To remove an image file:

SUMMARY STEPS

1. On the Update Image page, select a image.
2. Click **Remove Image**.
3. In the dialog box that appears, click **Yes** to remove the image. A message warns you if the image has not yet been installed on the router.

DETAILED STEPS

Step 1 On the Update Image page, select a image.

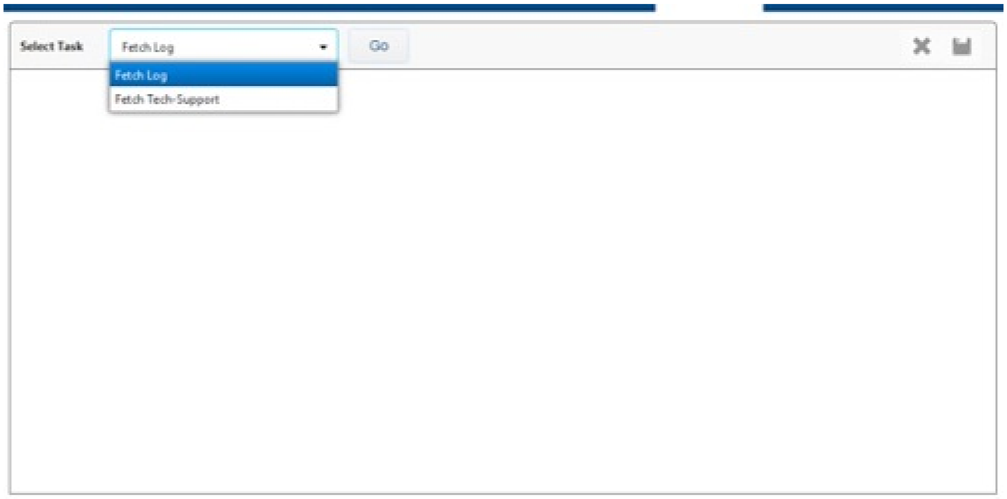
Step 2 Click **Remove Image**.

Step 3 In the dialog box that appears, click **Yes** to remove the image. A message warns you if the image has not yet been installed on the router.

Retrieving Logs

You can retrieve real-time log events from the IR800 and view them on the Log page or save the information to a file.

You can specify either the system log or the tech support log for retrieval.



Retrieving and Saving Logs

To retrieve real-time log events from the router:

SUMMARY STEPS

1. On the Device Manager main page, click the **Log tab**.
2. On the Log page, select the report retrieval task from the Select Task drop-down menu:
3. To save a copy of the retrieved log events displayed on the page, click Save.

4. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.
5. To clear the output, click the black cross.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Log tab**.

Step 2 On the Log page, select the report retrieval task from the Select Task drop-down menu:

- Fetch Log–Retrieves the output from the **show logging** command.
- Fetch Tech-Support–Retrieves the output from the **show tech-support** command.

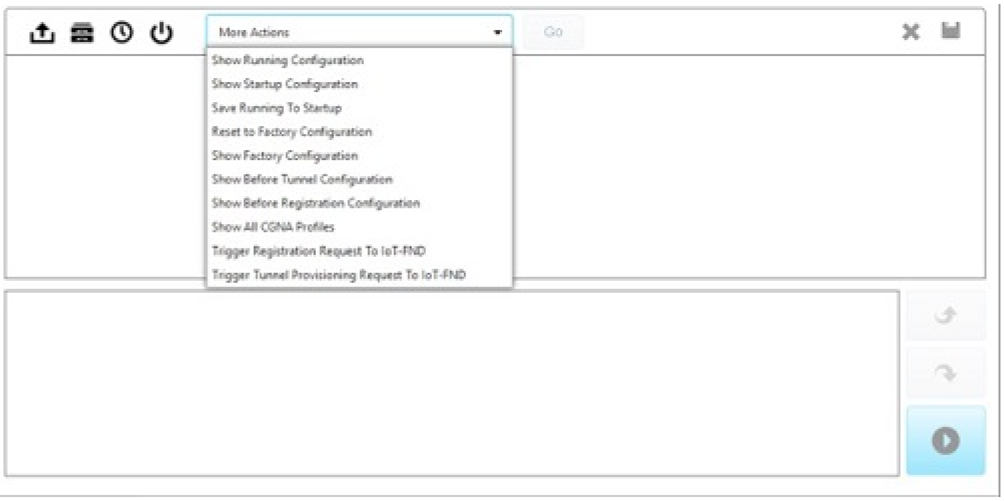
Step 3 To save a copy of the retrieved log events displayed on the page, click Save.

Step 4 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Step 5 To clear the output, click the black cross.

Executing Commands

The Advanced page provides access to the IR800 CLI to fine-tune or troubleshoot the router. You must have admin privilege and be familiar with Cisco IOS commands. For details on supported commands, refer to the IR800 software configuration guides at:https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config.html.


More Actions
Go
Show Running Configuration
Show Startup Configuration
Save Running To Startup
Reset to Factory Configuration
Show Factory Configuration
Show Before Tunnel Configuration
Show Before Registration Configuration
Show All CGNA Profiles
Trigger Registration Request To IoT-FND
Trigger Tunnel Provisioning Request To IoT-FND

SUMMARY STEPS

1. On the Device Manager main page, click the **Advanced** tab.
2. Enter Cisco IOS commands in the text input area at the bottom of the page as follows:
3. Use the buttons above the output area for the following common commands:

4. To save a copy of the output, click Save.
5. In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.
6. To clear the output, click the black cross.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Advanced** tab.

Step 2 Enter Cisco IOS commands in the text input area at the bottom of the page as follows:

- To execute an exec command (for example, **show Running Configuration**), type the command and click the execute button.
- To execute multiple exec commands, type one command per line and click the execute button.
- Use the up arrow to display the previous command.
- Use the down arrow to display the next command.
- To execute config commands, enclose all of the config commands between **configure terminal** and **end** commands, and click the execute button.

Command output appears in the output area above the text input area.

Step 3 Use the buttons above the output area for the following common commands:

- **Upload File**

  —Upload a new image file to the router.
- **File Directory**—Display the router file directory.
- **System Time**—Display the current setting of the system clock for the router.
- **Reboot**—Reboot the router.

You can also select a command from the **More Actions** drop-down menu, then click **Go**. The following commands are available:

- Show Running Configuration
- Show Startup Configuration
- Save Running to Startup
- Reset to Factory Configuration
- Show Factory Configuration
- Show Before Tunnel Configuration
- Show Before Registration Configuration
- Show All CGNA Profiles
- Trigger Registration Request to IoT-FND
- Trigger Tunnel Provisioning Request to IoT-FND

Step 4 To save a copy of the output, click Save.

Step 5 In the Save As dialog box, enter a file name and click **Save**. A message appears indicating that the output was saved successfully.

Step 6 To clear the output, click the black cross.

Disconnecting from the IR800

After finishing your work on the IR800, click the left arrow on the left side of the menu tabs area on the main page to disconnect Device Manager from the router. Click **Yes** to confirm that you want to disconnect from the device. Device Manager disconnects and displays the Device Manager opening page.

CHAPTER 6

Performing Tasks on the IR500

This chapter explains how to use the Device Manager to perform tasks on the Cisco 500 WPAN Industrial Router (IR500).

Connecting to the IR500

You can use Device Manager in the following ways:

- Operating with IoT-FND—When you have IoT-FND operating in the network, you can connect to that system with Device Manager to download and update work orders. Work orders allow Device Manager to view status and perform tasks on the IR500. To operate in conjunction with IoT-FND, follow the steps in Setting Up the IoT-FND Connection.
- Operating without IoT-FND—When you do not have IoT-FND operating in the network or do not want to connect to that system, use Device Manager to connect directly to an IR500 to view status.

Note When connecting to the IR500 without a work order, you cannot change the device configuration or send data to IoT-FND.

Note The laptop running Device Manager must be directly connected to the IR500.

For more information about the IR500 guides, see http://www.cisco.com/go/ir500 .

Connecting the Laptop to the IR500

To connect the laptop to the IR500, first ensure that you meet these prerequisites:

- You have installed the Device Manager software as described in Installation.
- You are familiar with the information in Managing Work Orders.
- You have a valid work order if you plan on changing any IR500 settings.

To connect the laptop to the IR500:

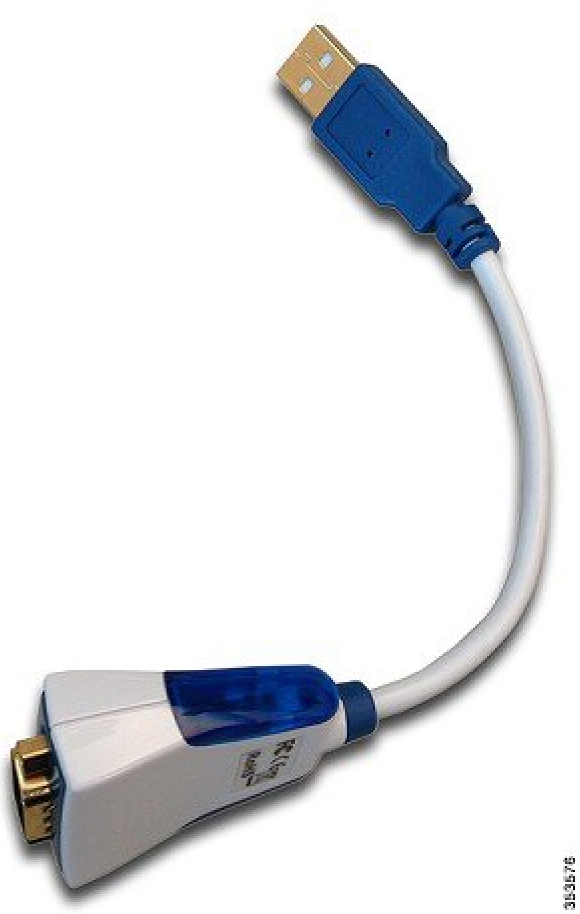
SUMMARY STEPS

1. Attach a serial-to-USB adapter to a serial cable. The serial-to-USB adapter and serial cable are not supplied with the IR500.
2. Connect the serial cable to the IR500 console port.
3. Connect the serial-to-USB adapter to the Windows 7 USB port on the laptop.
4. Launch IoT-Device Manager 5.0.
5. Connect to the IR500 as described in Connecting to the IR500 with a Work Order, on page 88 or Connecting to the IR500 Without a Work Order, on page 88.

DETAILED STEPS

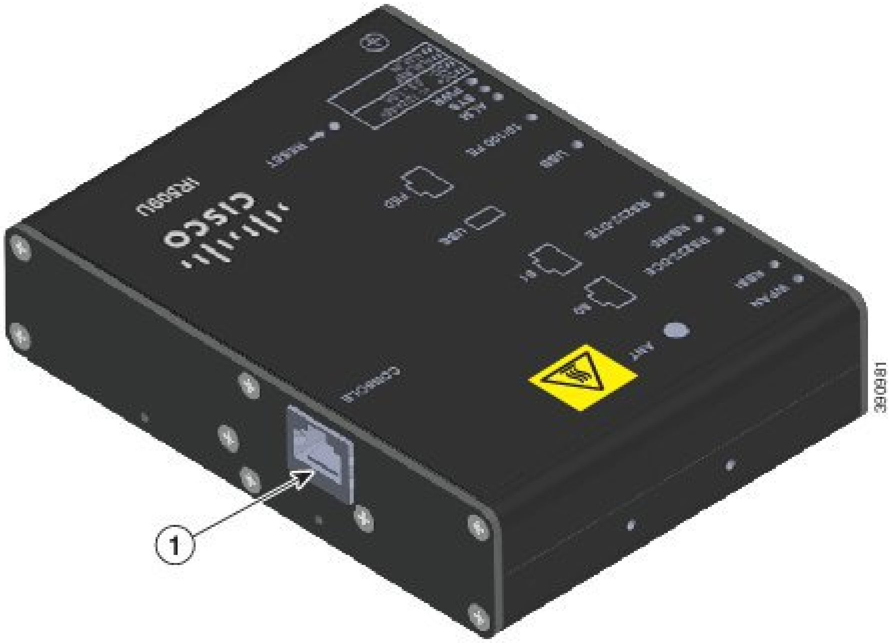
Step 1 Attach a serial-to-USB adapter to a serial cable. The serial-to-USB adapter and serial cable are not supplied with the IR500.

Figure 7: Serial-to-USB Adapter Cable



Step 2 Connect the serial cable to the IR500 console port.

Figure 8: IR500 Rear Panel



1	console port

Step 3 Connect the serial-to-USB adapter to the Windows 7 USB port on the laptop.

Step 4 Launch IoT-Device Manager 5.0.

Step 5 Connect to the IR500 as described in Connecting to the IR500 with a Work Order, on page 88 or Connecting to the IR500 Without a Work Order, on page 88.

For details about IR500 hardware, see the Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide .

Connecting to the IR500 with a Work Order

Before connecting to the router with a work order, you should be familiar with the information in Managing Work Orders.

To connect to the router with a work order, select a work order from the list on the Device Manager opening page and click **Connect**.

Connecting to the IR500 Without a Work Order

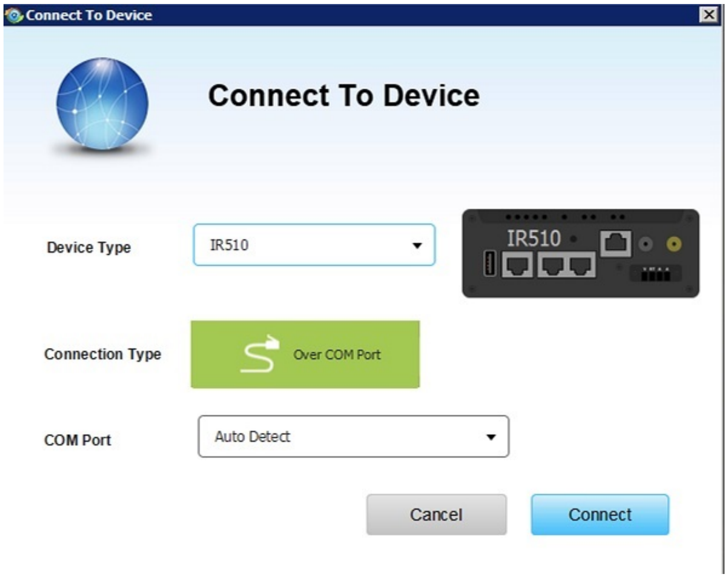
SUMMARY STEPS

1. On the Device Manager opening page, click **Connect Without Work Order**.
2. In the Connect to Device dialog box, select the Device Type: **IR500**.

3. Select the **Over COM port** or **Over Ethernet**.
4. Click **Connect**. The Device Manager main page appears.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Connect Without Work Order**.



Step 2 In the Connect to Device dialog box, select the Device Type: **IR500**.

Step 3 Select the **Over COM port** or **Over Ethernet**.

Step 4 Click **Connect**. The Device Manager main page appears.

Viewing Settings and Status

You can view details about IR500 settings and status from the subtabs of the Dashboard.

General Details

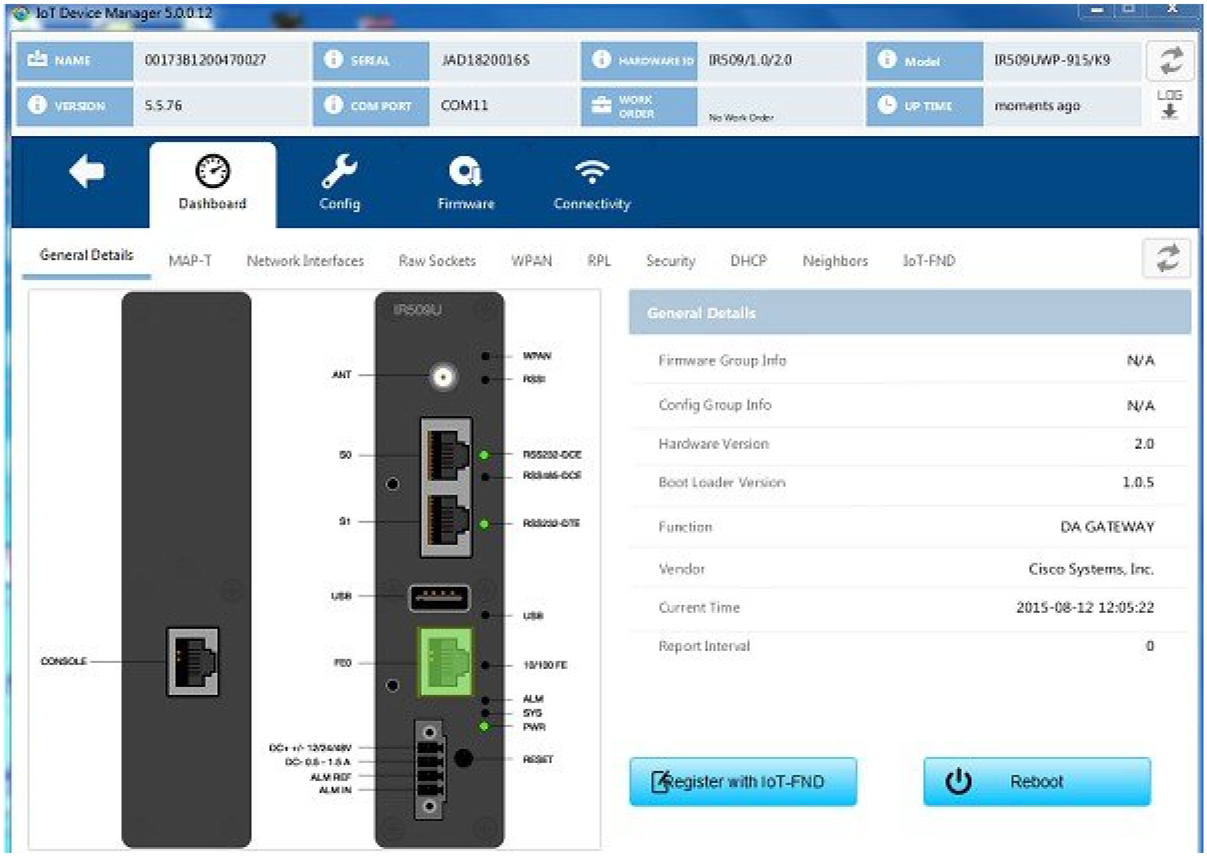
To view General Details:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **General Details** sub-tab.
2. View the General Details:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **General Details** sub-tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

Step 2 View the General Details:

- Firmware Group Info: The name of the firmware group that IoT-FND uses to upload and install firmware images on member devices.
- Config Group Info: The configuration group that IoT-FND uses to manage devices in bulk. The default config group for the DA Gateway is **default-ir500**.
- Hardware Version: The hardware version of the device.
- Boot Loader Version: The boot loader image version.
- Function: The function of the device in the Resilient Mesh network. The function of the IR500 is DA Gateway.
- Vendor: The manufacturer of this device.
- Current Time: The current date and time. The IR500 has a real-time clock that maintains the current time.
- Report Interval: The number of seconds between data updates. By default, Mesh Endpoints (MEs) send a new set of metrics to IoT-FND every 28,800 seconds (8 hours).

MAP-T

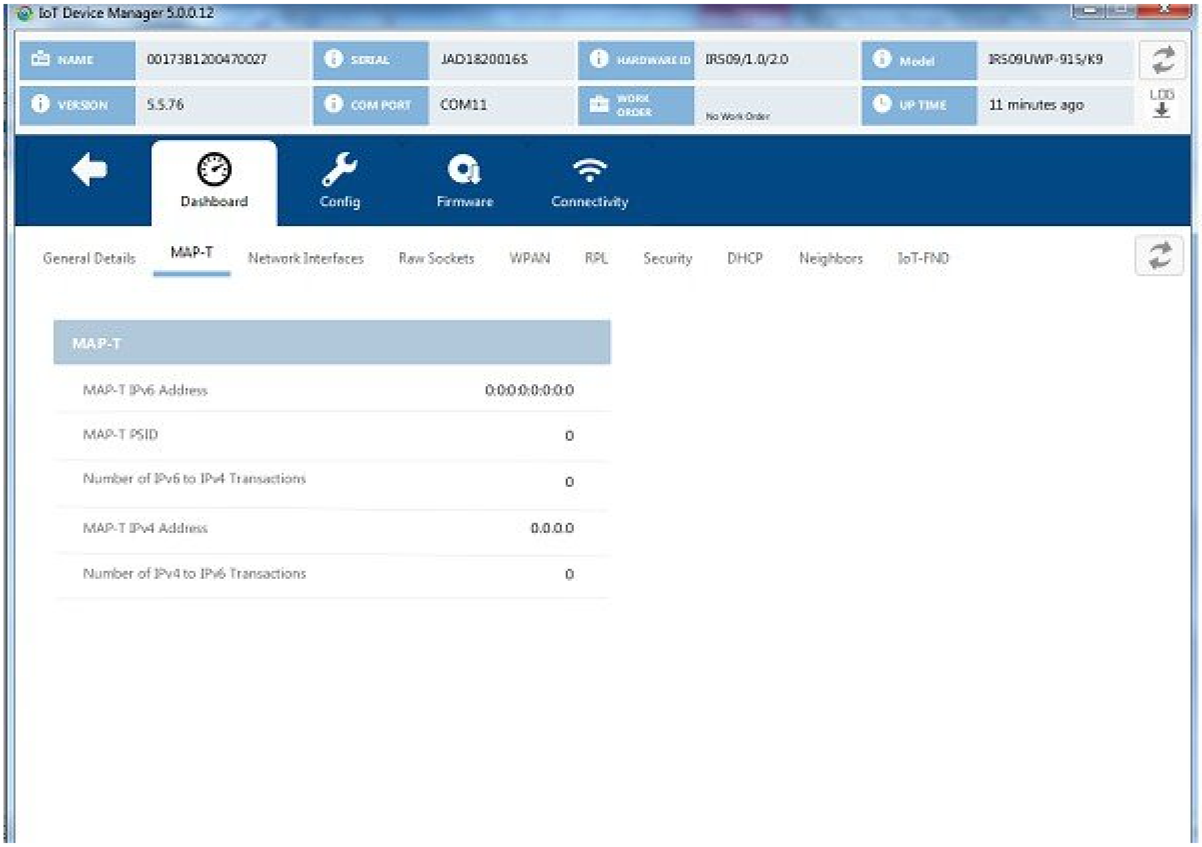
To view MAP-T information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **MAP-T** sub-tab.
2. View the MAP-T settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **MAP-T** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

MAP-T	
MAP-T IPv6 Address	0:0:0:0:0:0:0:0
MAP-T PSID	0
Number of IPv6 to IPv4 Transactions	0
MAP-T IPv4 Address	0.0.0.0
Number of IPv4 to IPv6 Transactions	0

Step 2 View the MAP-T settings and statistics:

- MAP-T IPv6 Address: Contains the IPv4 address used by devices external to the MAP-T domain to communicate with the IR500 Raw Socket over Serial and Ethernet ports.
- MAP-T PSID: The port-set ID (PSID) that algorithmically identifies a set of ports exclusively assigned to the IR500.
- Number of IPv6 to IPv4 Transactions: The number of IPv6 to IPv4 address translations.
- MAP-T IPv4 Address: IPv4 address used by IPv4 devices and applications outside the MAP-T domain to communicate with Raw Socket over Serial and Ethernet attached devices.

- Number of IPv4 to IPv6 Transactions: The number of IPv4 to IPv6 address translations.

Network Interfaces

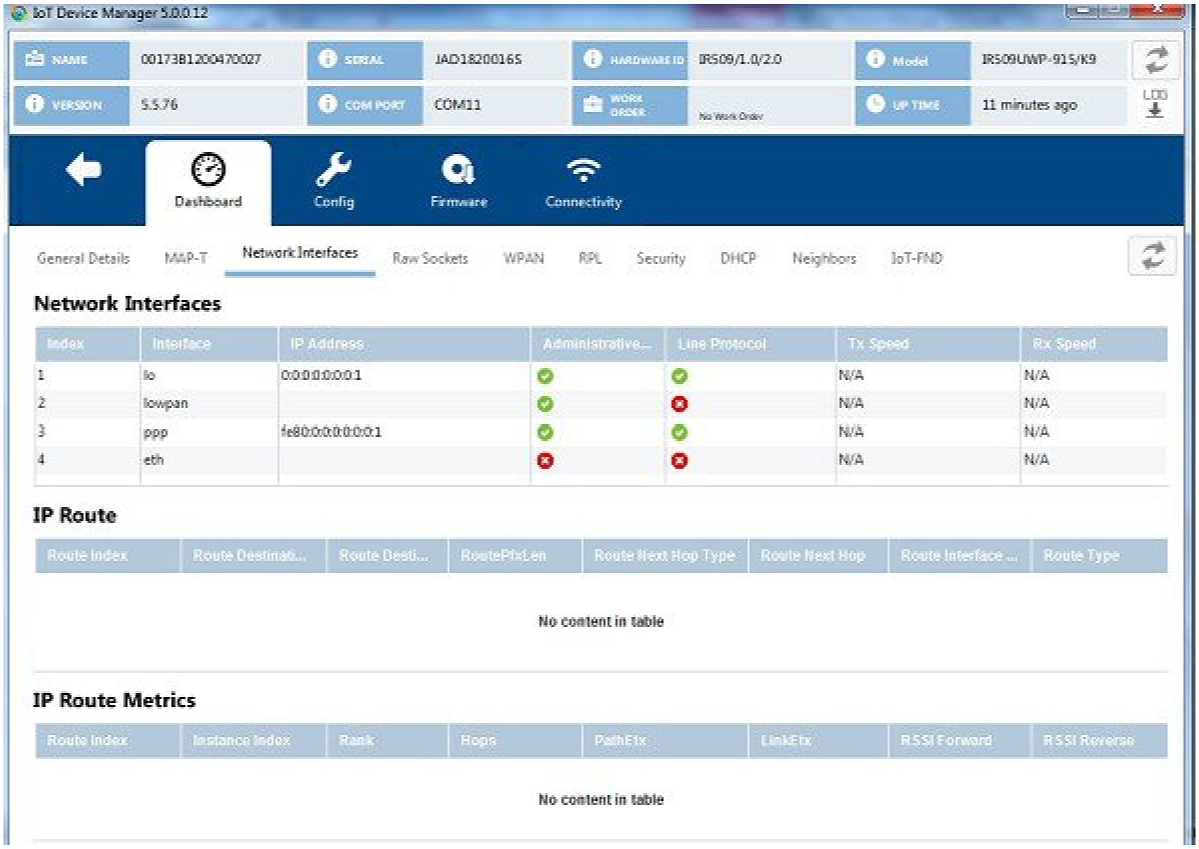
To view information for Network Interfaces:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Network Interfaces** sub-tab.
2. In the Network Interfaces area, view the settings and status for the IR500 interfaces:
3. In the IP Route area, view the IP route information. This table describes a particular IP route (identified by the index) attached to an interface.
4. In the IP Route Metrics area, view the IP Route IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) metrics. The Route Index corresponds to the same index in the IP Route table.

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Network Interfaces** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Network Interfaces

Index	Interface	IP Address	Administrative...	Line Protocol	Tx Speed	Rx Speed
1	lo	0:0:0:0:0:0:0:1	✓	✓	N/A	N/A
2	lowpan		✓	✗	N/A	N/A
3	ppp	fe80:0:0:0:0:0:0:1	✓	✓	N/A	N/A
4	eth		✗	✗	N/A	N/A

IP Route

Route Index	Route Destinati...	Route Desti...	RoutePfxLen	Route Next Hop Type	Route Next Hop	Route Interface ...	Route Type

No content in table

IP Route Metrics

Route Index	Instance Index	Rank	Hops	PathEtx	LinkEtx	RSSI Forward	RSSI Reverse

No content in table

Step 2 In the Network Interfaces area, view the settings and status for the IR500 interfaces:

- Index: Identifies the interface.
- Interface: Name of the IR500 interface.
- IP Address: IP address assigned to the interface.
- Administrative Status: When the administrative status for an interface is administratively *up* , the interface was brought up by the administrator. When the administrative status for an interface is *down* , the interface was taken down by the administrator.
- Line Protocol: When the line protocol for an interface is *up* , the line protocol is currently active. When the line protocol for an interface is *down* , it means the line protocol is not active.
- Tx Speed: Transmit speed.
- Rx Speed: Receive speed.

Step 3 In the IP Route area, view the IP route information. This table describes a particular IP route (identified by the index) attached to an interface.

- Route Index
- Route Destination Type
- Route Destination
- Route PfxLen: Route Prefix Length
- Route Next Hop Type
- Route Next Hop
- Route Interface Index
- Route Type
- Route Proto
- Route Age

Step 4 In the IP Route Metrics area, view the IP Route IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) metrics. The Route Index corresponds to the same index in the IP Route table.

- Route Index: Identifies the route.
- Instance Index: Identifies the instance.
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the Objective Function (OF) of the Directed Acyclic Graph (DAG). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [rfc6550]
- Hops: Hop count.
- PathEtx: Expected transmission count of the path. [rfc6550 and rfc6719]
- LinkEtx: Expected transmission count of the link. [rfc6550 and rfc6719]
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.

- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.
- Dag Size: Size of the DAG. [rfc6550]
- Phase: Electric power phase.

Raw Sockets

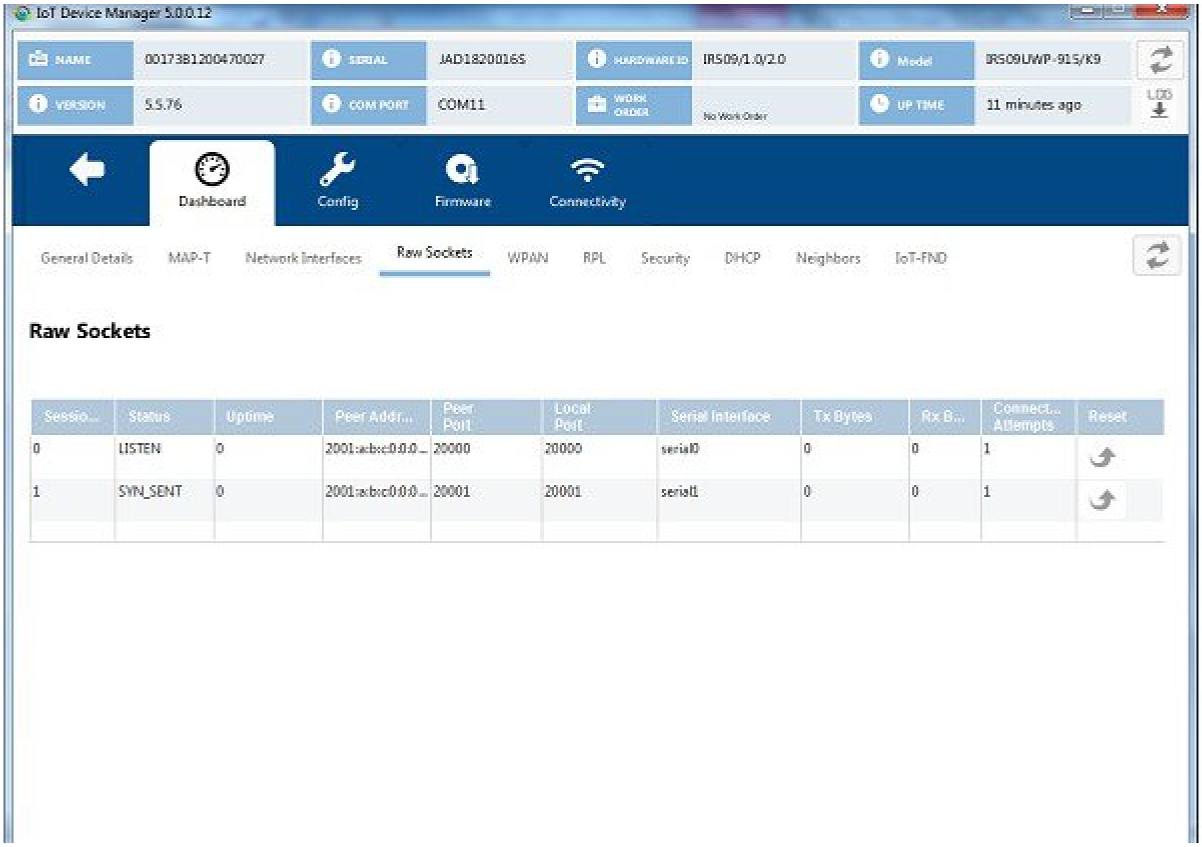
To view information about Raw Sockets:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Raw Sockets** sub-tab.
2. View the raw socket settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Raw Sockets** sub-tab.



NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME 11 minutes ago

Raw Sockets

Sessio...	Status	Uptime	Peer Addr...	Peer Port	Local Port	Serial Interface	Tx Bytes	Rx B...	Connect... Attempts	Reset
0	LISTEN	0	2001:a:b:c:0:0:0...	20000	20000	serial0	0	0	1	
1	SYN_SENT	0	2001:a:b:c:0:0:0...	20001	20001	serial1	0	0	1	

Step 2 View the raw socket settings and statistics:

- Session Index: Identifies the session.
- Status: The status of the raw socket connection.
- Uptime: The length of time that the connection has been up.
- Peer Address: IP address of the host connected to the device.
- Peer Port: The port number of the client/server connected to the device.
- Local Port: The port that either the server listens to for connections (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
- Serial Interface: The name of the serial interface configured for raw socket encapsulation.
- Tx Bytes: Number of bytes sent over the raw socket connection.
- Rx Bytes: Number of bytes received over the raw socket connection.
- Connection Attempts: Number of times that a raw socket client attempted a connection.

Click **Reset** to reset counters to zero.

WPAN

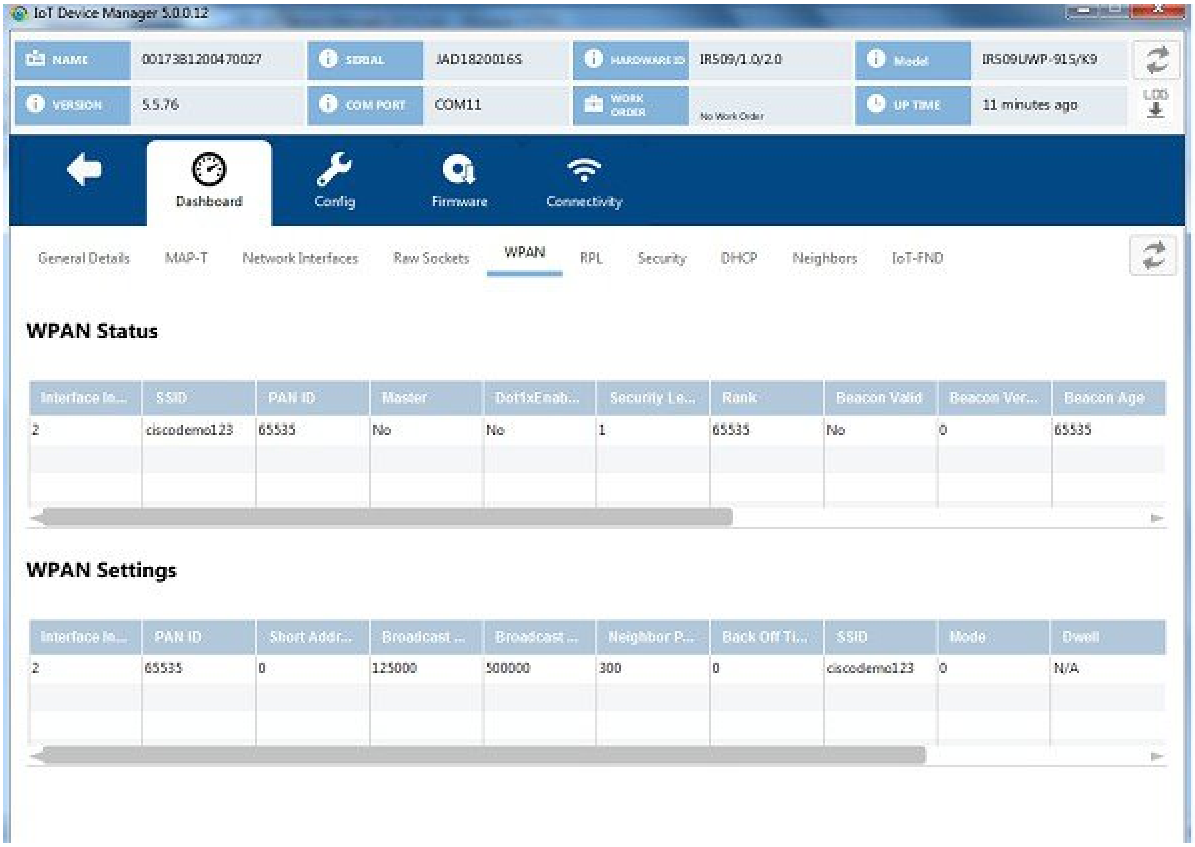
To view information about WPAN:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **WPAN** sub-tab.
2. View the following information in the WPAN Status area:
3. View the following information in the WPAN Settings area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **WPAN** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

WPAN Status

Interface In...	SSID	PAN ID	Master	Dot1xEnab...	Security Le...	Rank	Beacon Valid	Beacon Ver...	Beacon Age
2	ciscodemo123	65535	No	No	1	65535	No	0	65535

WPAN Settings

Interface In...	PAN ID	Short Addr...	Broadcast ...	Broadcast ...	Neighbor P...	Back Off Ti...	SSID	Mode	Dwell
2	65535	0	125000	500000	300	0	ciscodemo123	0	N/A

Step 2 View the following information in the WPAN Status area:

- Interface Index: Identifies the WPAN interface.
- SSID: Service Set Identifier (SSID) used to differentiate networks.
- PAN ID: Personal Area Network Identifier (PAN ID) used to differentiate WPANs.
- Master: Whether the endpoint is master (yes/no).
- Dot1xEnabled: Whether the 802.1x protocol is enabled.

- Security Level: Level of security corresponding to the protection offered (0–2).
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the DAG's Objective Function (OF). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [RFC6550]
- Beacon Valid: The validity of the beacon according to the beacon's age.
- Beacon Version: The beacon's version from the FAR.
- Beacon Age: Parameter related to the time interval received beacon.
- Tx Power: The device current transmission power.
- Metric: The value calculated by rank / the weight value of the rank + size / the weight value of the PAN size.
- Last Changed: The time (in hundredths of a second) since the device changed the PAN.
- LastChangedReason: The reason that the device updated the PAN.
- Demo Mode Enabled: Whether enable demo mode is enabled.
- TxFec: Whether forward error correction (FEC) is enabled.

Step 3 View the following information in the WPAN Settings area:

- Interface Index: Identifies the WPAN interface.
- PAN ID: Personal Area Network Identifier (PAN ID) used to differentiate WPANs.
- Short Address: 16-bit node identifier.
- Broadcast Slot Size: Slot size of the broadcast.
- Broadcast Period: Period of the broadcast.
- Neighbor Probe Rate:
- Back Off Timer: Timer for back off algorithm.
- SSID: Service Set Identifier (SSID) used to differentiate networks.
- Mode: Security mode. 0=no security, 1=802.1x security.
- Dwell: Dwell window in IEEE802.15.4g protocol.
- Notch: List of disabled channels.

RPL

To view information about RPL:

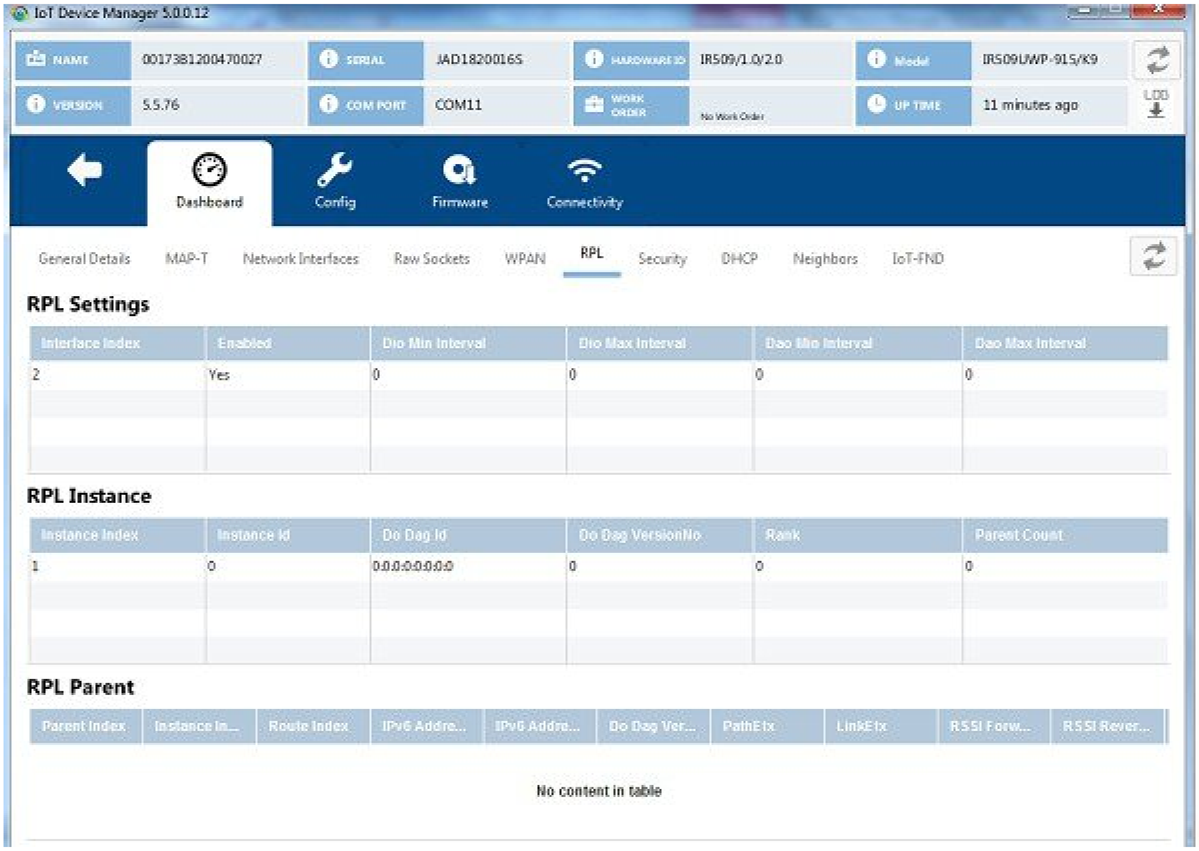
SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **RPL** sub-tab.
2. View the following information in the RPL Settings area:

3. View the following information in the RPL Instance area:
4. View the following information in the RPL Parent area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **RPL** sub-tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD1820016S	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

RPL Settings

Interface Index	Enabled	Dio Min Interval	Dio Max Interval	Dao Min Interval	Dao Max Interval
2	Yes	0	0	0	0

RPL Instance

Instance Index	Instance Id	Do Dag Id	Do Dag VersionNo	Rank	Parent Count
1	0	0:0:0:0:0:0:0:0	0	0	0

RPL Parent

Parent Index	Instance In...	Route Index	IPv6 Addre...	IPv6 Addre...	Do Dag Ver...	PathEtx	LinkEtx	RSSI Forw...	RSSI Rever...

No content in table

Step 2 View the following information in the RPL Settings area:

- Interface Index: Identifies the interface.
- Enabled: Whether the RPL protocol is enabled.
- Dio Min Interval: Minimum DODAG Information Object (DIO) interval in RPL protocol.
- Dio Max Interval: Maximum DIO interval in RPL protocol.
- Dao Min Interval: Minimum Destination Advertisement Object (DAO) interval in RPL protocol.
- Dao Max Interval: Maximum DAO interval in RPL protocol.

Step 3 View the following information in the RPL Instance area:

- Instance Index: Identifies the RPL instance.
- Instance Id: Identifies an RPL instance, which is a set of one or more DODAGS. [RFC6550]

- Dodag Id: Identifies the DODAG root. The DODAGID is unique within the scope of a RPL instance in the LLN.
- Dodag VersionNo: A sequential counter that is incremented by the root to form a new DODAG version.
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the DAG's Objective Function (OF). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [RFC6550]
- Parent Count:

Step 4 View the following information in the RPL Parent area:

- Parent Index: Identifies the parent.
- Instance Index: Identifies the instance.
- Route Index: Identifies the route.
- IPv6 Address Local: Unique local IPv6 address of the parent.
- IPv6 Address Global: IPv6 global unicast address of the parent.
- Dodag VersionNo: A sequential counter that is incremented by the root to form a new DODAG version.
- PathEtx: Expected transmission count of the path. [rfc6550]
- LinkEtx: Expected transmission count of the link. [rfc6550]
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.
- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.
- Hops: Hop count.

Security

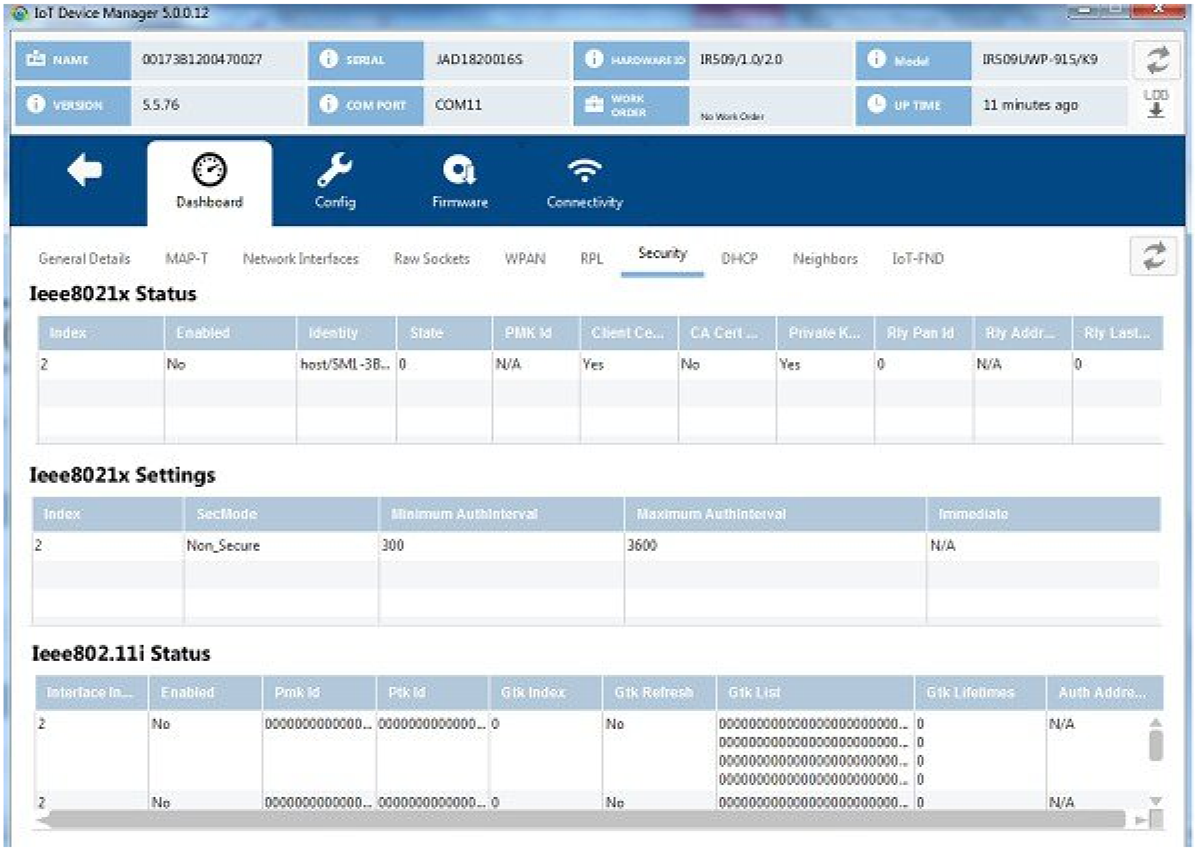
To view information about IEEE 802.1x for WPAN authentication and encryption:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Security** sub-tab.
2. View the information in the Ieee8021x Status area:
3. View the information in the Ieee8021x Settings area:
4. View the information in the Ieee80211i Status area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Security** sub-tab.



NAME	0017381200470027	SERIAL	JAD1820016S	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Ieee8021x Status

Index	Enabled	Identity	State	PMK Id	Client Ce...	CA Cert ...	Private K...	Rly Pan Id	Rly Addr...	Rly Last...
2	No	host/SML-3B...	0	N/A	Yes	No	Yes	0	N/A	0

Ieee8021x Settings

Index	SecMode	Minimum AuthInterval	Maximum AuthInterval	Immediate
2	Non_Secure	300	3600	N/A

Ieee802.11i Status

Interface In...	Enabled	Pmk Id	Ptk Id	Gtk Index	Gtk Refresh	Gtk List	Gtk Lifetimes	Auth Addre...
2	No	0000000000000...	0000000000000...	0	No	000000000000000000000000... 000000000000000000000000... 000000000000000000000000... 000000000000000000000000...	0 0 0 0	N/A
2	No	0000000000000...	0000000000000...	0	No	000000000000000000000000...	0	N/A

Step 2 View the information in the Ieee8021x Status area:

- Index: Identifies the network.
- Enabled: Whether 802.1x authentication is enabled.
- Identity: Subject of the X.509 digital certificate.
- State: Current state of Transport Layer Security (TLS).
- PMK Id: Pairwise Master Key identifier.
- Client Certificate:
- CA Certificate: Certificate Authority (CA) certificate
- Private Key: Encryption/decryption key.
- Rly Pan Id: Reply PAN ID.
- Rly Address: Reply address.
- Rly Last Heard: Time of last heard reply.

Step 3 View the information in the Ieee8021x Settings area:

- Index: Identifies the network.
- SecMode: The security mode in use.

- Minimum Auth Interval: The minimum authentication interval.
- Maximum Auth Interval: The maximum authentication interval.
- Immediate: Request authentication immediately.

Step 4 View the information in the Ieee80211i Status area:

- Interface Index: Identifies the interface.
- Enabled: Whether the 80211i protocol is enabled.
- Pmk Id: Pairwise Master Key identifier.
- Ptk Id: Pairwise Transient Key identifier.
- Gtk Index: Identifies the Group Temporal Key.
- Gtk Refresh:
- Gtk List: Group Temporal Key list.
- Gtk Lifetimes:
- Auth Address: Authenticator server address.

DHCP

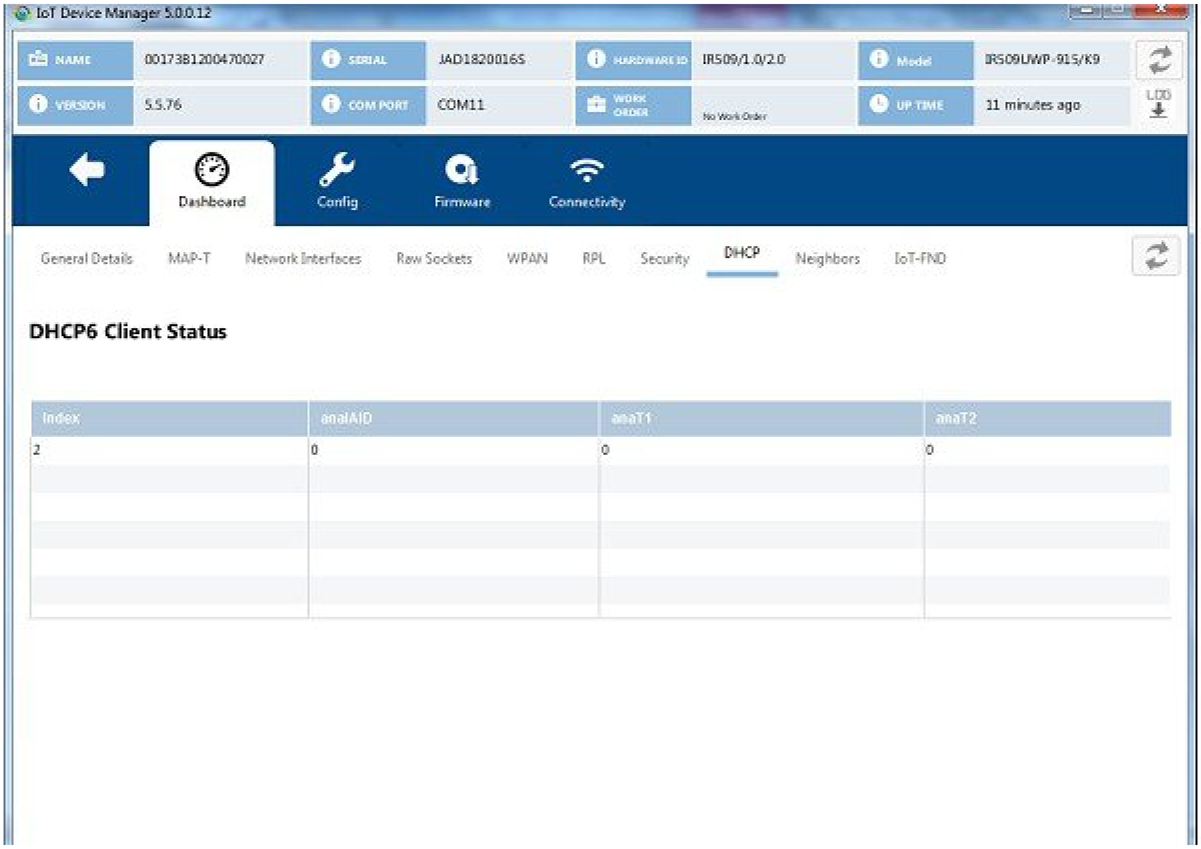
To view information about DHCPv6 for IPv6 address allocation:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **DHCP** sub-tab.
2. View the DHCP Client Status:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **DHCP** sub-tab.



NAME 00173B1200470027

SERIAL JAD18200165

HARDWARE ID IR509/1.0/2.0

Model IR509UWP-915/K9

VERSION 5.5.76

COM PORT COM11

WORK ORDER No Work Order

UP TIME 11 minutes ago

DHCP6 Client Status

Index	analAID	anaT1	anaT2
2	0	0	0

Step 2 View the DHCP Client Status:

- Index: Identifies the network.
- analAID: Interface Association Identifier.
- anaT1: Preferred-lifetime.
- anaT2: Valid-lifetime.

Neighbors

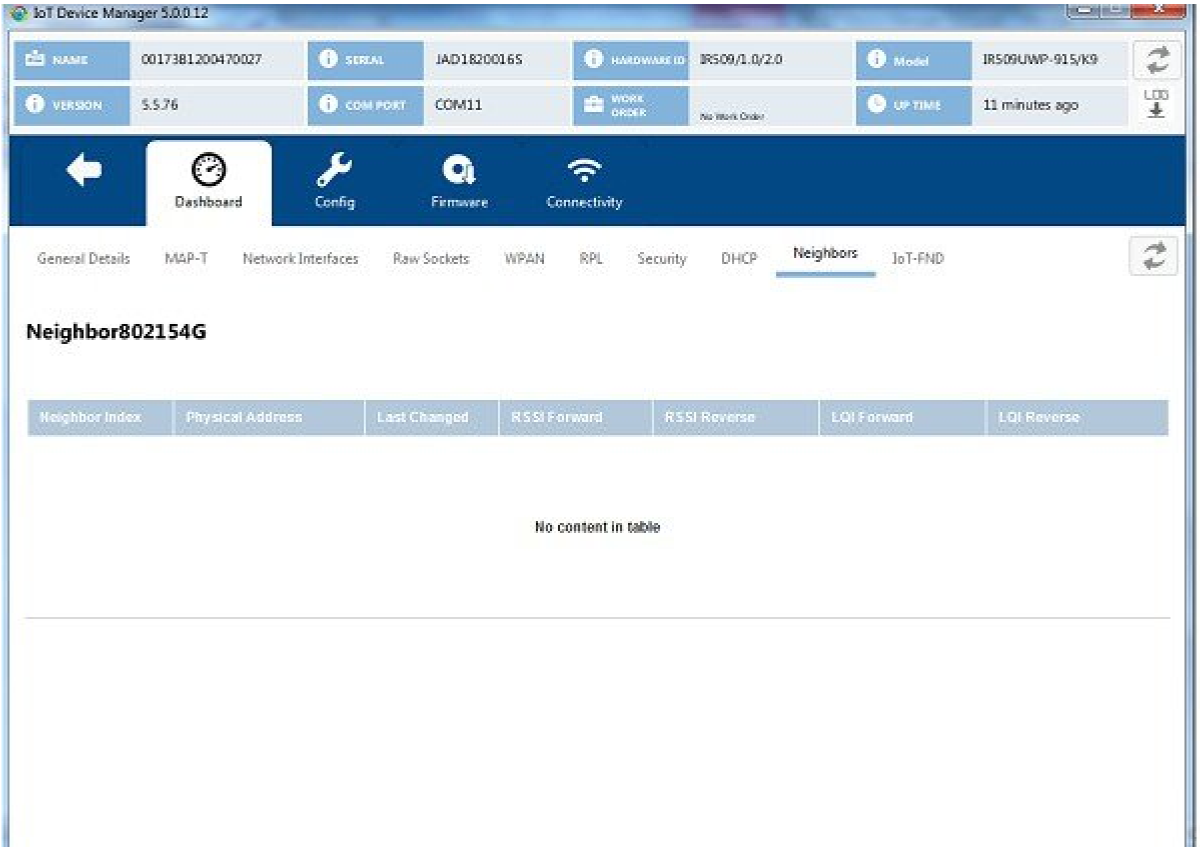
To view 802.15.4g neighbor information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Neighbors** sub-tab.
2. View the neighbors settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Neighbors** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Neighbor802154G

Neighbor Index	Physical Address	Last Changed	RSSI Forward	RSSI Reverse	LQI Forward	LQI Reverse

No content in table

Step 2 View the neighbors settings and statistics:

- Neighbor Index: Identifies the neighbor
- Physical Address: The 64-bit Extended Unique Identifier (EUI-64) of the device.
- Last Changed: The time (in hundredths of a second) since hearing from the neighbor.
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.
- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.

IoT-FND

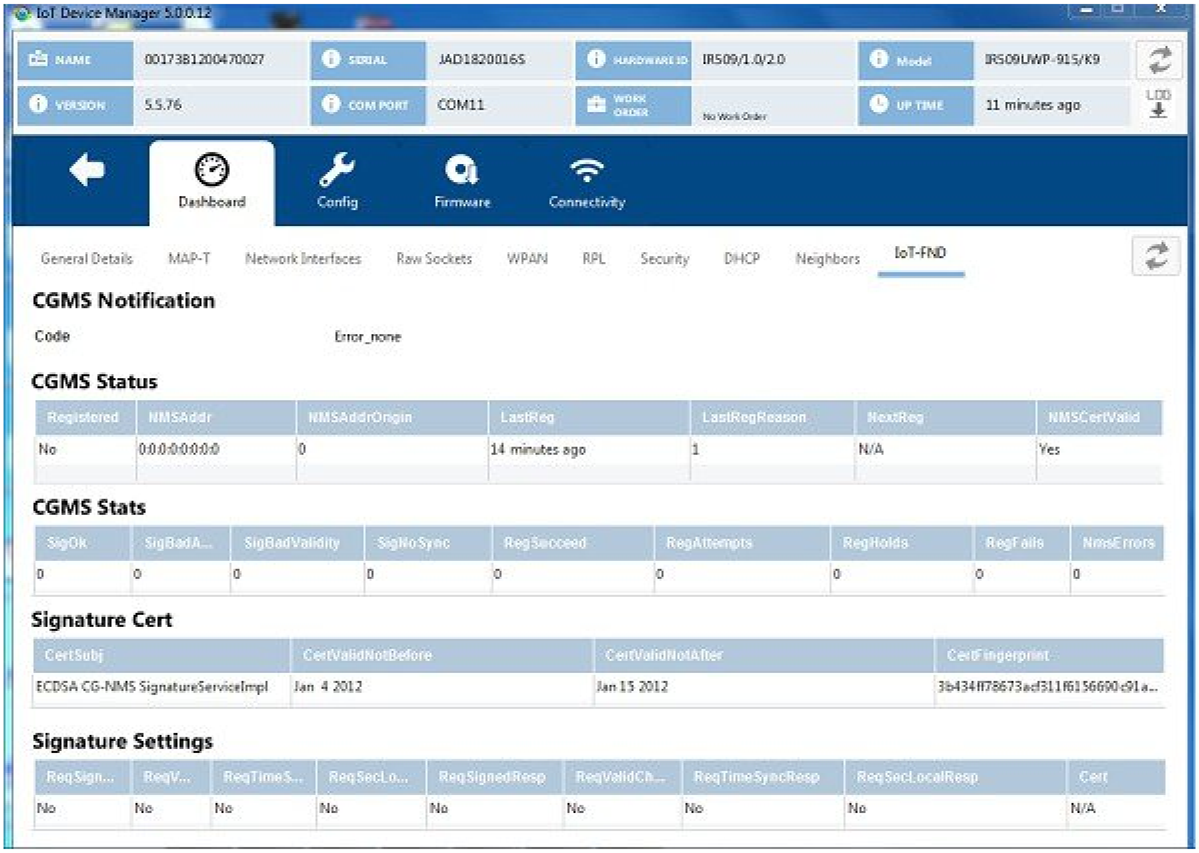
To view information about IoT-FND:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **IoT-FND** sub-tab.
2. View the information in the CGMS notification area:
3. View CGMS Status information:
4. View CGMS Stats:
5. View Signature Cert information:
6. View the Signature Settings information:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **IoT-FND** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

CGMS Notification

Code Error_none

CGMS Status

Registered	NMSAddr	NMSAddrOrigin	LastReg	LastRegReason	NextReg	NMSCertValid
No	0:0:0:0:0:0:0:0	0	14 minutes ago	1	N/A	Yes

CGMS Stats

SigOk	SigBadA...	SigBadValidity	SigNoSync	RegSucceed	RegAttempts	RegHolds	RegFails	NmsErrors
0	0	0	0	0	0	0	0	0

Signature Cert

CertSubj	CertValidNotBefore	CertValidNotAfter	CertFingerprint
ECDSA CG-NMS SignatureServiceImpl	Jan 4 2012	Jan 15 2012	3b434ff78673acf311f6156690c91a...

Signature Settings

ReqSign...	ReqV...	ReqTimeS...	ReqSecLo...	ReqSignedResp	ReqValidCh...	ReqTimeSyncResp	ReqSecLocalResp	Cert
No	No	No	No	No	No	No	No	N/A

Step 2 View the information in the CGMS notification area:

Code Values:

- 1 = COAP Error
- 2 = Signature Error
- 3 = Registration Processing Error

Step 3 View CGMS Status information:

- Registered: Whether the end point is registered with NMS.
- NMSAddr: Address of NMS.
- NMSAddrOrigin: Origin of NMS address.
- LastReg: Last registration time.
- LastRegReason: Reason for last registration.
- NextReg: Time of next registration.
- NMSCertValid: Whether the certificate is valid.

Step 4 View CGMS Stats:

- SigOk: Count of verified signatures.
- SigBadAuth: Count of bad authorized signatures.
- SigBadValidity: Count of bad validity signatures.
- SigNoSync: Count of signatures that are not synchronized.
- RegSucceed: Count of successful registrations.
- RegAttempts: Count of registration attempts.
- RegHolds: Count of registration holds.
- RegFails: Count of registration failures.
- NmsErrors: Count of NMS errors.

Step 5 View Signature Cert information:

- CertSubj: Certificate subject.
- CertValidNotBefore: Certificate valid.
- CertValidNotAfter: Certificate not valid.
- CertFingerprint: Fingerprint of the certificate.

Step 6 View the Signature Settings information:

- ReqSignedPost: Whether request signed post.
- ReqValidCheckPost: Whether request valid check post.
- ReqTimeSyncPost: Whether request time synchronization post.
- ReqSecLocalPost: Whether request security local post.
- ReqSignedResp: Whether request signed response.
- ReqValidCheckResp: Whether valid check response.
- ReqTimeSyncResp: Whether time synchronization response.

- ReqSecLocalResp: Whether request security local response.

ACL

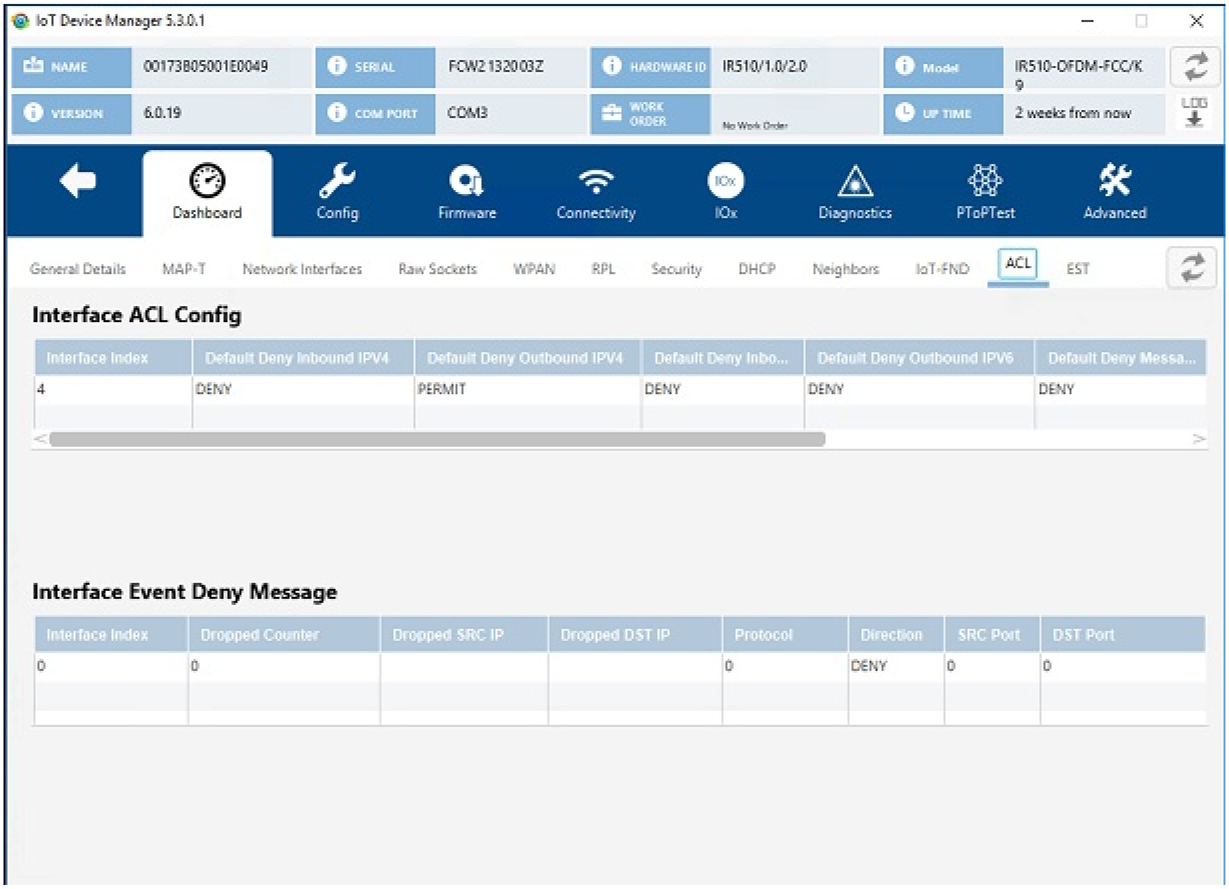
To view Access Control List (ACL) information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **ACL** sub-tab.
2. View the ACL settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **ACL** sub-tab.



NAME	00173B05001E0049	SERIAL	FCW2132003Z	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.0.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	2 weeks from now

Interface ACL Config

Interface Index	Default Deny Inbound IPV4	Default Deny Outbound IPV4	Default Deny Inbo...	Default Deny Outbound IPV6	Default Deny Messa...
4	DENY	PERMIT	DENY	DENY	DENY

Interface Event Deny Message

Interface Index	Dropped Counter	Dropped SRC IP	Dropped DST IP	Protocol	Direction	SRC Port	DST Port
0	0			0	DENY	0	0

Step 2 View the ACL settings and statistics:

- Interface ACL Config

- Interface Event Deny Message

EST

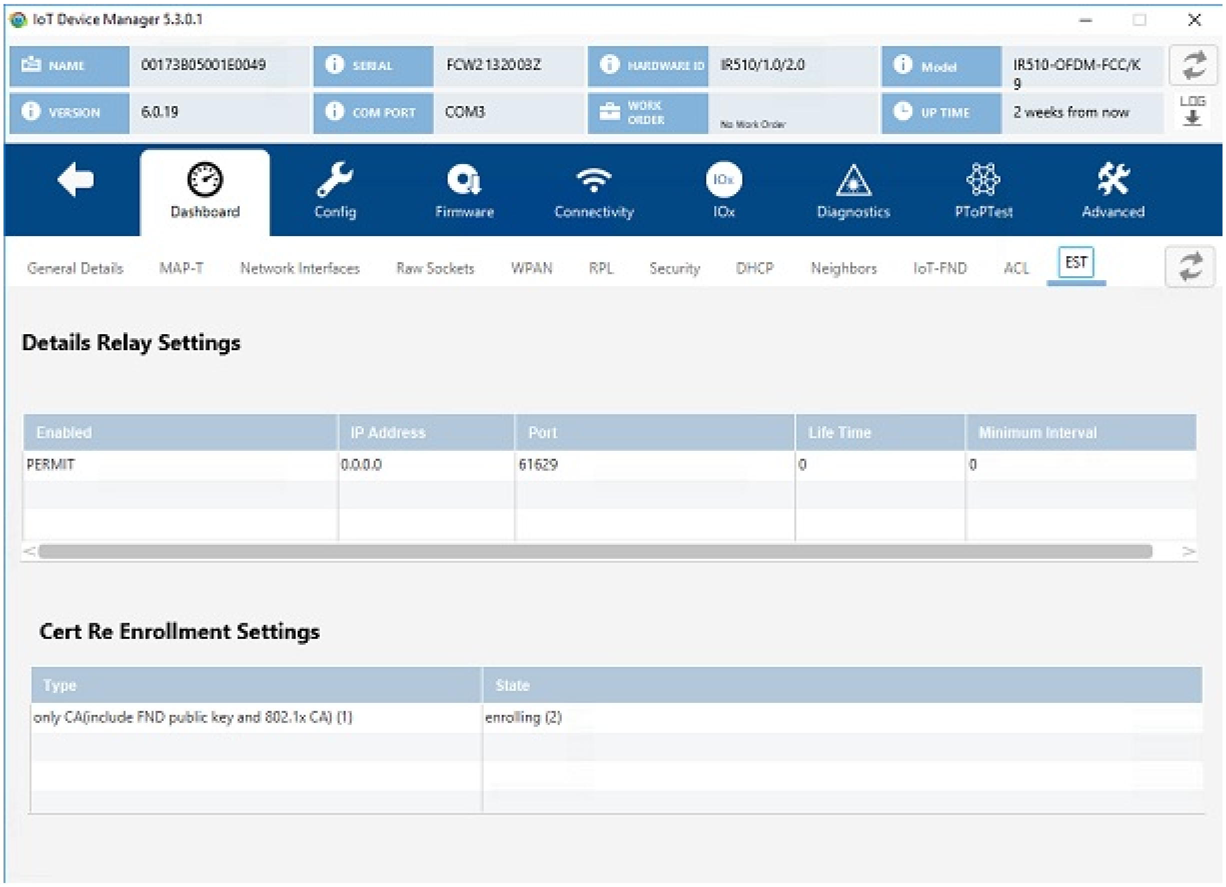
To view Enrollment settings (EST) information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **EST** sub-tab.
2. View the EST settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **EST** sub-tab.



Details Relay Settings

Enabled	IP Address	Port	Life Time	Minimum Interval
PERMIT	0.0.0.0	61629	0	0

Cert Re Enrollment Settings

Type	State
only CA(include FND public key and 802.1x CA) (1)	enrolling (2)

Step 2 View the EST settings and statistics:

- Details Relay Settings

- Cert Re Enrollment Settings

Viewing Interface Details

You can view details for the Ethernet and the two serial interfaces from the Device Manager main page (Dashboard).

Ethernet Interface Details

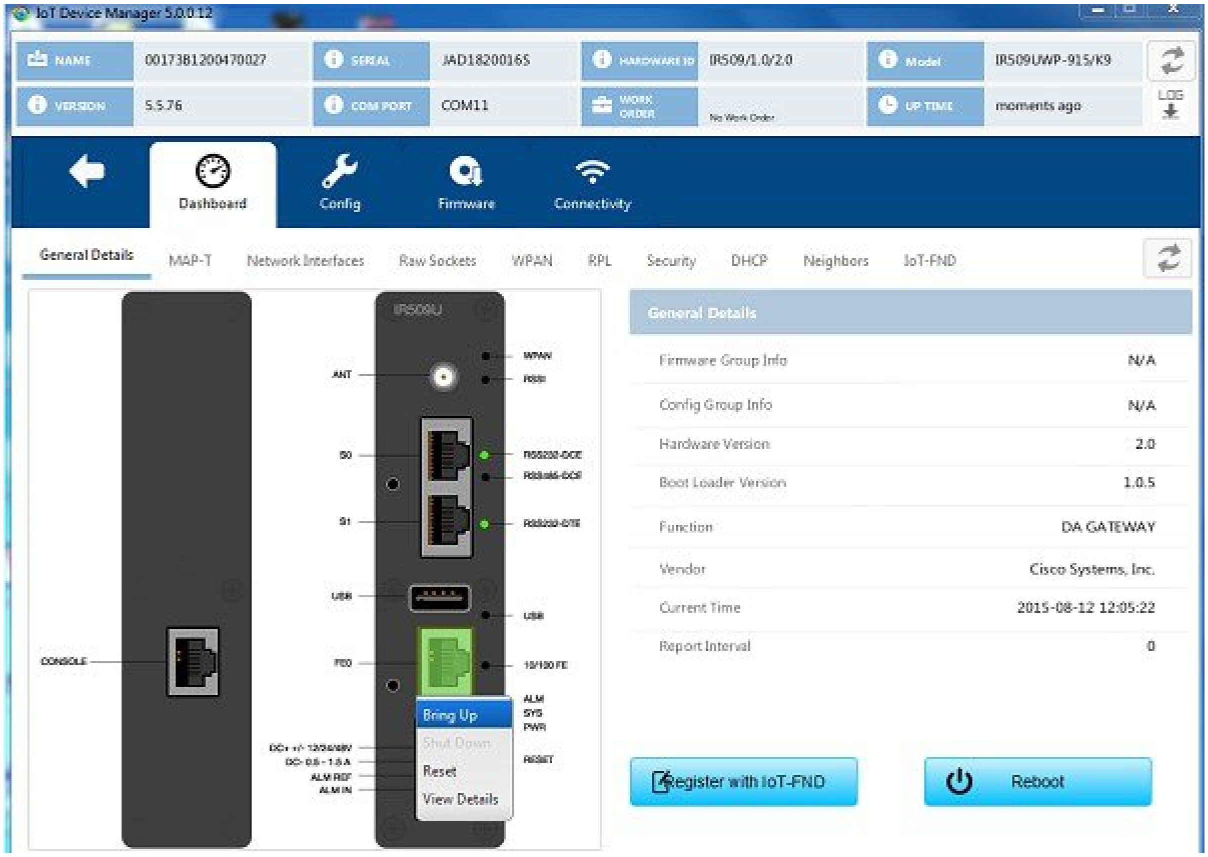
To view details for the Ethernet interface:

SUMMARY STEPS

1. On the Device Manager main page, click the Ethernet port to display the popup menu and select **View Details**.
2. To refresh the display, click the refresh icon in the upper right corner of the View Details window.

DETAILED STEPS

Step 1 On the Device Manager main page, click the Ethernet port to display the popup menu and select **View Details**.

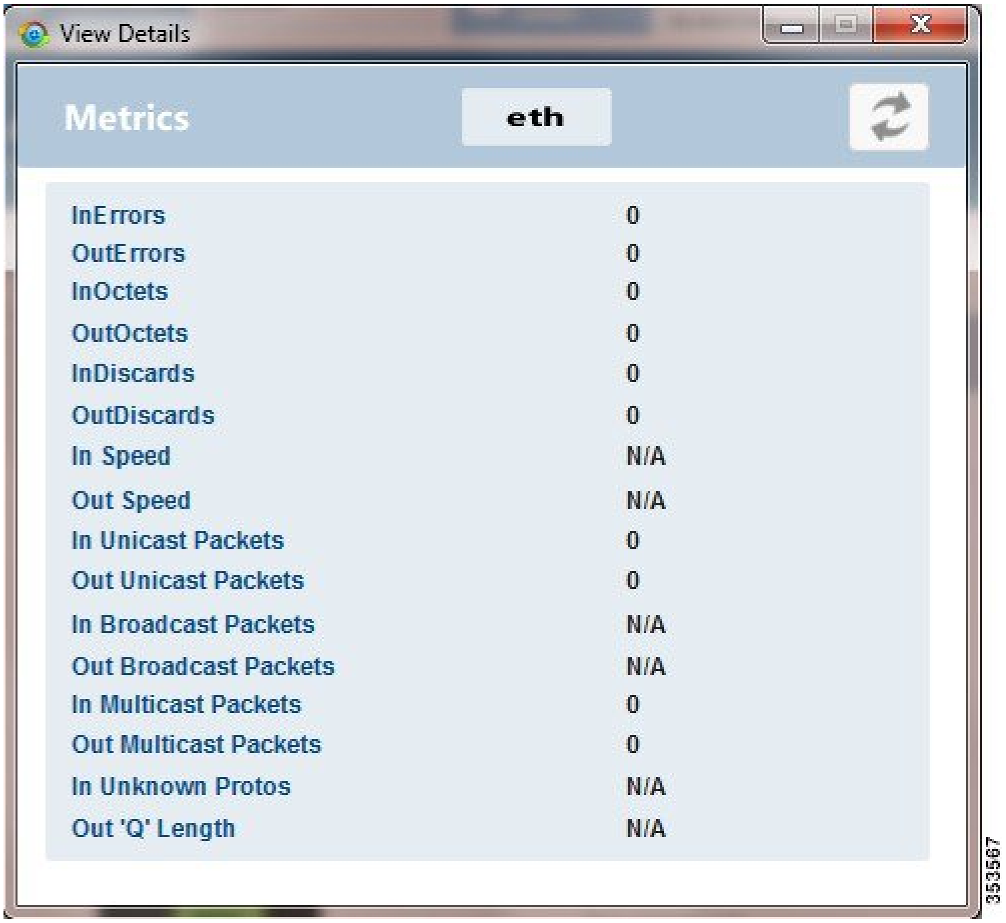


IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details	
Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

The View Details window displays the Ethernet metrics.



InErrors	0
OutErrors	0
InOctets	0
OutOctets	0
InDiscards	0
OutDiscards	0
In Speed	N/A
Out Speed	N/A
In Unicast Packets	0
Out Unicast Packets	0
In Broadcast Packets	N/A
Out Broadcast Packets	N/A
In Multicast Packets	0
Out Multicast Packets	0
In Unknown Protos	N/A
Out 'Q' Length	N/A

Step 2 To refresh the display, click the refresh icon in the upper right corner of the View Details window.

Serial Interface Details

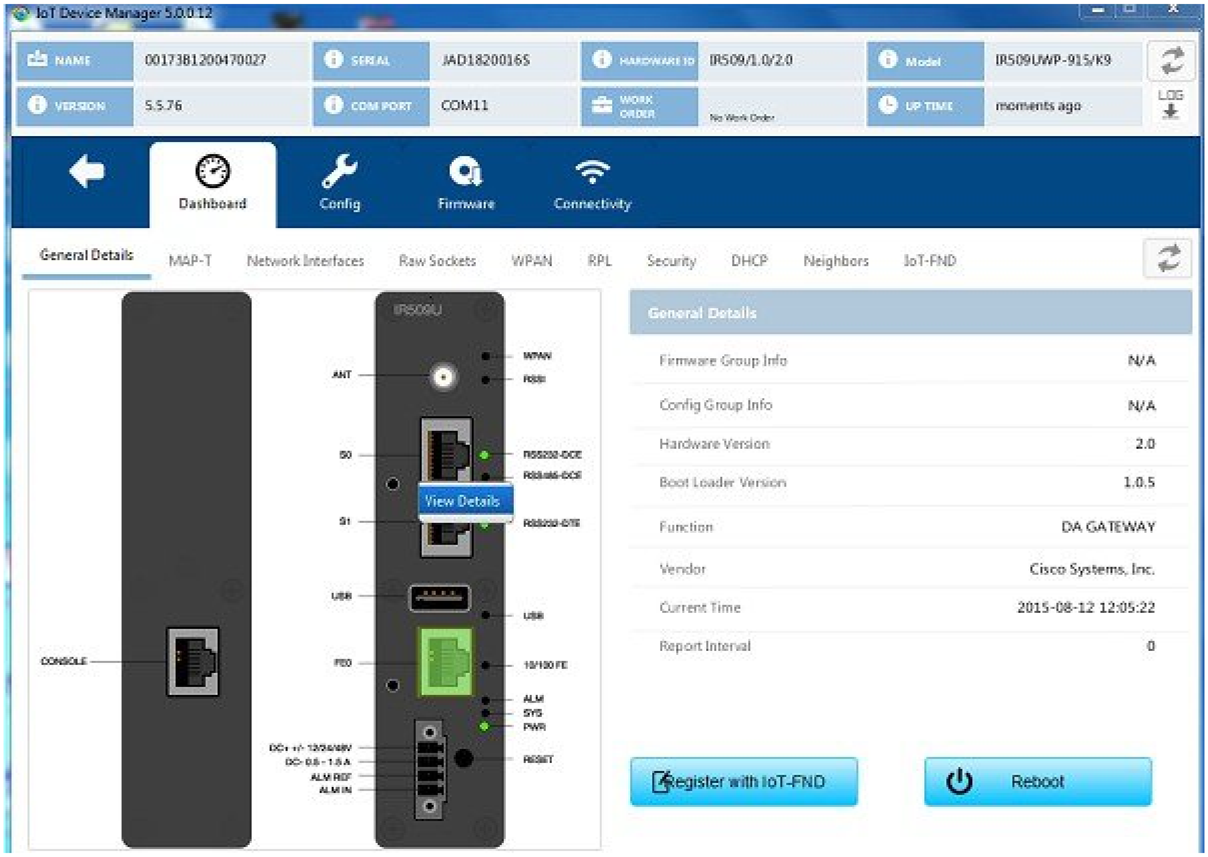
To view details for serial interface 0 (DCE) or serial interface 1 (DTE):

SUMMARY STEPS

1. On the On the Device Manager main page, click a serial port to display the popup menu and select **View Details**.
2. To refresh the display, click the refresh icon in the upper right corner of the View Details window.

DETAILED STEPS

Step 1 On the On the Device Manager main page, click a serial port to display the popup menu and select **View Details**.



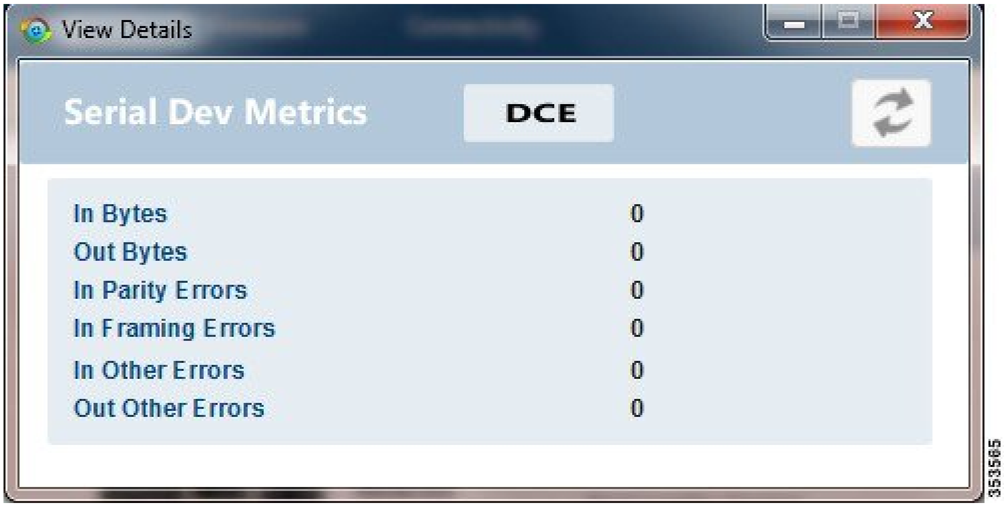
IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

The View Details window displays the DCE or DTE metrics.



View Details

Serial Dev Metrics DCE

In Bytes	0
Out Bytes	0
In Parity Errors	0
In Framing Errors	0
In Other Errors	0
Out Other Errors	0

Step 2 To refresh the display, click the refresh icon in the upper right corner of the View Details window.

Managing the Ethernet Interface

To bring up, shut down, or reset the Ethernet interface:

SUMMARY STEPS

1. On the Device Manager main page, click the Ethernet port to display the popup menu and select the operation you want to perform on the interface: **Bring Up**, **Shut Down**, or **Reset**.
2. In the confirmation dialog box that appears, click **Yes** to continue the operation.

DETAILED STEPS

Step 1 On the Device Manager main page, click the Ethernet port to display the popup menu and select the operation you want to perform on the interface: **Bring Up**, **Shut Down**, or **Reset**.

Step 2 In the confirmation dialog box that appears, click **Yes** to continue the operation.

Registering with IoT-FND

When you connect to the IR500 with a work order, the IR500 registers with IoT-FND. Registration notifies IoT-FND that the device is on the network and provides a mechanism for pushing management configuration information to the device.

You can also manually cause the IR500 to re-register with IoT-FND for load balancing or delegation to specific sites. In this case, IoT-FND redirects the IR500 to re-register with an alternate IoT-FND.

To register with IoT-FND, on the Device Manager main page (Dashboard), click **Register with IoT-FND**. Device Manager displays messages to inform you of the redirection status.

Rebooting the IR500

To immediately reboot the IR500, on the Device Manager main page (Dashboard), click **Reboot**. Device Manager displays messages to inform you of the reboot status.

Changing the Configuration

You can view or change the following IR500 settings from the Config page:

Note For detailed information about IR500 operation and configuration, including Raw Socket and MAP-T information, refer to the Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide .

Changing General Settings

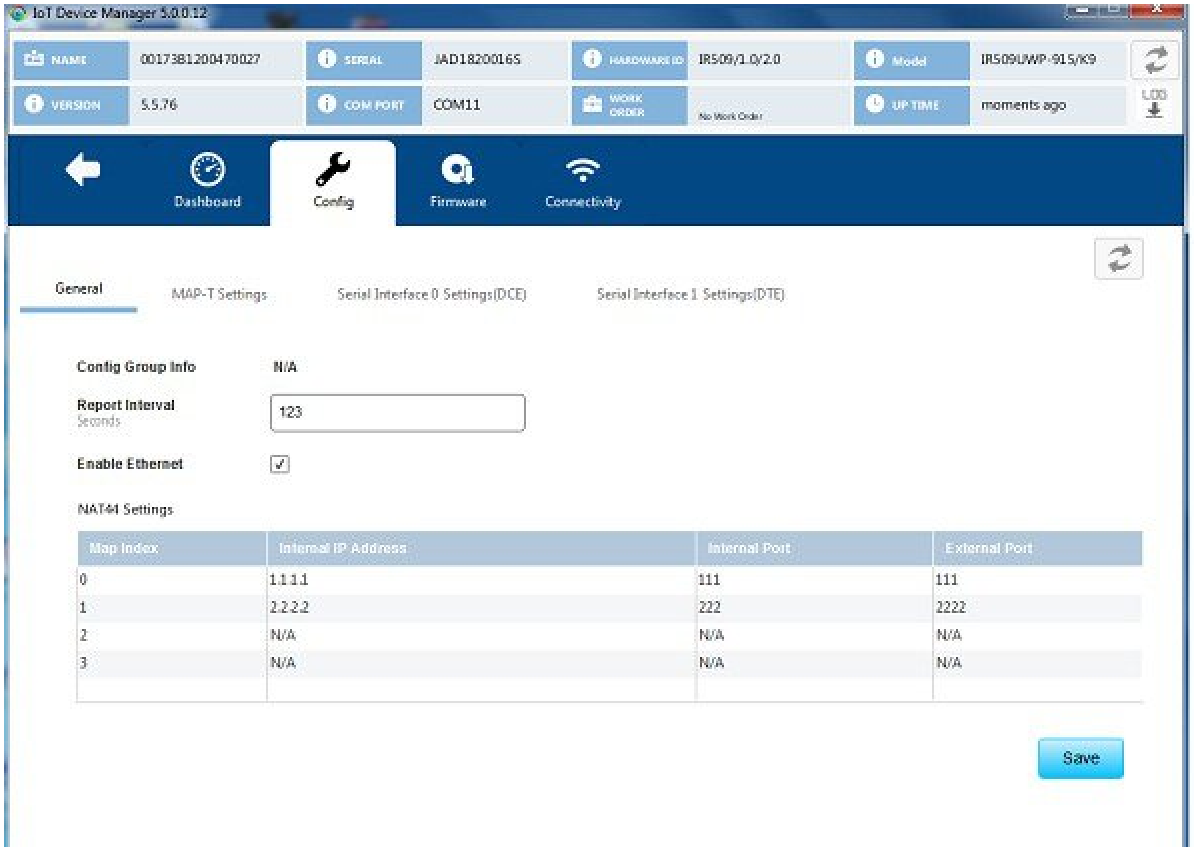
To view or change general IR500 configuration settings:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. View or modify General settings:
3. Click Save.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
LOG
Save

NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

Config Group Info N/A

Report Interval (Seconds) 123

Enable Ethernet ☑

NAT44 Settings

Map Index	Internal IP Address	Internal Port	External Port
0	1.1.1.1	111	111
1	2.2.2.2	222	2222
2	N/A	N/A	N/A
3	N/A	N/A	N/A

Step 2 View or modify General settings:

- **Config Group Info**: The configuration group that IoT-FND uses to manage devices in bulk. The default config group for the DA Gateway is **default-ir500**.
- **Report Interval**: The number of seconds between data updates. By default, Mesh Endpoints (MEs) send a new set of metrics to IoT-FND every 28,800 seconds (8 hours).
- **Enable Ethernet**: Select this check box for IPv4 connectivity to devices and to enable NAT44 configuration.

- **NAT44 Settings**:
  - Map Index: Identifies the map.
  - Internal IP Address: The internal address of the NAT 44 configured device.
  - Internal Port: The internal port number of the NAT 44 configured device.
  - External Port: The external port number of the NAT 44 configured device.

Step 3 Click Save.

Changing MAP-T Settings

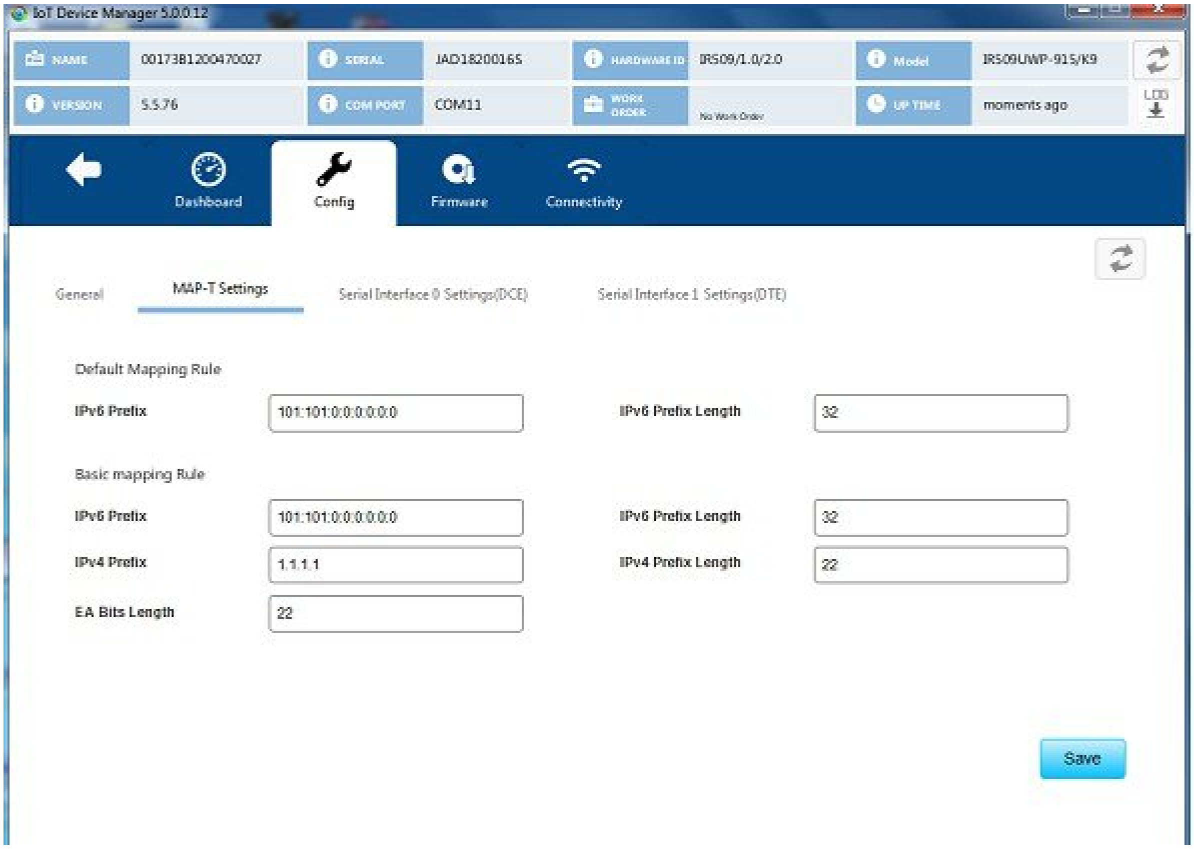
To view or change MAP-T configuration settings:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **MAP-T Settings** and view or modify these settings:
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
LOD
Save

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

Default Mapping Rule

IPv6 Prefix	101:101:0:0:0:0:0:0	IPv6 Prefix Length	32

Basic mapping Rule

IPv6 Prefix	101:101:0:0:0:0:0:0	IPv6 Prefix Length	32
IPv4 Prefix	1.1.1.1	IPv4 Prefix Length	22
EA Bits Length	22		

Step 2 Click **MAP-T Settings** and view or modify these settings:

- Default Mapping Rule: These fields specify an IPv6 prefix used to address all destinations outside the MAP-T domain.
  - **IPV6 Prefix**: IPv6 prefix used to embed any IPv4 addresses outside the MAP-T domain.
  - **IPV6 Prefix Length**: Length of the IPv6 prefix used to embed any IPv4 addresses outside the MAP-T domain.
- Basic Mapping Rule: These fields specify the IPv6 and IPv4 prefixes used to address MAP-T nodes inside the MAP-T domain.
  - **IPV6 Prefix**: MAP-T IPv6 End-user prefix, which contains the MAP-T Basic Mapping Rule or MAP-T IPv6 prefix + the IPv4 suffix of the assigned IPv4 address.
  - **IPV4 Prefix**: IPv4 prefix that specifies the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain.
  - **EA Bits Length**: Length of the IPv4 Embedded Address (EA) bits that indicates the length of the IPv4 suffix embedded in the MAP-T IPv6 End-user IPv6 prefix.
  - **IPV6 Prefix Length**: Length of the IPv6 prefix used to embed the IPv4 address of nodes inside the MAP-T domain.
  - **IPV4 Prefix Length**: Length of the IPv4 prefix that specifies the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain.

Step 3 Click **Save**.

Changing Serial Interface 0 Settings (DCE)

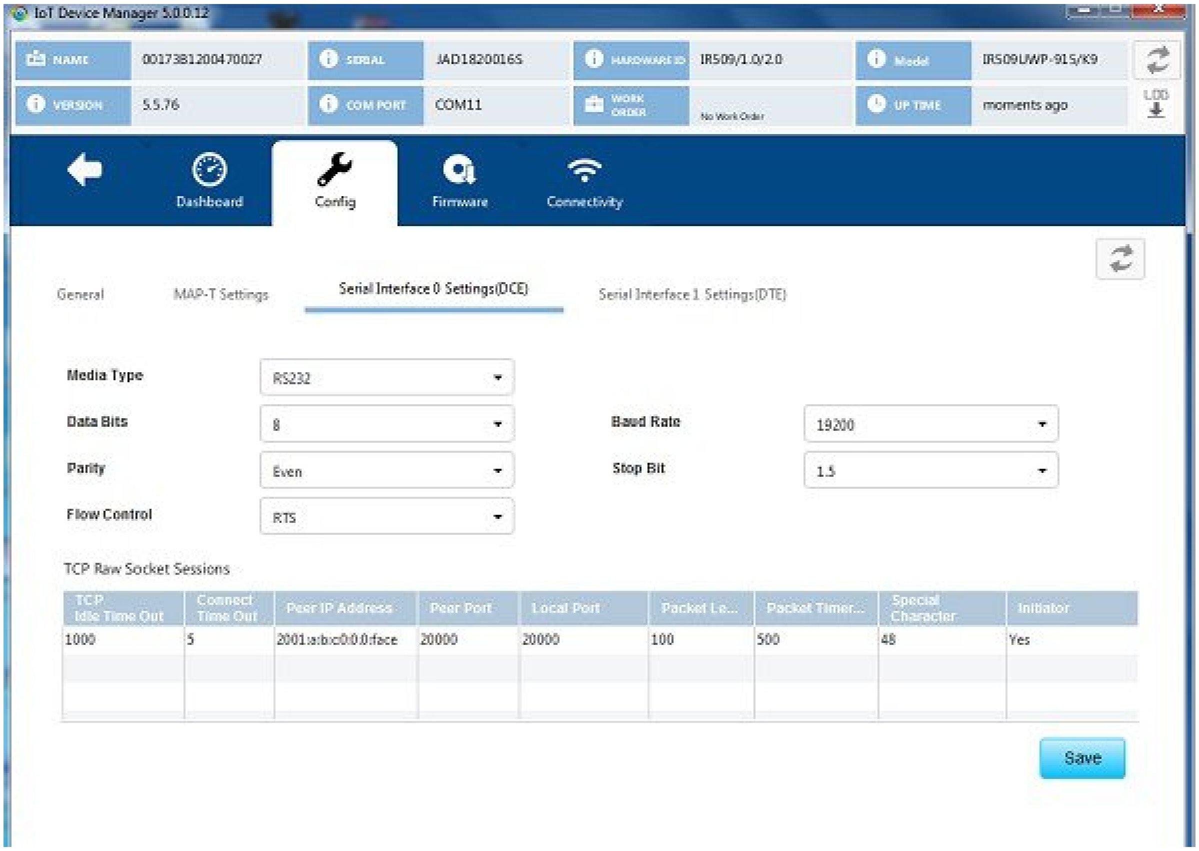
To view or change the configuration for Serial Interface 0 (DCE):

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Serial Interface 0 Settings (DCE)** and view or modify these settings:
3. View or modify settings for TCP Raw Socket Sessions:
4. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
LOG
Save

NAME	0017381200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

Media Type: RS232
Data Bits: 8
Baud Rate: 19200
Parity: Even
Stop Bit: 1.5
Flow Control: RTS

TCP Raw Socket Sessions

TCP Idle Time Out	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Le...	Packet Timer...	Special Character	Initiator
1000	5	2001:a:b:c0:0:0:face	20000	20000	100	500	48	Yes

Step 2 Click **Serial Interface 0 Settings (DCE)** and view or modify these settings:

- **Media Type**: The serial interface type.
  - Disable

    - LoopBack
    - RS232
    - RS485 Full Duplex
    - RS485 Half Duplex

- **Data Bits**: Number of data bits per character. Default value is 8.
- **Parity**: Odd or even parity for error detection. Default value is None.
- **Flow Control**: The use of flow control on the line. Default value is None.
- **Baud Rate**: Data transmission rate in bits per second. Default value is 115200.
- **Stop Bit**: The asynchronous line stop bit. Default value is 1.

Step 3 View or modify settings for TCP Raw Socket Sessions:

- **TCP Idle Time Out**: The time to maintain an idle connection.
- **Connect Time Out**: TCP client connect timeout for Initiator DA Gateway devices.
- **Peer IP Address**: IP address of the host connected to the device.
- **Peer Port**: Port number of the client/server connected to the device.
- **Local Port**: Port number of the device.
- **Packet Length**: Maximum length of serial data to convert into the TCP packet.
- **Packet Timer (ms)**: The time interval between each TCP packet creation.
- Special Character: The delimiter for TCP packet creation.
- **Initiator**: Designates the device as the client/server.

Step 4 Click **Save**.

Changing Serial Interface 1 Settings (DTE)

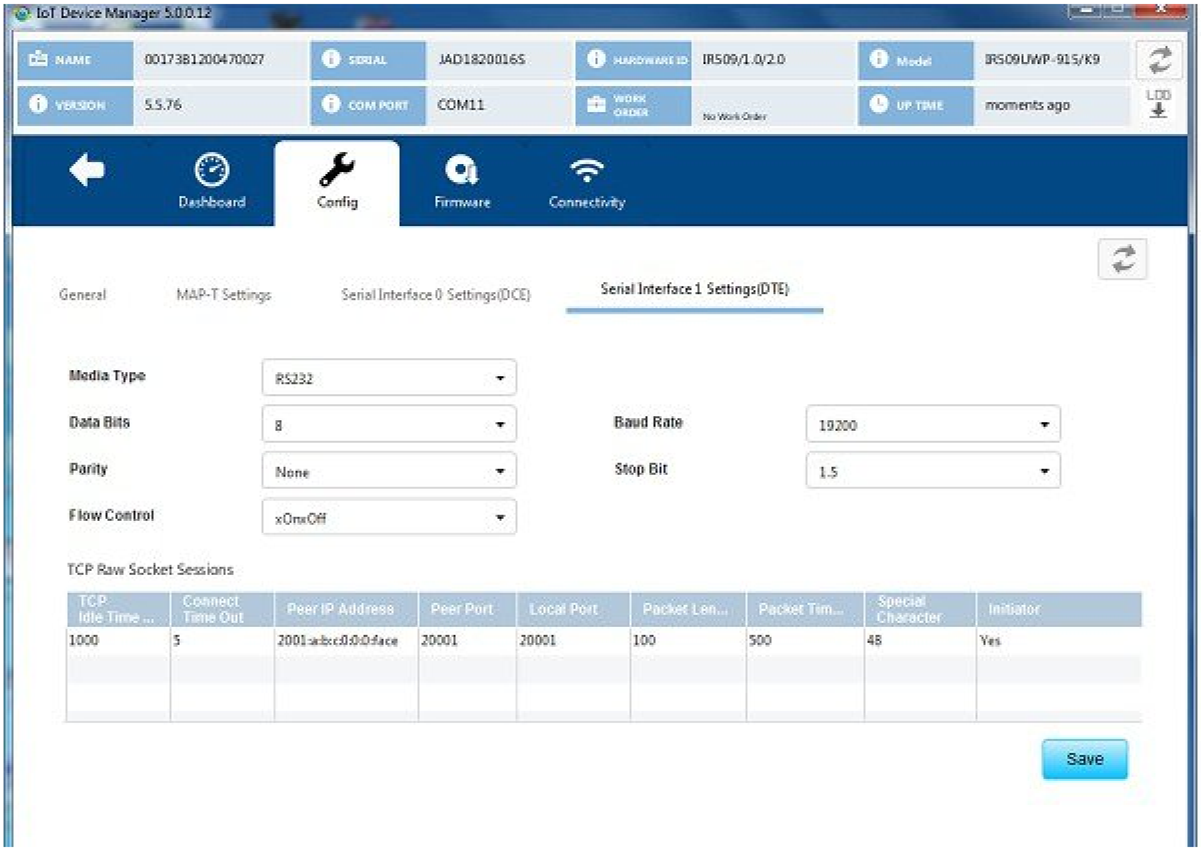
To view or change the configuration for Serial Interface 1 (DTE):

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Serial Interface 1 Settings (DTE)** and view or modify these settings:
3. View or modify settings for TCP Raw Socket Sessions.
4. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
LDD
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
Save

NAME 0017381200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

Media Type: RS232
Data Bits: 8
Baud Rate: 19200
Parity: None
Stop Bit: 1.5
Flow Control: xOnxOff

TCP Raw Socket Sessions

TCP Idle Time ...	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Len...	Packet Tim...	Special Character	Initiator
1000	5	2001:a:b:c:0:0:0:face	20001	20001	100	500	48	Yes

Step 2 Click **Serial Interface 1 Settings (DTE)** and view or modify these settings:

- **Medial Type**: The serial interface type.
  - Disable
  - LoopBack
  - RS232
  - RS485 Full Duplex
  - RS485 Half Duplex
- **Data bits**: The number of data bits per character. Default value is 8.
- **Parity**: Odd or even parity for error detection. Default value is None.
- **Flow Control**: The use of flow control on the line. Default value is None.
- **Baud Rate**: The data transmission rate in bits per second. Default value is 115200.
- **Stop Bit**: The asynchronous line stop bit. Default value is 1.

Step 3 View or modify settings for TCP Raw Socket Sessions.

- **TCP Idle Time Out**: The time to maintain an idle connection.
- **Connect Time Out**: TCP client connect timeout for Initiator DA Gateway devices.
- **Peer IP Address**: IP address of the host connected to the device.
- **Peer Port**: Port number of the client/server connected to the device.
- **Local Port**: Port number of the device.
- **Packet Length**: Maximum length of serial data to convert into the TCP packet.
- **Packet Timer (ms)**: The time interval between each TCP packet creation.
- Special Character: The delimiter for TCP packet creation.
- **Initiator**: Designates the device as the client/server.

Step 4 Click **Save**.

Changing ACL Settings

To view or change ACL configuration settings:

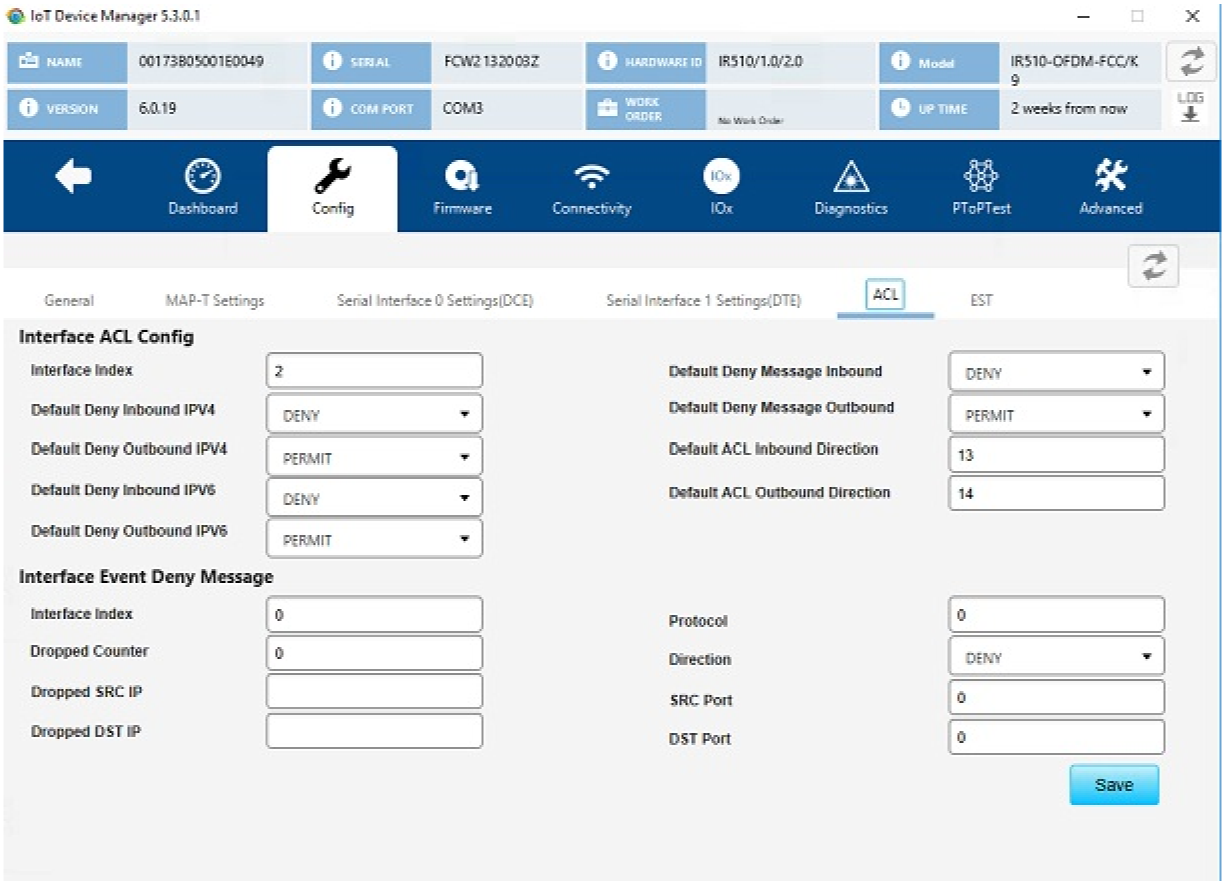
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click the **ACL** tab and view or modify the settings.
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **ACL** tab and view or modify the settings.



NAME	00173B05001E0049	SERIAL	FCW2132003Z	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.0.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	2 weeks from now

Interface ACL Config

Interface Index	2	Default Deny Message Inbound	DENY
Default Deny Inbound IPV4	DENY	Default Deny Message Outbound	PERMIT
Default Deny Outbound IPV4	PERMIT	Default ACL Inbound Direction	13
Default Deny Inbound IPV6	DENY	Default ACL Outbound Direction	14
Default Deny Outbound IPV6	PERMIT		

Interface Event Deny Message

Interface Index	0	Protocol	0
Dropped Counter	0	Direction	DENY
Dropped SRC IP		SRC Port	0
Dropped DST IP		DST Port	0

Step 3 Click **Save**.

Changing EST Settings

To view or change EST settings:

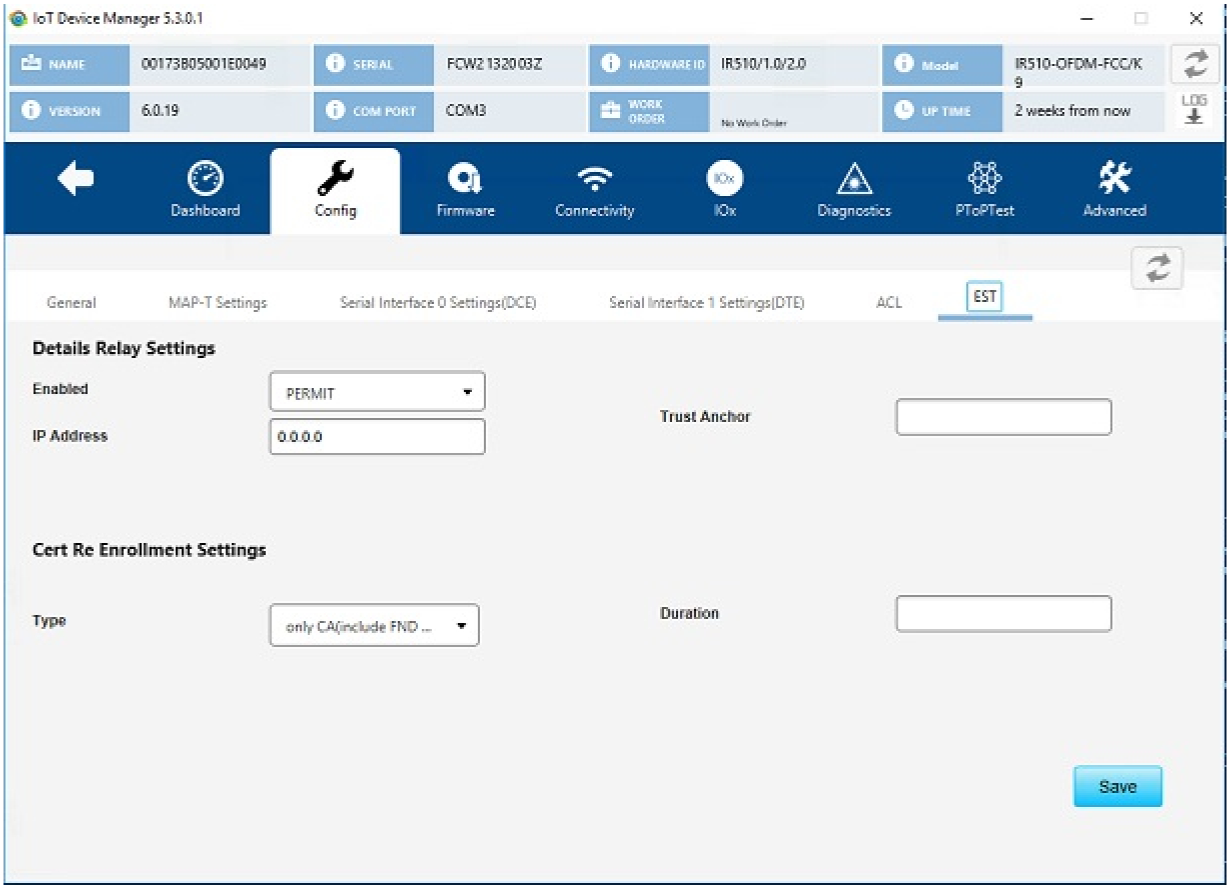
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click the **EST** tab and view or modify the settings.
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **EST** tab and view or modify the settings.



NAME: 00173B05001E0049
SERIAL: FCW2132003Z
HARDWARE ID: IR510/1.0/2.0
Model: IR510-OFDM-FCC/K9
VERSION: 6.0.19
COM PORT: COM3
WORK ORDER: No Work Order
UP TIME: 2 weeks from now

Details Relay Settings

Enabled: PERMIT

IP Address: 0.0.0.0

Trust Anchor:

Cert Re Enrollment Settings

Type: only CA(include FND ...

Duration:

Step 3 Click **Save**.

Generating and Uploading Bootstrap Configuration

To generate and upload bootstrap configuration files, follow these steps:

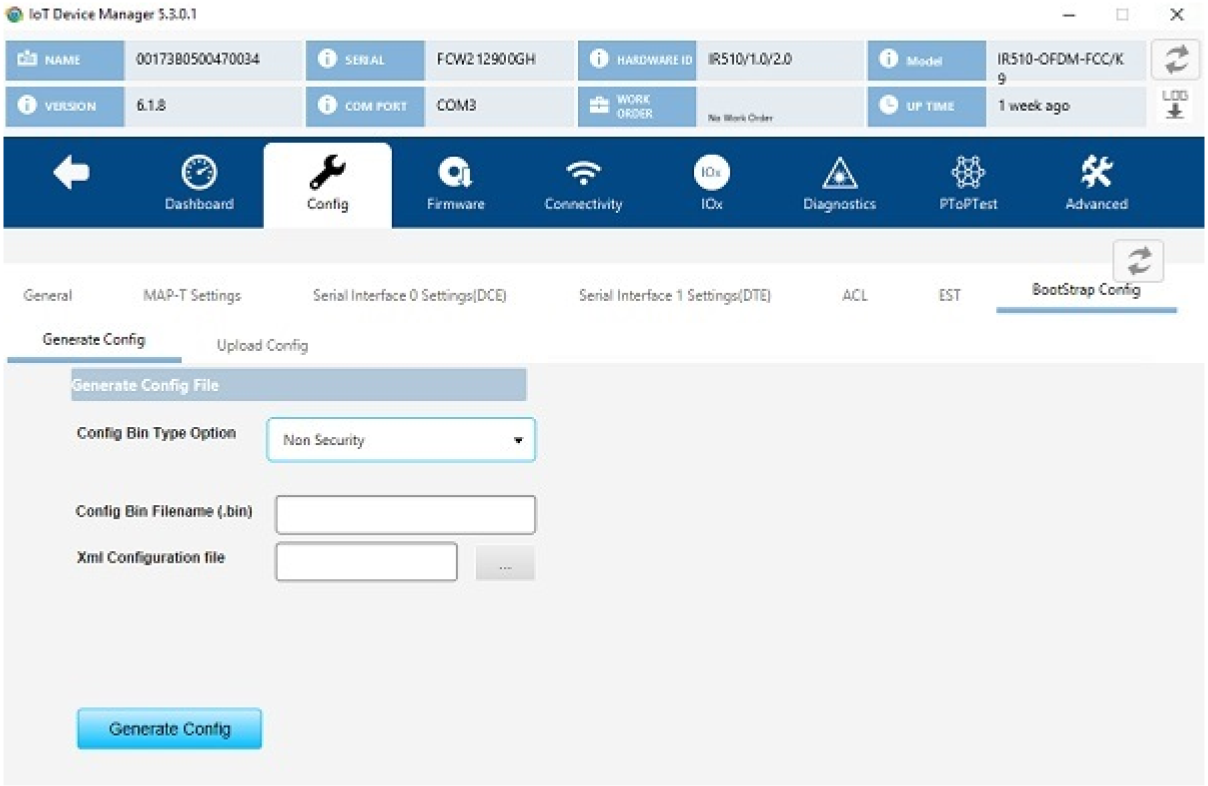
Before you begin

From IoT Device Manager Release 5.5, you can generate and upload bootstrap configuration files to one or more IR510 devices with Cisco Resilient Mesh Release 6.0 and later.

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **BootStrap Config** tab and then click the **Generate Config** subtab.

a) To generate non security bootstrap configurations, choose **Non Security** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, and browse to choose the XML configuration file to be provided as input, as shown in the following figure.



IoT Device Manager 5.3.0.1

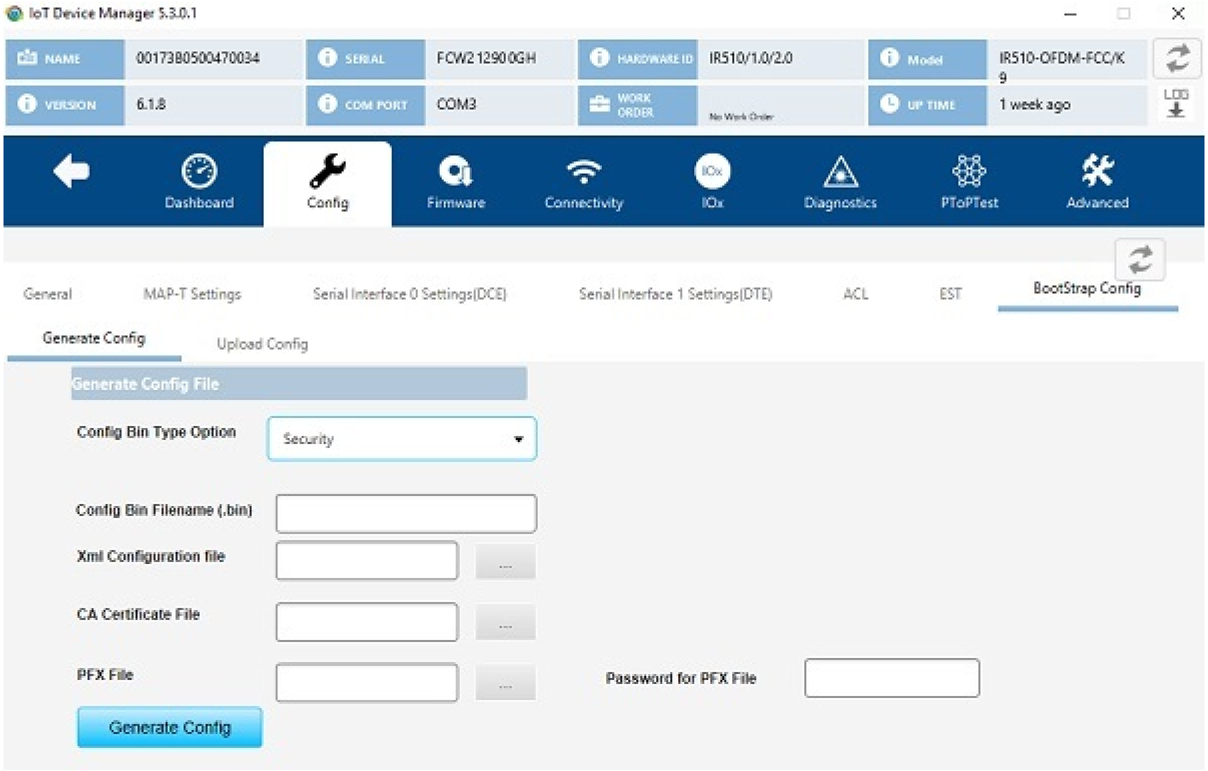
NAME: 00173B0500470034
SERIAL: FCW212900GH
HARDWARE ID: IR510/1.0/2.0
Model: IR510-OFDM-FCC/K9
VERSION: 6.1.8
COM PORT: COM3
WORK ORDER: No Work Order
UP TIME: 1 week ago

Config Bin Type Option: Non Security

Config Bin Filename (.bin):

Xml Configuration file:

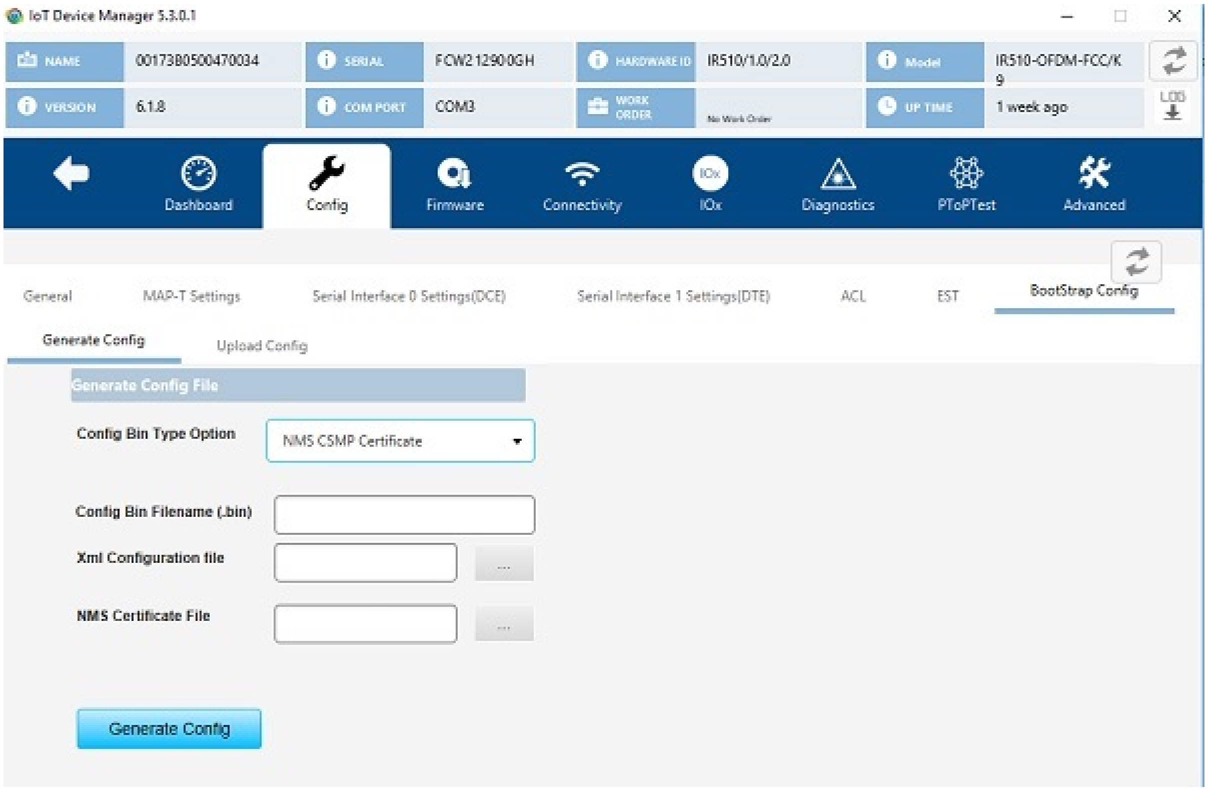
b) To generate security bootstrap configurations, choose **Security** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input, the CA certificate file and PFX file, and enter the password for the PFX file, as shown in the following figure.



NAME: 00173B0500470034
SERIAL: FCW2129000GH
HARDWARE ID: IR510/1.0/2.0
Model: IR510-OFDM-FCC/K9
VERSION: 6.1.8
COM PORT: COM3
WORK ORDER: No Work Order
UP TIME: 1 week ago

Config Bin Type Option: Security

c) To generate bootstrap configuration with NMS CSMP certificate, choose **NMS CSMP Certificate** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input and the NMS certificate file for connecting to FND, as shown in the following figure.



NAME 00173B0500470034

SERIAL FCW21290GH

HARDWARE ID IR510/1.0/2.0

Model IR510-OFDM-FCC/K9

VERSION 6.1.8

COM PORT COM3

WORK ORDER No Work Order

UP TIME 1 week ago

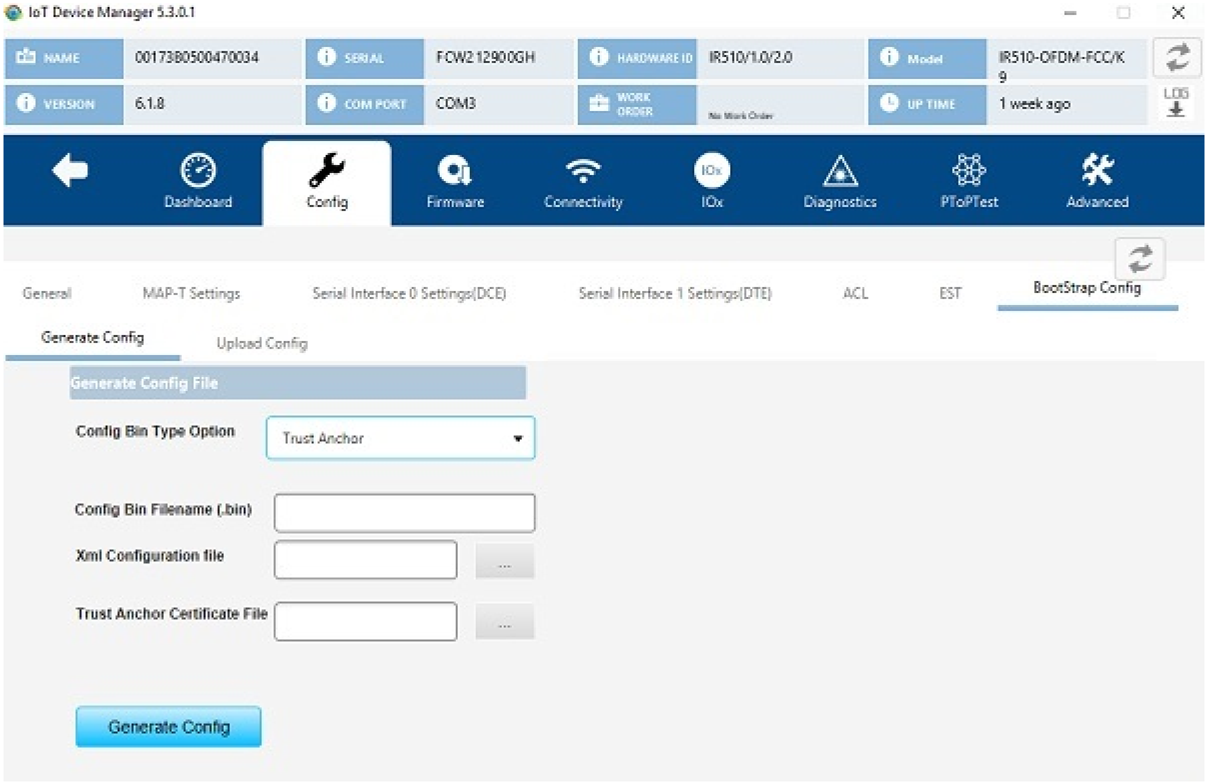
Config Bin Type Option: NMS CSMP Certificate

Config Bin Filename (.bin)

Xml Configuration file

NMS Certificate File

d) To generate bootstrap configuration with trustanchor for EST, choose **Trust Anchor** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input and the Trust Anchor certificate file for EST, as shown in the following figure.



NAME 00173B0500470034
SERIAL FCW212900GH
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 6.1.8
COM PORT COM3
WORK ORDER No Work Order
UP TIME 1 week ago

Generate Config File

Config Bin Type Option: Trust Anchor

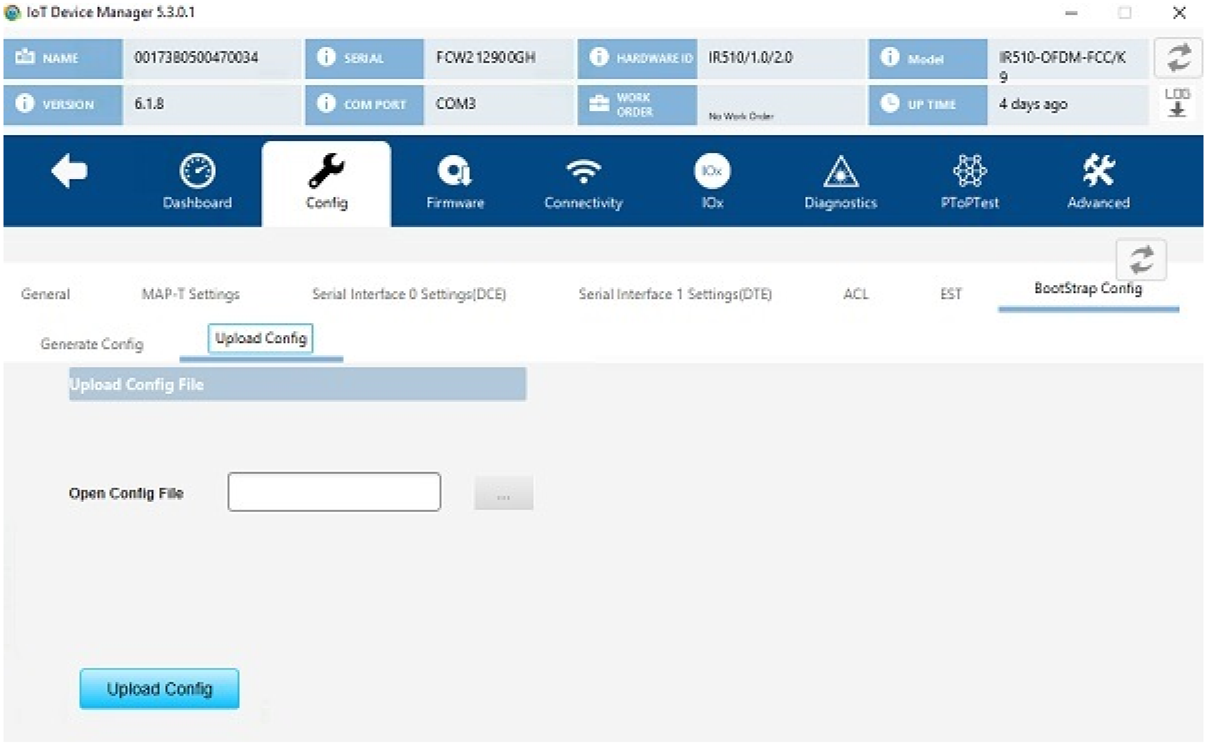
Config Bin Filename (.bin):

Xml Configuration file:

Trust Anchor Certificate File:

Step 3 Click the Generating Config button. The configuration bin file is created and a dialog box appears showing the location of the created configuration bin file. If there are errors while creating the configuration bin file, the error is shown in the dialog box.

Step 4 Click the **Uplooad Config** subtab.



IoT Device Manager 5.3.0.1

NAME 00173805004700034

SERIAL FCW2129000GH

HARDWARE ID IR510/1.0/2.0

Model IR510-OFDM-FCC/K9

VERSION 6.1.8

COM PORT COM3

WORK ORDER No Work Order

UP TIME 4 days ago

Step 5 Browse to choose the location of the config bin file in the **Open Config File** field.

Step 6 Click the Upload Config button. The configuration bin file is executed in the device and a dialog box appears with a success message. If there are any errors while executing the configuration bin file, the error is shown to in the dialog box.

Updating the Firmware Image

Use the Firmware page to perform these tasks: upload an image, install an image, and set the backup.

Uploading an Image

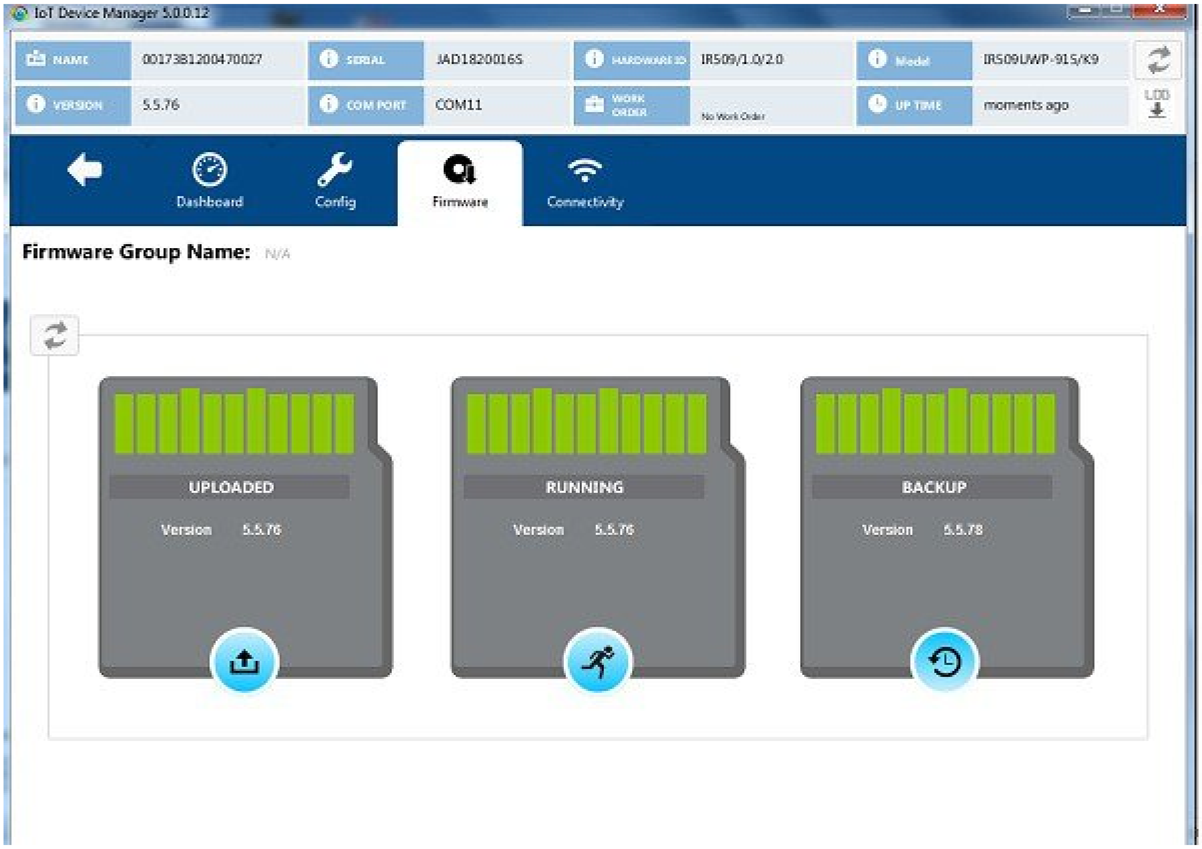
To upload an image to the IR500:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. On the left of the Firmware page, click the Upload icon and select an image to upload. The new image is stored on the IR500 until you are ready to install the image on the IR500. (See Installing an Image, on page 127.)
3. In the dialog box that appears, click **Yes** to upload the selected image.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.



IoT Device Manager 5.0.0.12

NAME 0017381200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

Firmware Group Name: N/A

UPLOADED Version 5.5.76
RUNNING Version 5.5.76
BACKUP Version 5.5.78

Step 2 On the left of the Firmware page, click the Upload icon and select an image to upload. The new image is stored on the IR500 until you are ready to install the image on the IR500. (See Installing an Image, on page 127.)

Step 3 In the dialog box that appears, click **Yes** to upload the selected image.

Installing an Image

To install an uploaded image on the IR500:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. In the middle of the Firmware page, click the Install icon.
3. In the dialog box that appears, click **Yes** to install the image on the IR500.
4. In the dialog box that appears after the installation is completed, click **Save Results** or **OK**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 In the middle of the Firmware page, click the Install icon.

Step 3 In the dialog box that appears, click **Yes** to install the image on the IR500.

If you did not previously upload an image to install, Device Manager displays the Upload to Device dialog box for you to upload an image.

After you confirm the installation, the image installs automatically on the device. No manual reboot is required.

Step 4 In the dialog box that appears after the installation is completed, click **Save Results** or **OK**.

Setting the Backup

To set the running image as the backup image:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. On the right of the Firmware page, click the Set Backup icon.
3. In the dialog box that appears, click **Yes**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 On the right of the Firmware page, click the Set Backup icon.

Step 3 In the dialog box that appears, click **Yes**.

Testing Connectivity

Use the Connectivity page to test connectivity to a target with an IPv6 address. You can test connectivity of the Ethernet or 6LoWPAN interface.

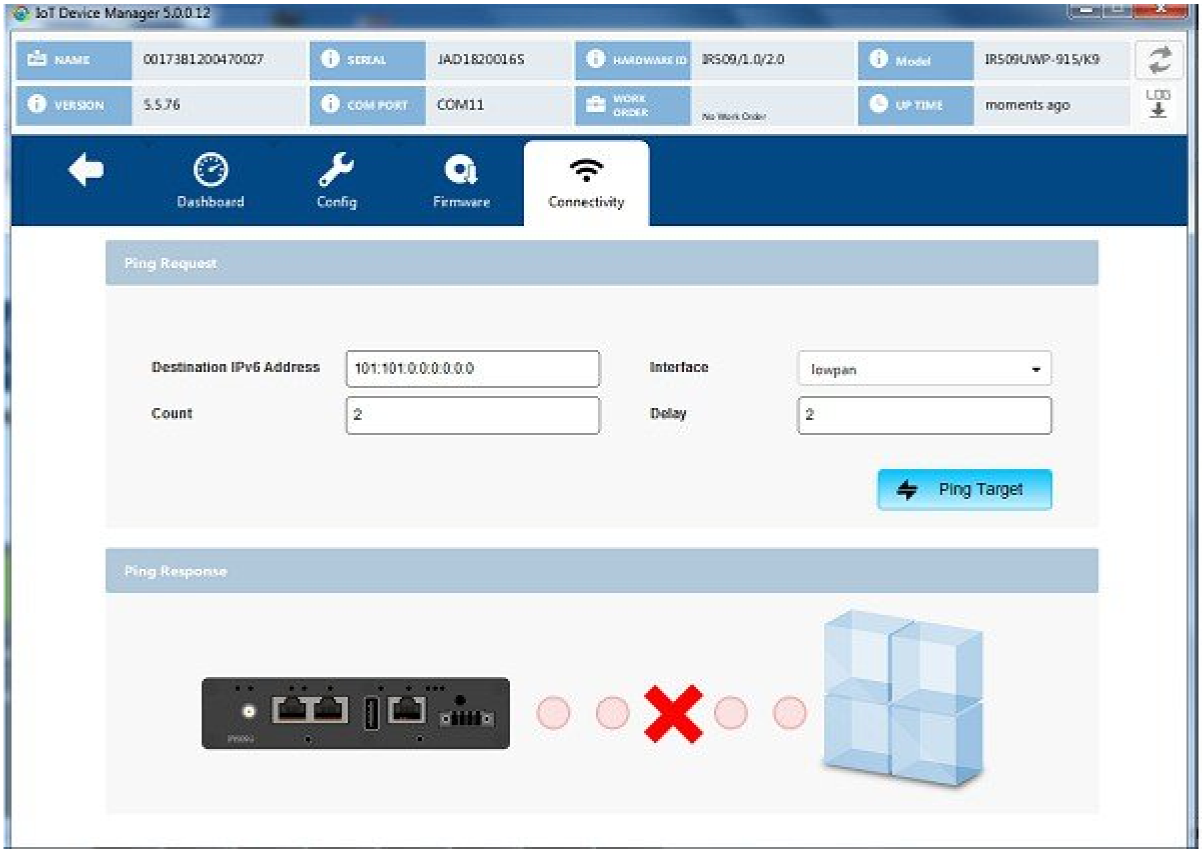
To test connectivity:

SUMMARY STEPS

1. On the Device Manager main page, click the **Connectivity** tab.
2. Configure the Ping Request settings:
3. Click **Ping Target**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Connectivity** tab.



NAME 00173B1200470027

SERIAL JAD18200165

HARDWARE ID IR509/1.0/2.0

Model IR509UWP-915/K9

VERSION 5.5.76

COM PORT COM11

WORK ORDER No Work Order

UP TIME moments ago

Destination IPv6 Address 101:101:0:0:0:0:0:0

Interface lowpan

Count 2

Delay 2

Step 2 Configure the Ping Request settings:

- **Destination IPv6 Address:** IPv6 address of the ping target
- **Interface**:
  - **eth**: Ethernet.
  - **lowpan:** 6LoWPAN.
- **Count**: Number of ping requests to send (0 to 9).
- **Delay**: Number of seconds to wait between sending each request (0 to 9).

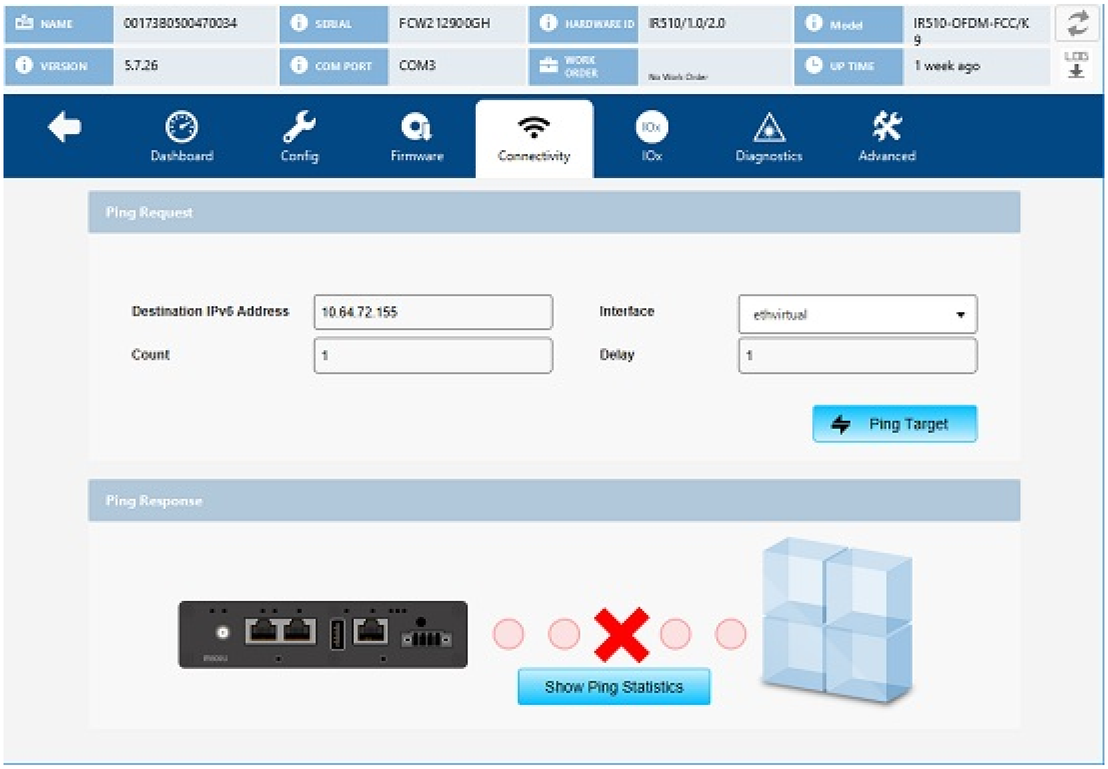
Step 3 Click **Ping Target**.

A dialog box appears indicating that the IR500 is attempting to ping the target IPv6 address. When the IR500 successfully pings the target, the Ping Response area of the Connectivity page displays a green check mark. If the ping is unsuccessful, the response area displays a red X.

To see the contents of the ping response message as a tooltip, hover over the icon for the target device.

Ping Test Enhancement on IR510

Under Connectivity tab, **Show Ping Statistics** is supported for IR510. On clicking this button, a dialog box will be displayed to show the details of the ping operation performed. This function is disabled by default. Once the Ping operation is completed, the **Show Ping Statistics** button will be enabled.



NAME	00173B0500470034	SERIAL	FCW212900GH	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	5.7.26	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	1 week ago

Ping Request

Destination IPv6 Address: 10.64.72.155

Interface: ethvirtual

Count: 1

Delay: 1

Ping Response

Offline Authorization—FTT Secured Wireless Console for IR510

In IoT-Device Manager Release 5.6, an authorization security procedure is introduced between IoT-DM FTT wireless console and target node (IR510) by using wireless console authorize TLV 342. Currently, FTT wireless console session with target nodes from IoT-DM is validating the connection by following an authentication procedure through DTLS certificates. However, DTLS channel is suspectable for various security attacks (man-in-the-middle, Denial of Service attacks, and so on) as well as security vulnerabilities. This feature will ensure the target node to connect and process the request from a legible source. As part of this feature, IoT-DM will receive signed authorization TLV 342 message byte array from FND through work order. IoT-DM will send the authorization message to target after the successful post operation of TLV 341 to the neighboring target node and DTLS secure channel establishment. Based on the authorization response received from target node, IoT-DM will process the same and start the wireless console session with supported authorized TLV's. This way the device node will execute only the communicated authorize TLV commands.

Note

- This feature cannot work when IR510 is connected to COM port or connected without work order option.
- IPV4 connectivity from IoT-DM to relay node is not supported.
- Management command is not supported.

As shown in the following figures, the FND admin creates the work order with authorization message which contains wireless authorize console TLV and FND signature TLV and the same will be assigned to IoT-DM. You need to connect to the device through the respective work order. While starting the wireless console, IoT-DM will transfer the authorization message to the target after establishing the DTLS channel. Target node validates the same and send the response to the IoT-DM and IoT-DM process the response. If it is a successful response, IoT-DM will perform a get TLV 342 operation and based on the get response TLV command execution session start with supported TLV's list received as part of TLV 342 get request.

Figure 9: Authorization TLV Message Procedure

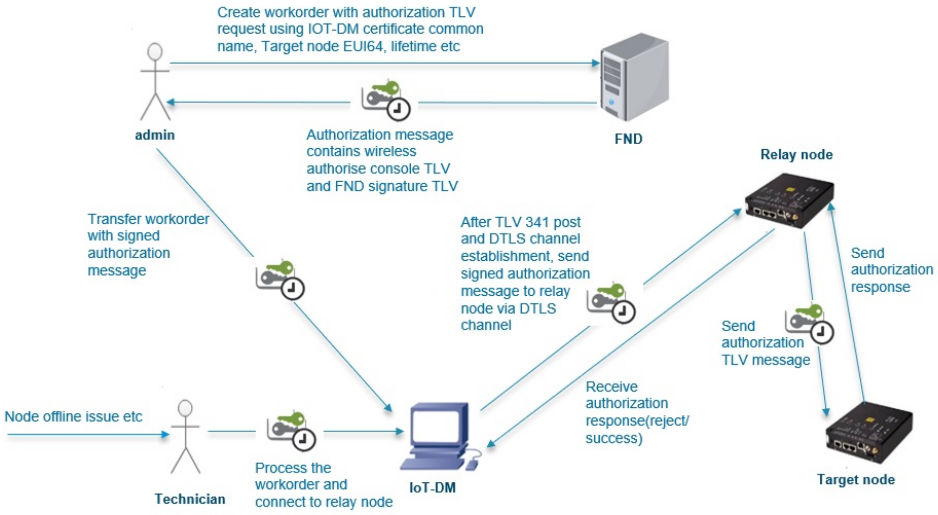
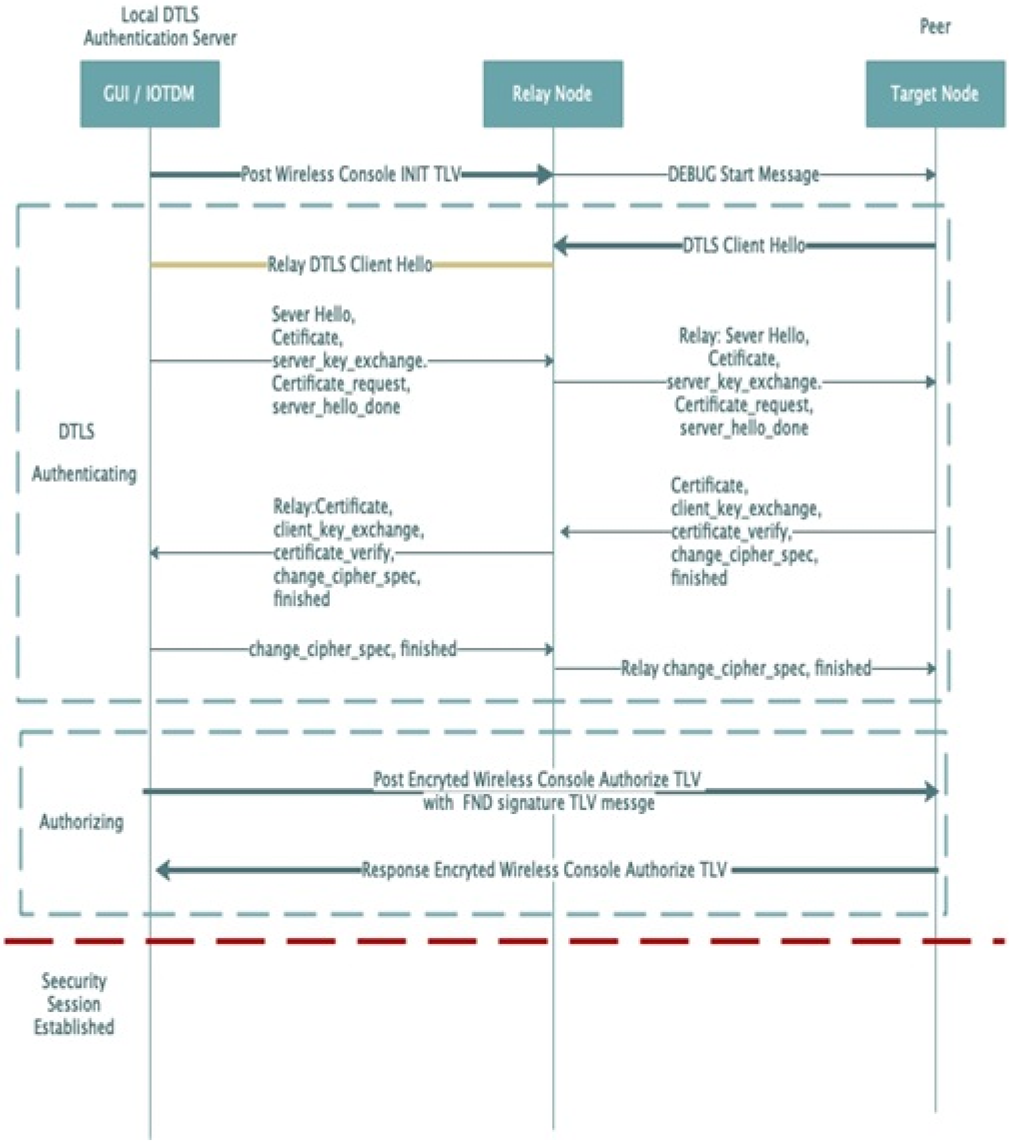

Create workorder with authorization TLV request using IOT-DM certificate common name, Target node EUI64, lifetime etc
admin
Authorization message contains wireless authorise console TLV and FND signature TLV
FND
Relay node
Transfer workorder with signed authorization message
After TLV 341 post and DTLS channel establishment, send signed authorization message to relay node via DTLS channel
Send authorization response
Send authorization TLV message
Receive authorization response(reject/ success)
Node offline issue etc
Technician
Process the workorder and connect to relay node
IoT-DM
Target node

Figure 10: Authorization Message Request Procedure Between IoT-DM and Target Node


Local DTLS Authentication Server
Peer
GUI / IOTDM
Relay Node
Target Node
Post Wireless Console INIT TLV
DEBUG Start Message
DTLS Client Hello
Relay DTLS Client Hello
Sever Hello, Cetificate, server_key_exchange. Certificate_request, server_hello_done
Relay: Sever Hello, Cetificate, server_key_exchange. Certificate_request, server_hello_done
DTLS
Authenticating
Relay:Certificate, client_key_exchange, certificate_verify, change_cipher_spec, finished
Certificate, client_key_exchange, certificate_verify, change_cipher_spec, finished
change_cipher_spec, finished
Relay change_cipher_spec, finished
Post Encryted Wireless Console Authorize TLV with FND signature TLV messge
Authorizing
Response Encryted Wireless Console Authorize TLV
Seecurity Session Established

FND will send a work order with its type, whether it is FTT or Non-FTT work order. After Sync up with FND, IoT-DM will list the work order with the type parameter in the work order table. If you want to enable the FTT feature, you need to choose the respective work order type.

Prerequisites

- SSM[CSMP] service should be up and running in FND. You should be able to download CSMP certificate from UI [Admin -> certificates -> certificate for CSMP].
- Target node EID should be present in the FND endpoint.
- Configure IPv6 address on relay node ethernet interface and then program it with security mode enabled.
- Sample Relay node configuration: **decxu_sec.xml**

Import **FTT.keystore** into IOT-DM which contains the following three certificates with alias of ca_cert, server_cert, server.key:

1. root_ca_ec.crt—Root CA's public key, for verifying the client certificate.

2. server_ec.crt—DTLS server's certificate signed by root CA's private key for TLS handshake. Client will use the root CA's public key to verify it.

3. server_pk8.key—DTLS server's private key, for representing himself in TLS handshake.

- Program the Target node with following certificates, keys and config.xml:

  1. root_ca_ec.der—Root CA's public key. (Same Root CA certificate is used, but it is converted in to der format.)

  2. client_ec.der —Generate CSR in any linux and get it signed by root CA's private key and convert into der format.

  3. client_pk8.der—Generate private key in pkcs8 standard and convert into der format.

  4. nms_ec.der— Export the CSMP certificate (SSM cert) from FND and convert into der format.

  5. decxu_sec.xml—Same as relay node enable security mode and config.xml properties should be the same as relay xml config SSID, phy-mode, TX power ReqSignedPost, and ReqValidCheckPost

  6. Sample Target node configuration: decxu_sec.xml

- From Relay node to target node, RSSI strength should be good. To verify this, you can use TLV - 52 [Neighbor802154G].

  1. -90 <= -60 - Good

  2. -100 <= -90 - Fair

  3. -110 <= -100 - Poor

- FND should be release 4.6.115 and later

- IOT-DM should be Release 5.6.0.25 and later

- Mesh (IR510) should be Release 6.2.19 and later. Target and Relay should have the same firmware.

Note FTT is not supported when IR510 is connected to COM Port. IPV4 connectivity from IoT-DM to relay node is not supported.

Steps to Install Custom Certificates (jboss) in the Browser Client for FND

- Export the custom certificate from CA server in *.pfx format and keep in below directory,

  ```
  cd /opt/cgms/server/cgms/conf/
  ```

- Rename the following files to keep as backup jbossas.keystore, vault.keystore and VAULT.dat

  Delete existing jbossas.keystore, vault.keystore and VAULT.dat

- To view the certificate in pfx format:

  ```
  keytool -list -v -keystore <BGL_CA.pfx> -storetype pkcs12
  ```

  Copy the alias <**lab-win-bhl6pvc7ngu-ca**> to import it into the new jbossas.keystore file.

- Import the certificate into jbossas.keystore with the alias name of jboss:

  ```
  keytool -importkeystore -v -srckeystore <BGL_CA.pfx> -srcstoretype pkcs12 -destkeystore
   /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks -srcalias
  <lab-win-bhl6pvc7ngu-ca> -destalias jboss -destkeypass <your_keystore_password>
  ```

  Enter destination keystore password: <keystore>

  Enter source keystore password: <keystore>

  [Storing /opt/cgms/server/cgms/conf/jbossas.keystore]

- Create a new vault.keystore file:

  ```
  keytool -genseckey -alias vault -storetype jceks -keyalg AES -keysize 128 -storepass
  <your_keystore_password> -keypass <your_keystore_password> -keystore
  /opt/cgms/server/cgms/conf/vault.keystore
  ```

- Update the VAULT.dat file with the new password: [/opt/cgms/server/cgms/conf/VAULT.dat file - Keystore password is stored]

  ```
  /opt/cgms/bin/vault.sh -k /opt/cgms/server/cgms/conf/vault.keystore -p
  <your_keystore_password> -e /opt/cgms/server/cgms/conf -i 50 -s 12345678 -v vault -b
  keystore_pass -a password -x <your_keystore_password>
  ```

  Example:

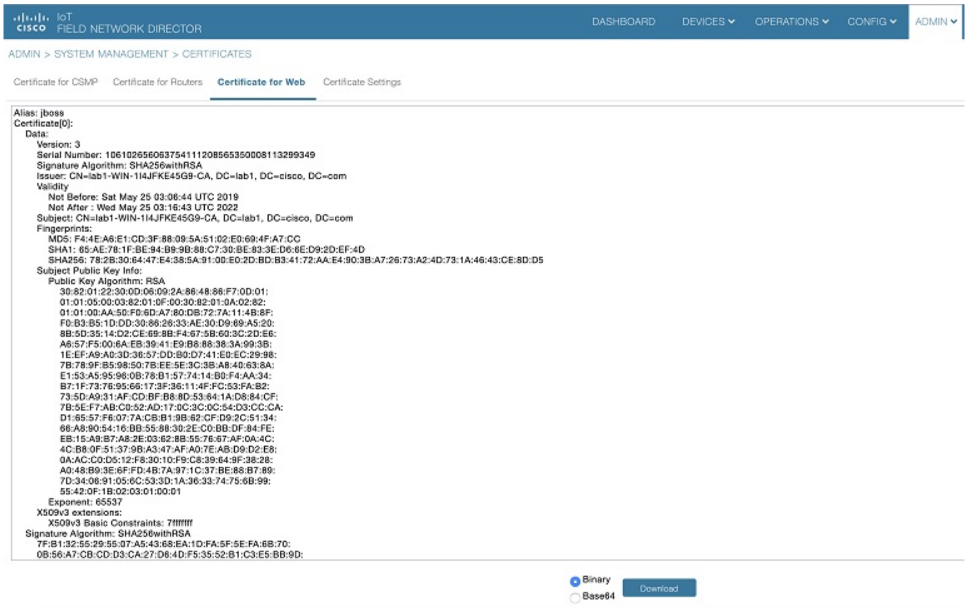
  ```
  Vault Configuration in AS7 config file:
  *******************************************
  </extensions>
  <vault>
  <vault-option name="KEYSTORE_URL" value="/opt/cgms/server/cgms/conf/vault.keystore"/>
  <vault-option name="KEYSTORE_PASSWORD" value="MASK-VKsAwH928fwt.3H2qUwOG"/>
  <vault-option name="KEYSTORE_ALIAS" value="vault"/>
  <vault-option name="SALT" value="12345678"/>
  <vault-option name="ITERATION_COUNT" value="50"/>
  <vault-option name="ENC_FILE_DIR" value="/opt/cgms/server/cgms/conf/"/>
  </vault><management> ...
  ```

- Take backup of following two files: /opt/cgms/standalone/configuration/standalone.xml and standalone-cluster.xml

  Update the generated vault tags in /opt/cgms/standalone/configuration/standalone.xml or standalone-cluster.xml file.

- service cgms restart

- When FND comes up, check for the updated custom certificate either through browser view certificate or through login to FND and choose Admin → Certificate → Certificate For Web.



```
Alias: jboss
Certificate[0]:
  Data:
    Version: 3
    Serial Number: 106102656063754111208565350008113299349
    Signature Algorithm: SHA256withRSA
    Issuer: CN=lab1-WIN-1I4JFKE45G9-CA, DC=lab1, DC=cisco, DC=com
    Validity
      Not Before: Sat May 25 03:06:44 UTC 2019
      Not After : Wed May 25 03:16:43 UTC 2022
    Subject: CN=lab1-WIN-1I4JFKE45G9-CA, DC=lab1, DC=cisco, DC=com
    Fingerprints:
      MD5: F4:4E:A6:E1:CD:3F:88:09:5A:51:02:E0:69:4F:A7:CC
      SHA1: 65:AE:78:1F:BE:94:B9:9B:88:C7:30:BE:83:3E:D6:6E:D9:2D:EF:4D
      SHA256: 78:2B:30:64:47:E4:38:5A:91:00:E0:2D:BD:B3:41:72:AA:E4:90:3B:A7:26:73:A2:4D:73:1A:46:43:CE:8D:D5
    Subject Public Key Info:
      Public Key Algorithm: RSA
        30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:
        01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:
        01:01:00:AA:50:F0:6D:A7:80:DB:72:7A:11:4B:8F:
        F0:B3:B5:1D:DD:30:86:26:33:AE:30:D9:69:A5:20:
        8B:5D:35:14:D2:CE:69:8B:F4:67:5B:60:3C:2D:E6:
        A6:57:F5:00:6A:EB:39:41:E9:B8:88:38:3A:99:3B:
        1E:EF:A9:A0:3D:36:57:DD:B0:D7:41:E0:EC:29:98:
        7B:78:9F:B5:98:50:7B:EE:5E:3C:3B:A8:40:63:8A:
        E1:53:A5:95:96:0B:78:B1:57:74:14:B0:F4:AA:34:
        B7:1F:73:76:95:66:17:3F:36:11:4F:FC:53:FA:B2:
        73:5D:A9:31:AF:CD:BF:B8:8D:53:64:1A:D8:84:CF:
        7B:5E:F7:AB:C0:52:AD:17:0C:3C:0C:54:D3:CC:CA:
        D1:65:57:F6:07:7A:CB:B1:9B:62:CF:D9:2C:51:34:
        66:A8:90:54:16:BB:55:88:30:2E:C0:BB:DF:84:FE:
        EB:15:A9:B7:A8:2E:03:62:8B:55:76:67:AF:0A:4C:
        4C:B8:0F:51:37:9B:A3:47:AF:A0:7E:AB:D9:D2:E8:
        0A:AC:C0:D5:12:F8:30:10:F9:C8:39:64:9F:38:28:
        A0:48:B9:3E:6F:FD:4B:7A:97:1C:37:BE:88:B7:89:
        7D:34:06:91:05:6C:53:3D:1A:36:33:74:75:6B:99:
        55:42:0F:1B:02:03:01:00:01
      Exponent: 65537
    X509v3 extensions:
      X509v3 Basic Constraints: 7fffffff
  Signature Algorithm: SHA256withRSA
    7F:B1:32:55:29:55:07:A5:43:68:EA:1D:FA:5F:5E:FA:6B:70:
    0B:56:A7:CB:CD:D3:CA:27:D6:4D:F5:35:52:B1:C3:E5:BB:9D:
```

SSM Certificate Installation Steps for FND (Import jboss Certificate Into SSM Web Keystore)

```
#################################################
Default SSM Passwords and alias name:-
ssm_csmp_keystore password : ciscossm
csmp alias name : ssm_csmp
key password : ciscossm
ssm_web_keystore password: ssmweb
#################################################
```

- Download and install the ssm rpm in your FND server:

  ```
  rpm -ivh <cgms-ssm-4.6.0-*.x86_64.rpm>
  ```

- Login to FND GUI:

  ```
  Admin -> certificates -> certificate for web
  ```

  Download the Binary version of "Certificate for Web" from the FND GUI. Save the downloaded file in CGMS under the following path /opt/certForWeb.bin.

- Stop the CGMS and SSM service:

  ```
  service ssm stop
  service cgms stop
  ```

- Copy the ssm port and password in cgms.properties:

  ```
  cd /opt/cgms-ssm/bin/
  ./ssm_setup.sh
  Enter your choice : 5.    [Print CG-NMS configuration for SSM]
  Enter current ssm_csmp_keystore password : <ciscossm>
  Enter alias name : <ssm_csmp>
  Enter key password : <ciscossm>
  ```

  Example:

  ```
  security-module=ssm
  ssm-host=<Replace with IPv4 address of SSM server>
  ssm-port=8445
  ```

```
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

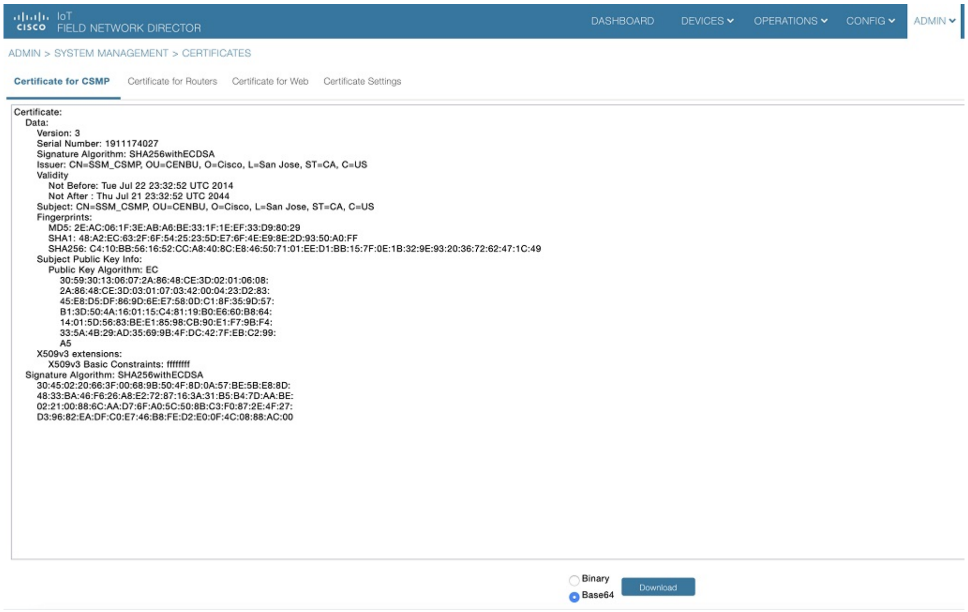
- Update the generated ssm properties in vim /opt/cgms/server/cgms/conf/cgms.properties.
- Add the FND jboss certificate (Certificate for Web) in to ssm_web_keystore.

```
cd /opt/cgms-ssm/bin/
./ssm_setup.sh
Enter your choice : 8
Enter current ssm_web_keystore password : <ssmweb>
Enter the alias for import: fnd
Certificate file name: /opt/certForWeb.bin
Trust this certificate? [no]: yes
Certificate was added to keystore
```

- Start the SSM and CGMS service.

```
service ssm start
service cgms start
```

- Login to FND and choose Admin -> certificates -> Certificate for CSMP. The CSMP certificate will be displayed.



```
Certificate:
   Data:
      Version: 3
      Serial Number: 1911174027
      Signature Algorithm: SHA256withECDSA
      Issuer: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
      Validity
         Not Before: Tue Jul 22 23:32:52 UTC 2014
         Not After : Thu Jul 21 23:32:52 UTC 2044
      Subject: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
      Fingerprints:
         MD5: 2E:AC:06:1F:3E:AB:A6:BE:33:1F:1E:EF:33:D9:80:29
         SHA1: 48:A2:EC:63:2F:6F:54:25:23:5D:E7:6F:4E:E9:8E:2D:93:50:A0:FF
         SHA256: C4:10:BB:56:16:52:CC:A8:40:8C:E8:46:50:71:01:EE:D1:BB:15:7F:0E:1B:32:9E:93:20:36:72:62:47:1C:49
      Subject Public Key Info:
         Public Key Algorithm: EC
            30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:
            2A:86:48:CE:3D:03:01:07:03:42:00:04:23:D2:83:
            45:E8:D5:DF:86:9D:6E:E7:58:0D:C1:8F:35:9D:57:
            B1:3D:50:4A:16:01:15:C4:81:19:B0:E6:60:B8:64:
            14:01:5D:56:83:BE:E1:85:98:CB:90:E1:F7:9B:F4:
            33:5A:4B:29:AD:35:69:9B:4F:DC:42:7F:EB:C2:99:
            A5
      X509v3 extensions:
         X509v3 Basic Constraints: ffffffff
   Signature Algorithm: SHA256withECDSA
      30:45:02:20:66:3F:00:68:9B:50:4F:8D:0A:57:BE:5B:E8:8D:
      48:33:BA:46:F6:26:A8:E2:72:87:16:3A:31:B5:B4:7D:AA:BE:
      02:21:00:88:6C:AA:D7:6F:A0:5C:50:8B:C3:F0:87:2E:4F:27:
      D3:96:82:EA:DF:C0:E7:46:B8:FE:D2:E0:0F:4C:08:88:AC:00
```

SSM debug log: /opt/cgms-ssm/log/ssm.log - SSM logs

Steps to Generate Certificates and Keys for Relay and Target Node

To use FTT wireless console, you need to import CA certificate and IOT-DM certificate into ftt.keystore.

Before you generate certificates and keys for relay and target node, make sure you have the following prerequisites met:

1. Openssl is installed
2. Java JDK is installed for Keytool
3. openssl.cnf

4. fwubl_win732bit_x.x.x.exe
5. cfgwriter-x.x.xx.jar
6. decxu_sec.xml

Follow these steps to generate certificates and keys for relay and target node:

1. On Linux1, generate Root_CA and key with self-signed certificate, using the following commands:

   ```
   mkdir CA
   mkdir CA/{newcerts,certreqs,crl,private}
   touch CA/index.txt
   touch CA/serial
   echo 01 > serial
   cd CA
   ```

   Then copy the openssl.cnf file into the CA directory.

   - Generate root CA ECC private key.

     ```
     openssl ecparam -genkey -name prime256v1 -out root_ca_ec.key
     ```

   - Use root CA private key to generate Self-signed SHA-256 root_ca.crt.

     ```
     openssl req -new -sha256 -x509 -days 1095 -config openssl.cnf -extensions v3_ca -key

     root_ca_ec.key -out root_ca_ec.crt   >>>  DTLS server Root_certificate
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:root_ca_cert
     ```

   - Convert root_ca cert from PEM to DER.

     ```
     openssl x509 -in root_ca_ec.crt -outform der -out root_ca_ec.der >>> Target Node
     Root_certificate
     ```

2. On Linux2, the IoT-DM DTLS server,

   - Generate DTLS server ECC private key.

     ```
     openssl ecparam -genkey -name prime256v1 -out server_ec.key
     ```

   - Generate CSR from DTLS server.

     ```
     openssl req -new -sha256 -key server_ec.key -out server.csr -extensions v3_req -config
      openssl.cnf
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:server_cert
     ```

     Copy the above **server_ec.key** and **server.csr** files to Linux1 CA directory, then execute the following commands from Linux1:

   - Use the Root_CA cert, Root_CA key, and Server CSR to give the signed certificate of root_CA[server.crt].

     ```
     openssl ca -days 365 -cert root_ca_ec.crt -keyfile root_ca_ec.key -md sha256
     -extensions v3_req
     -config openssl.cnf -in server.csr -out server_ec.crt    >>>      DTLS server
     certificate
     ```

   - Convert the DTLS server ECC key to PKCS8 standard.

```
openssl pkcs8 -topk8 -nocrypt -in server_ec.key -outform PEM -out server_pk8.key >>>
 DTLS server Private key
```

3. On Linux3, the target node IR510,

   - Generate ECC private key for the target node.

     ```
     openssl ecparam -genkey -name prime256v1 -out client_ec.key
     ```

   - Generate CSR from the target node.

     ```
     openssl req -new -sha256 -key client_ec.key -out client.csr -extensions v3_req -config
      openssl.cnf
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:client_cert
     ```

     Copy the above **client_ec.key** and **client.csr** files to Linux1 CA directory, then execute the following commands from Linux1:

   - Use the Root_CA cert, Root_CA key and Server CSR to give the signed certificate of root_CA[client.crt].

     ```
     openssl ca -days 365 -cert root_ca_ec.crt -keyfile root_ca_ec.key -md sha256
     -extensions v3_req
     -config openssl.cnf -in client.csr -out client_ec.crt
     ```

   - Convert the target node ECC key to PKCS8 standard.

     ```
     openssl pkcs8 -topk8 -nocrypt -in client_ec.key -outform PEM -out client_pk8.key
     ```

   - Convert the PKCS8 PEM to DER.

     ```
     openssl pkcs8 -topk8 -nocrypt -in client_pk8.key -outform DER
     -out client_pk8.der    >>>  Target Node Private key
     ```

   - Convert client cert from PEM to DER.

     ```
     openssl x509 -in client_ec.crt -outform der -out client_ec.der    >>>   Target Node
      certificate
     ```

4. Download CSMP certificate from FND

   - Login to FND and navigate to Admin -> certificates -> certificate for CSMP. Download the Base64 version of "Certificate for CSMP" from the FND GUI.

   - Convert CSMP cert from PEM to DER.

     ```
     openssl x509 -inform PEM -in certForCsmp.pem -outform DER -out cert_ssm.der  >>>
       Target Node CSMP certificate
     ```

Generate ftt.keystore for IoT-DM

Before you generate ftt.keystore for IoT-DM, copy the following 3 files in a directory:

- root_ca_ec.crt
- server_ec.crt
- server_pk8.key

In that directory where you copied the above files, follow these steps to generate ftt.keystore for IoT-DM:

1. Import server private key into server.crt and generate ftt.keystore:

   ```
   openssl pkcs12 -export -in server_ec.crt -inkey server_pk8.key -out ftt.keystore
   -name server.key
   ```

2. Import server_ec.crt in to ftt.keystore:

   ```
   keytool -import -alias server_cert -keystore ftt.keystore -file server_ec.crt
   ```

3. Import root_ca.crt in to ftt.keystore:

   ```
   keytool -import -alias ca_cert -keystore ftt.keystore -file root_ca_ec.crt
   >>>     ftt.keystore for IOT-DM
   ```

Configuring Target Node with Generated Certificates and Keys

1. Create a folder and keep the following 7 files in Target node windows machine.
   a. root_ca_ec.der
   b. client_pk8.der
   c. client_ec.der
   d. cert_ssm.der
   e. fwubl_win732bit_x.x.x.exe
   f. cfgwriter-x.x.xx.jar
   g. decxu_sec.xml

2. Open cmd prompt and go to the folder where all 7 files were copied:
   - Execute the below command to generate bin file for target IR510

     ```
     java -jar cfgwriter-6.1.24.jar -v --ca root_ca_ec.der -c client_ec.der -k
     client_pk8.der -nc cert_ssm.der -w decxu_sec.xml target_node.bin
     ```

   - Connect to IR510 with below command:

     ```
     fwubl_win732bit_1.0.5.exe com1
     ```

   - Hard reboot the IR510.
   - Push the generated bin into IR510 with following command:

     ```
     fwubl_win732bit_1.0.5.exe -w target_node.bin -a 0x80e0000 com1
     ```

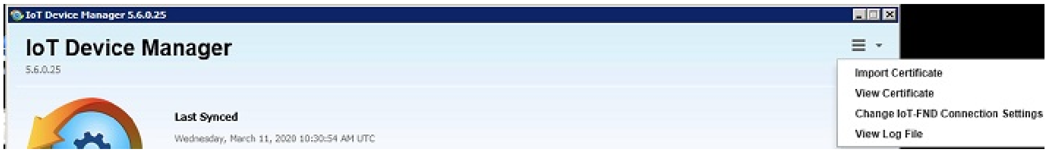
   - Hard reboot the IR510 again.

To verify the applied configuration:

- TLV - 35 WPANStatus
- TLV - 33 Ieee802.1xStatus

Secured Wireless Connection to Target Node

To import the keystore containing these certificates, on the Device Manager opening page, select **Import Certificate** from the drop-down menu on the upper right.



IoT Device Manager 5.6.0.25

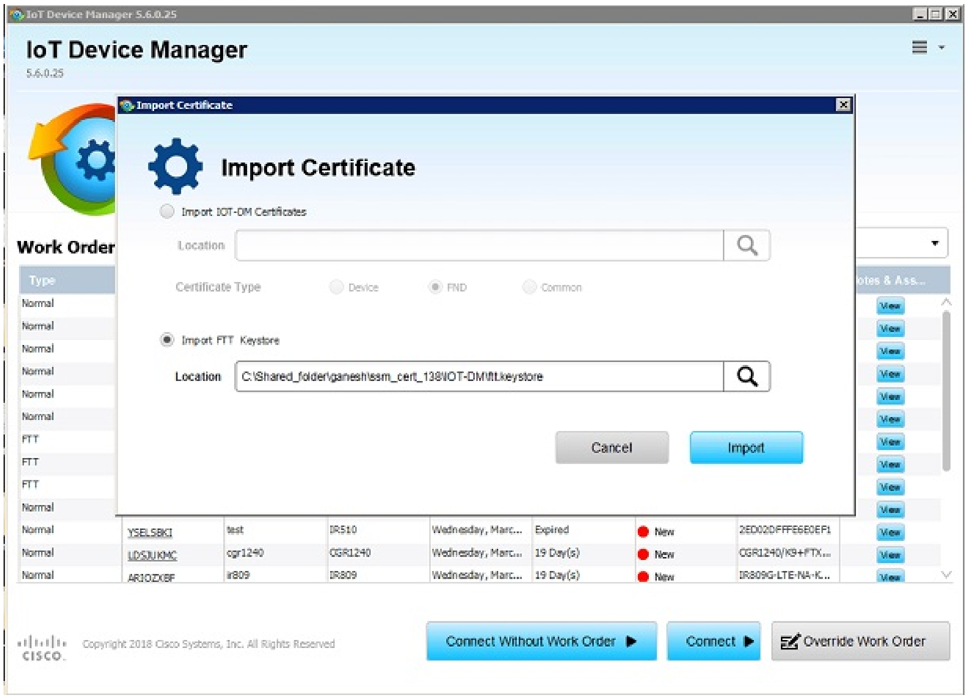
IoT Device Manager
5.6.0.25

Last Synced
Wednesday, March 11, 2020 10:30:54 AM UTC

[redacted]

In the Import Certificate dialog box, browse to the location of the certificate file on your laptop.

Select Import FTT keystore radio button. Then choose the ftt.keystore file and click on Import.



IoT Device Manager 5.6.0.25

IoT Device Manager
5.6.0.25

Import Certificate

Import Certificate

○ Import IOT-DM Certificates

Location

Certificate Type ○ Device ● FND ○ Common

● Import FTT Keystore

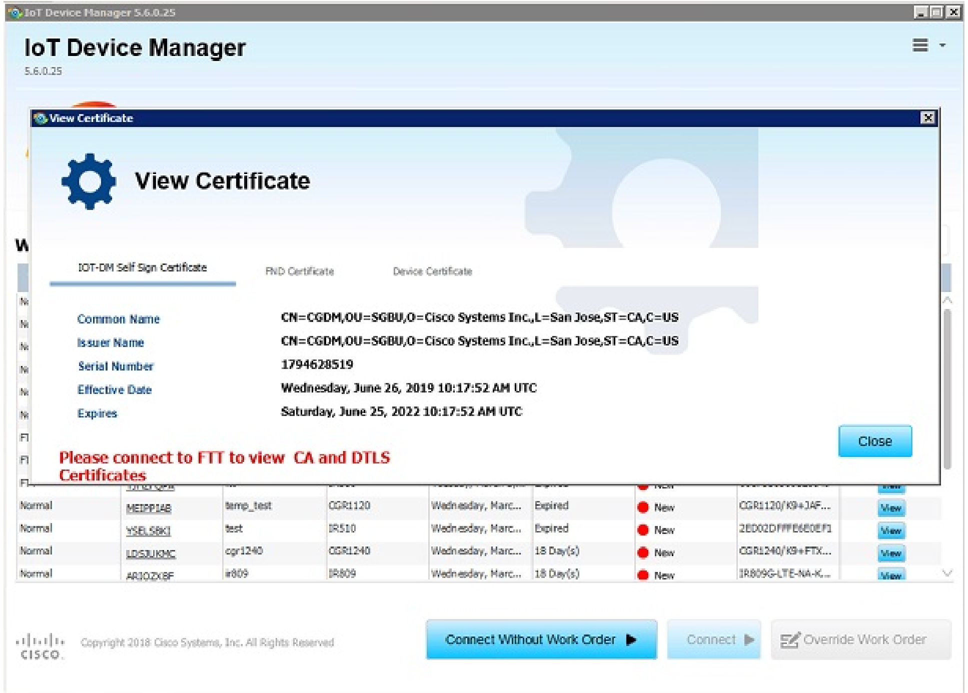
Location C:\Shared_folder\ganesh\ssm_cert_138\IOT-DM\ftt.keystore

Work Order

Type								...otes & Ass...
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
FTT								View
FTT								View
FTT								View
Normal								View
Normal	YSELSBKI	test	IR510	Wednesday, Marc...	Expired	● New	2ED02DFFFE6E0EF1	View
Normal	LDSJUKMC	cgr1240	CGR1240	Wednesday, Marc...	19 Day(s)	● New	CGR1240/K9+FTX...	View
Normal	ARIOZXBF	ir809	IR809	Wednesday, Marc...	19 Day(s)	● New	IR809G-LTE-NA-K...	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Note After importing ftt.keystore, you need to connect to FTT to view the certificates; otherwise you will see the warning message to connect to FTT in the View Certificate page as shown below.



IoT Device Manager 5.6.0.25

View Certificate

IOT-DM Self Sign Certificate | FND Certificate | Device Certificate

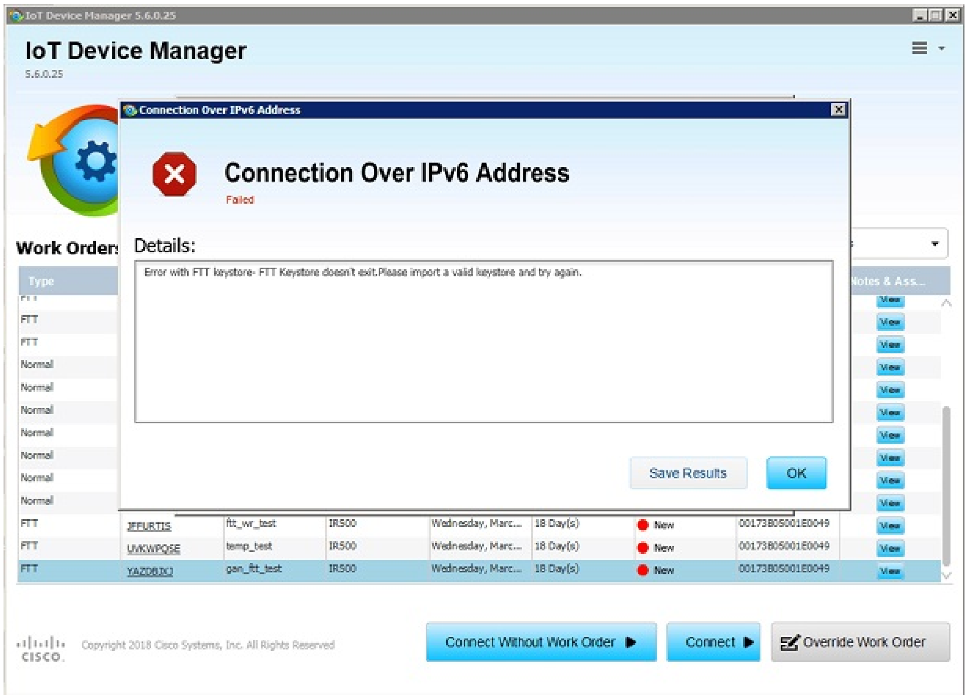
Common Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Issuer Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Serial Number	1794628519
Effective Date	Wednesday, June 26, 2019 10:17:52 AM UTC
Expires	Saturday, June 25, 2022 10:17:52 AM UTC

Please connect to FTT to view CA and DTLS Certificates

Normal	MEIPP1AB	temp_test	CGR1120	Wednesday, Marc...	Expired	● New	CGR1120/K9+JAF...	View
Normal	YSELS8KI	test	IR510	Wednesday, Marc...	Expired	● New	2ED02DFFFE6E0EF1	View
Normal	LDSJUKMC	cgr1240	CGR1240	Wednesday, Marc...	18 Day(s)	● New	CGR1240/K9+FTX...	View
Normal	ARJOZXBF	ir809	IR809	Wednesday, Marc...	18 Day(s)	● New	IR809G-LTE-NA-K...	View

Close
Connect Without Work Order
Connect
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- If ftt.keystore is not imported while connecting to FTT, you will get an error as shown below.



IoT Device Manager 5.6.0.25

Connection Over IPv6 Address

Failed

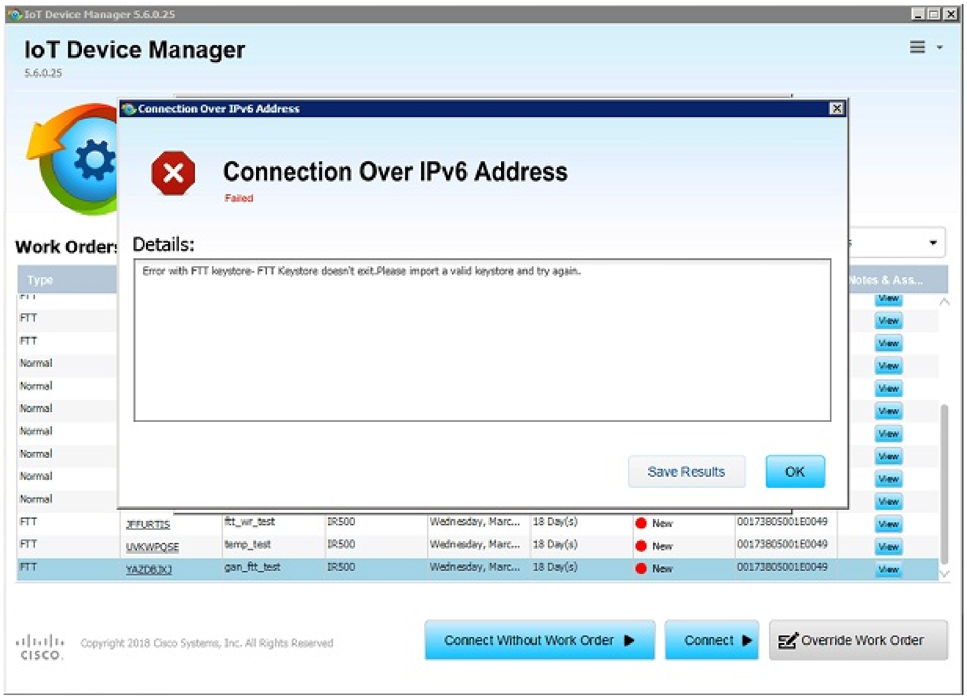
Details:

Error with FTT keystore- FTT Keystore doesn't exit.Please import a valid keystore and try again.

FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View

Work Orders
Type
Notes & Ass...
Save Results
OK
Connect Without Work Order
Connect
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- If a wrong password is provided while connecting to FTT, you will get an error as shown below.


IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
Work Orders
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
CISCO
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Connection Over IPv6 Address

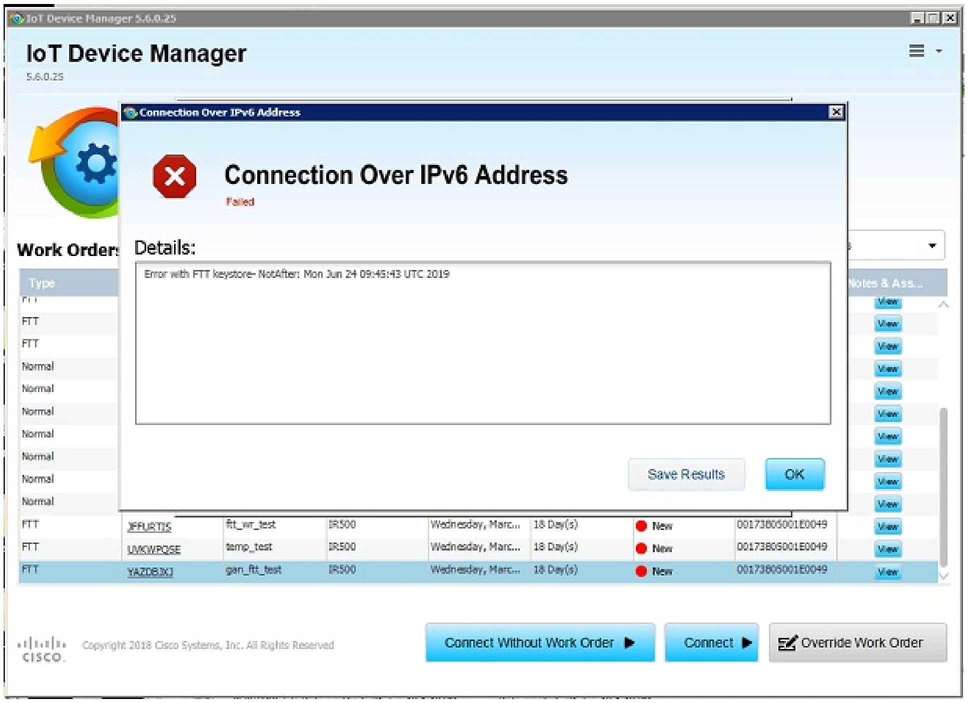
Connection Over IPv6 Address
Failed

Details:

```
Error with FTT keystore- FTT Keystore doesn't exit.Please import a valid keystore and try again.
```

Type								Notes & Ass...
FTT								View
FTT								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View

- If the certificate is expired while connecting to FTT, you will get an error as shown below.


IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
Work Orders
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
CISCO
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Connection Over IPv6 Address

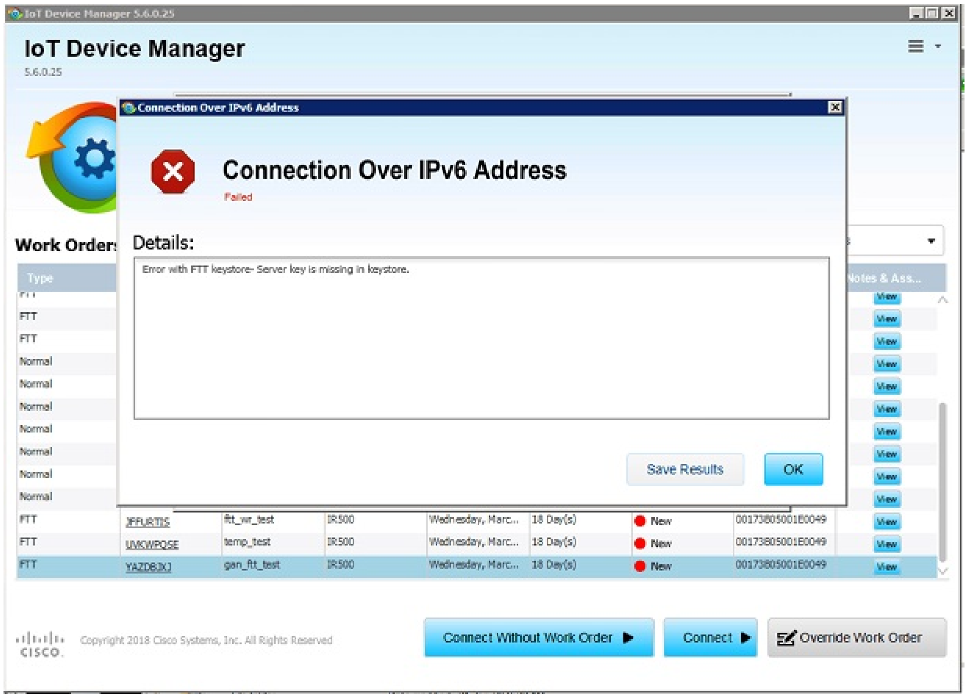
Connection Over IPv6 Address
Failed

Details:

```
Error with FTT keystore- NotAfter: Mon Jun 24 09:45:43 UTC 2019
```

Type								Notes & Ass...
FTT								View
FTT								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View

- If the server key alias is missing while connecting to FTT, you will get an error as shown below.



IoT Device Manager

5.6.0.25

Connection Over IPv6 Address

Failed

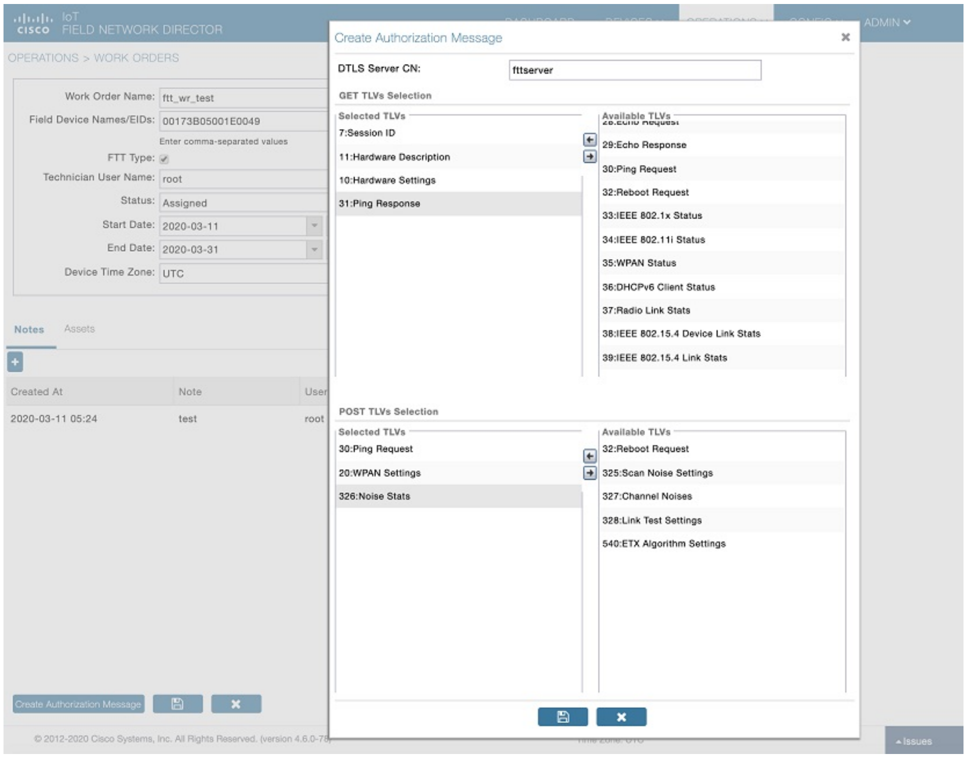
Details:

```
Error with FTT keystore- Server key is missing in keystore.
```

IoT Device Manager 5.6.0.25
Work Orders
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Type									Notes & Ass...
FTT									View
FTT									View
Normal									View
Normal									View
Normal									View
Normal									View
Normal									View
Normal									View
Normal									View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049		View
FTT	UKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049		View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049		View

Create a work order from FND. Enter DTLS server Common Name, give permissions to GET and POST TLVs.



IoT FIELD NETWORK DIRECTOR
ADMIN
OPERATIONS > WORK ORDERS
Notes
Assets
Create Authorization Message
Issues
© 2012-2020 Cisco Systems, Inc. All Rights Reserved. (version 4.6.0-78)

Work Order Name:	ftt_wr_test
Field Device Names/EIDs:	00173B05001E0049
	Enter comma-separated values
FTT Type:	☑
Technician User Name:	root
Status:	Assigned
Start Date:	2020-03-11
End Date:	2020-03-31
Device Time Zone:	UTC

Created At	Note	User
2020-03-11 05:24	test	root

Create Authorization Message

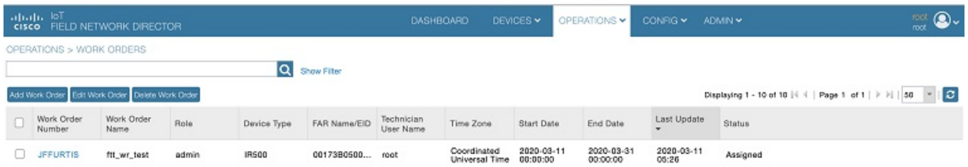
DTLS Server CN: fttserver

GET TLVs Selection

Selected TLVs	Available TLVs
7:Session ID	28:Echo Request
11:Hardware Description	29:Echo Response
10:Hardware Settings	30:Ping Request
31:Ping Response	32:Reboot Request
	33:IEEE 802.1x Status
	34:IEEE 802.11i Status
	35:WPAN Status
	36:DHCPv6 Client Status
	37:Radio Link Stats
	38:IEEE 802.15.4 Device Link Stats
	39:IEEE 802.15.4 Link Stats

POST TLVs Selection

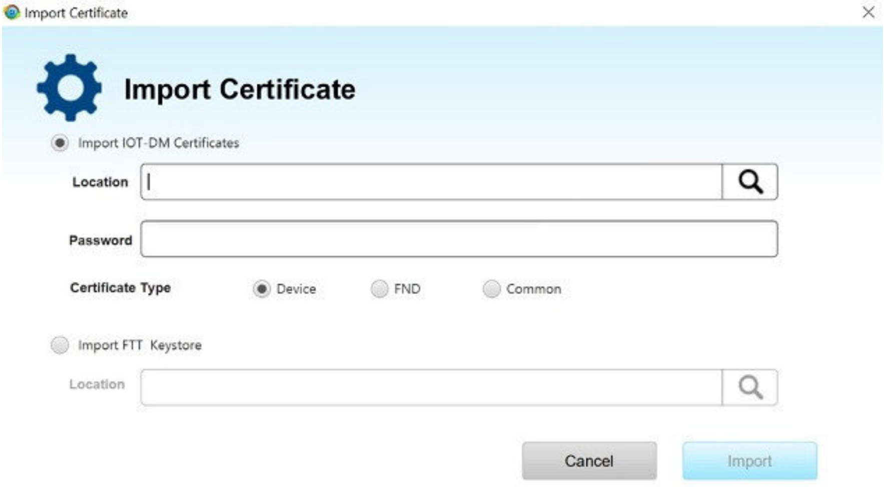
Selected TLVs	Available TLVs
30:Ping Request	32:Reboot Request
20:WPAN Settings	325:Scan Noise Settings
326:Noise Stats	327:Channel Noises
	328:Link Test Settings
	540:ETX Algorithm Settings



□	Work Order Number	Work Order Name	Role	Device Type	FAR Name/EID	Technician User Name	Time Zone	Start Date	End Date	Last Update	Status
□	JFFURTIS	ftt_wr_test	admin	IR500	00173B0500...	root	Coordinated Universal Time	2020-03-11 00:00:00	2020-03-31 00:00:00	2020-03-11 05:26	Assigned

Use one of the following ways to sync the created WR from FND to IOT-DM:

1. Import the FND custom web certificate in to IOT-DM: IOT-DM Application → Settings → Import Certificate → Select Import IOT-DM certificates → Select FND radio button → choose the *.pfx file → enter password and click on Import.



● Import IOT-DM Certificates

Location

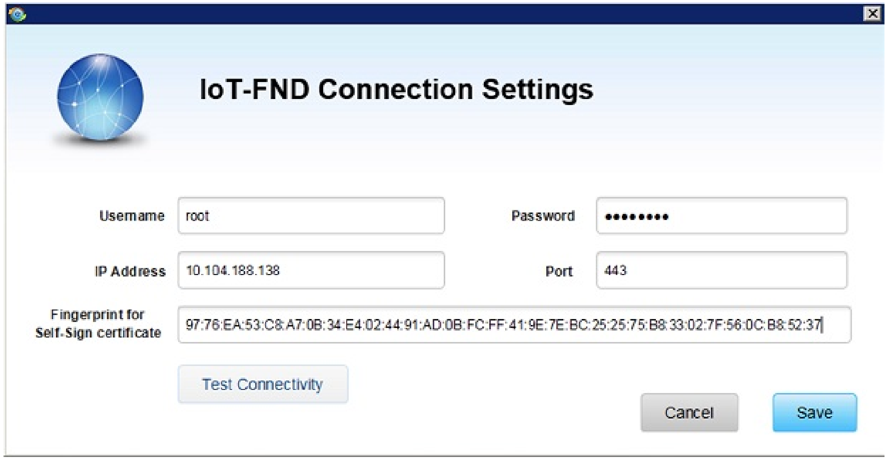
Password

Certificate Type ● Device ○ FND ○ Common

○ Import FTT Keystore

Location

2. Enter the fingerprint of web certificate in IOT-FND Connection Settings.



Username: root

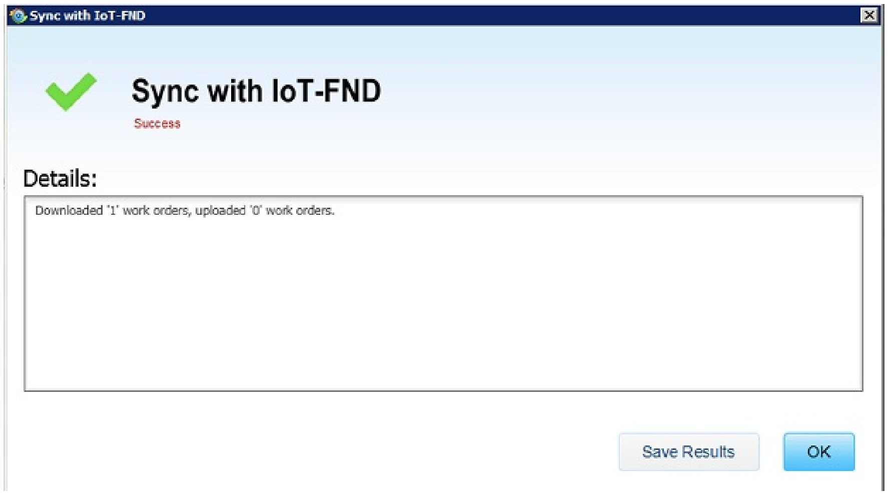
Password: ••••••••

IP Address: 10.104.188.138

Port: 443

Fingerprint for Self-Sign certificate: 97:76:EA:53:C8:A7:0B:34:E4:02:44:91:AD:0B:FC:FF:41:9E:7E:BC:25:25:75:B8:33:02:7F:56:0C:B8:52:37

Click on Sync with IOT-FND.



Sync with IoT-FND

Sync with IoT-FND

Success

Details:

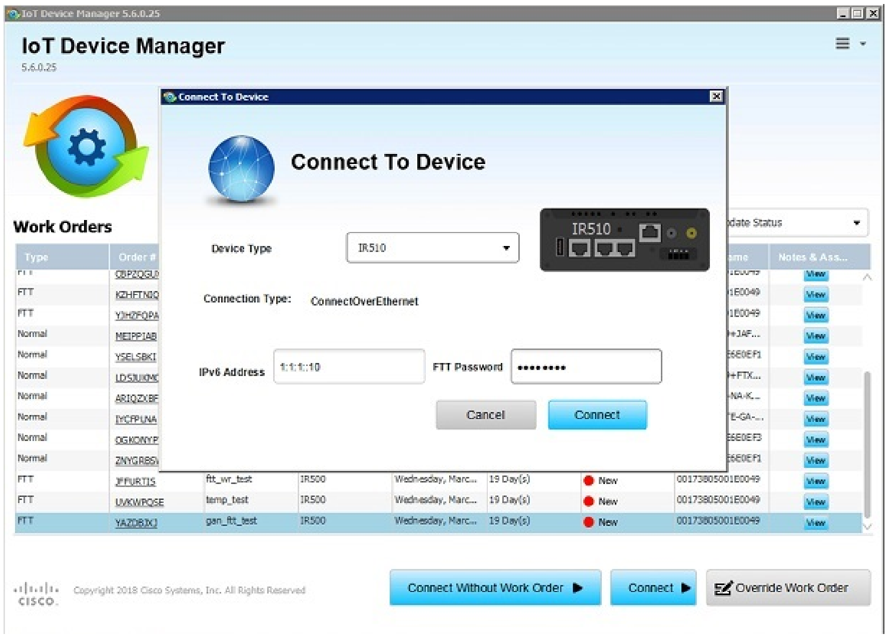
Downloaded '1' work orders, uploaded '0' work orders.

Viewing the Imported FTT keystore in IOT-DM

Select the downloaded FTT type work order and click the Connect button. Select IR510 as device type, enter Relay node IPv6 address, and provide FTT password, then click on connect. Once the dashboard page is launched, disconnect from device.

Note The feature will only be enabled when you connect to the device with work order which has TLV 342 message. If the work order is non FTT type, the IR510 device connected com port. If the work order type is FTT, the Connect button redirects to another screen and you need to provide IPV6 address of the relay node and FTT password. Connect to IR510 via IPV6. Once the connection to IR510 is established through IPV6 Address, the DTLS server 1.2 will be started. IoT-DM uses port number 5556 for DTLS server.

- Connectivity to Relay Node With Work Order



IoT Device Manager 5.6.0.25

IoT Device Manager
5.6.0.25

Connect To Device

Connect To Device

Device Type: IR510

Connection Type: ConnectOverEthernet

IPv6 Address: 1:1:1::10

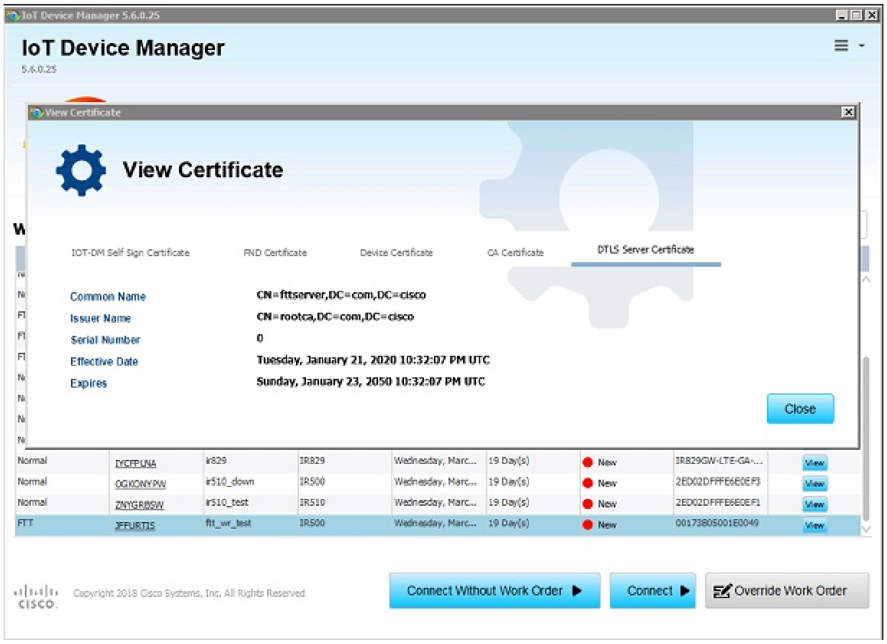
FTT Password: ••••••••

Work Orders

Type	Order #						...me	Notes & Ass...
FTT	CBPZQGU						...1E0049	View
FTT	KZHFTNIQ						...1E0049	View
FTT	YJHZFQPA						...1E0049	View
Normal	MEIPP1AB						...+JAF...	View
Normal	YSELSBKI						...E6E0EF1	View
Normal	LDSJUKMC						...+FTX...	View
Normal	ARIQZXBF						...-NA-K...	View
Normal	IYCFPLNA						...E-GA-...	View
Normal	OGKONYP						...E6E0EF3	View
Normal	ZNYGRBS						...E6E0EF1	View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View
FTT	YAZDBXJ	gan_ftt_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- Once the ftt.keystore is imported, they can be viewed in the View Certificate tab as shown below,



IoT Device Manager 5.6.0.25

IoT Device Manager
5.6.0.25

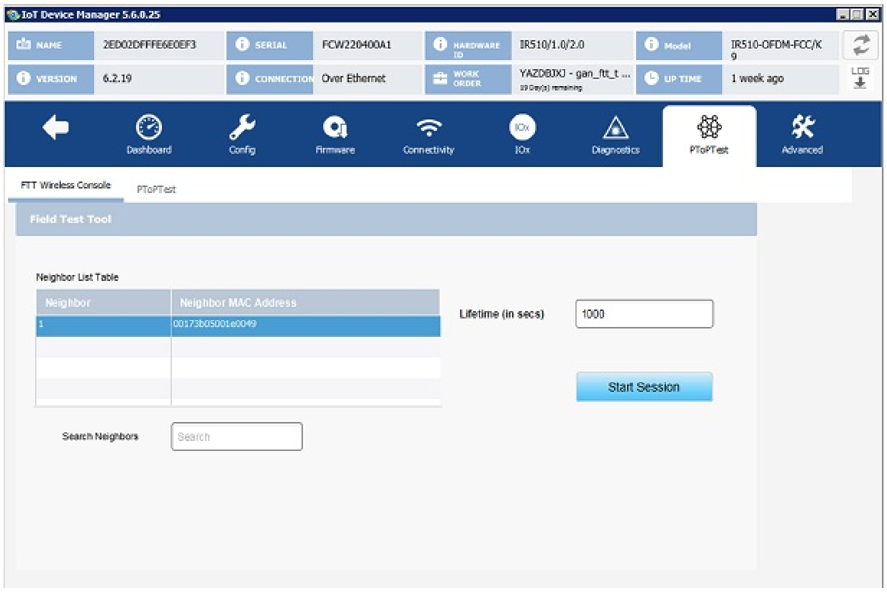
View Certificate

Common Name	CN=fttserver,DC=com,DC=cisco
Issuer Name	CN=rootca,DC=com,DC=cisco
Serial Number	0
Effective Date	Tuesday, January 21, 2020 10:32:07 PM UTC
Expires	Sunday, January 23, 2050 10:32:07 PM UTC

Normal	IYCFPLNA	ir829	IR829	Wednesday, Marc...	19 Day(s)	● New	IR829GW-LTE-GA-...	View
Normal	OGKONYPW	ir510_down	IR500	Wednesday, Marc...	19 Day(s)	● New	2ED02DFFFE6E0EF3	View
Normal	ZNYGR8SW	ir510_test	IR510	Wednesday, Marc...	19 Day(s)	● New	2ED02DFFFE6E0EF1	View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173B05001E0049	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- Login again with the same work order and navigate to PToPTest tab. You need to choose neighbour target node from "Neighbour List table" (populated based on TLV 52), enter the lifetime (in seconds) and click on Start Session. It will post TLV 341 and connect to the respective target node and establish DTLS channel. IoT-DM will send authorization message to the connected target node. If the target node address is not matching with the target node EUI ID mentioned in the authorization message, target node will reject the request. Otherwise, it will establish the connection.



IoT Device Manager 5.6.0.25

NAME	2ED02DFFFE6E0EF3	SERIAL	FCW220400A1	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.2.19	CONNECTION	Over Ethernet	WORK ORDER	YAZDBJXJ - gan_ftt_t ... 19 Day(s) remaining	UP TIME	1 week ago

Field Test Tool

Neighbor List Table

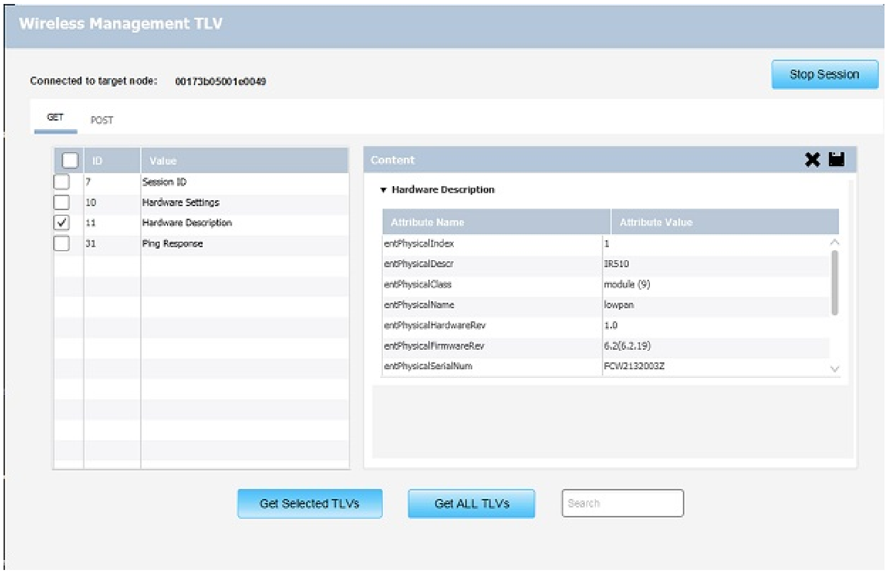
Neighbor	Neighbor MAC Address
1	00173b05001e0049

Lifetime (in secs) 1000

Search Neighbors Search

Wireless Console Screen

- GET Authorized TLV Tab



Wireless Management TLV

Connected to target node: 00173b05001e0049

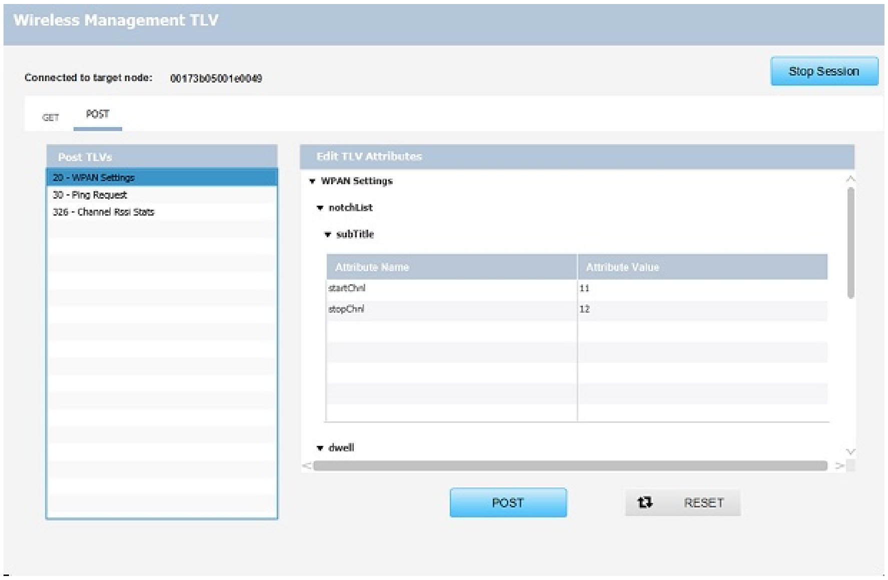
☐	ID	Value
☐	7	Session ID
☐	10	Hardware Settings
☑	11	Hardware Description
☐	31	Ping Response

Content

▾ Hardware Description

Attribute Name	Attribute Value
entPhysicalIndex	1
entPhysicalDescr	IR510
entPhysicalClass	module (9)
entPhysicalName	lowpan
entPhysicalHardwareRev	1.0
entPhysicalFirmwareRev	6.2(6.2.19)
entPhysicalSerialNum	FCW2132003Z

- POST Authorized TLV Tab



Wireless Management TLV

Connected to target node: 00173b05001e0049

Post TLVs

- 20 - WPAN Settings
- 30 - Ping Request
- 326 - Channel Rssi Stats

Edit TLV Attributes

▾ WPAN Settings

▾ notchList

▾ subTitle

Attribute Name	Attribute Value
startChnl	11
stopChnl	12

▾ dwell

- To terminate the session, click the Stop Session button.

Note As part of this feature, management command support via FTT wireless console is removed, hence the "wireless management console screen" supported by starting the wireless console session will be removed from IOT-DM Release 5.6 and later.

Running Point to Point Test Between Two IR510s

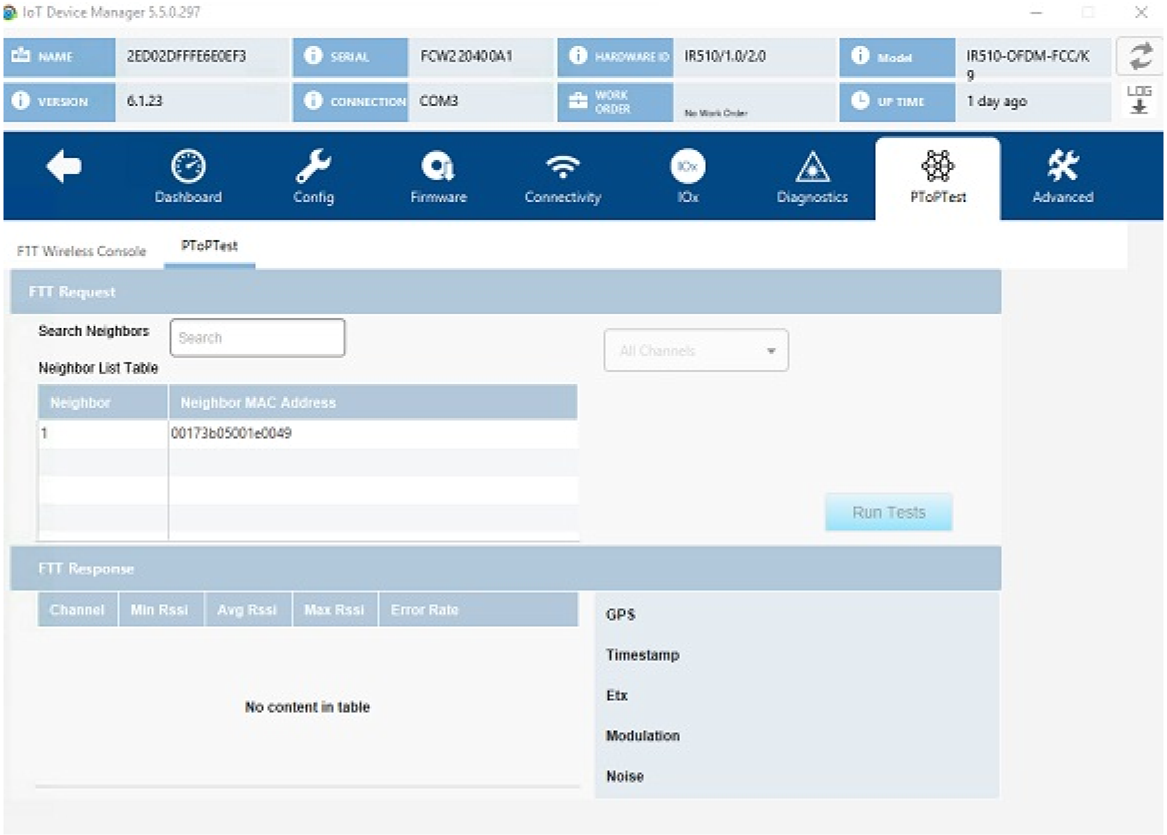
Use the **PToPTest** page to run point to point test between two IR510s.

Step 1 Connect to IR 510 via IOT-DM.

Step 2 Click the **PToPTest** tab, select a neighbour, choose a channel option, and click the **Run Tests** button. If you do not choose a channel option, the test will be running with the default of "All Channels."

Use the Select channel drop-down menu to select one of the following channel options.

- All Channels: the default selection
- Single Channel: choose from 0 to 32
- Channel Range: choose the start channel and the end channel
- Multi Channels: enter channel numbers seperated by commas (for example, "1,5,23,") in the text box



NAME	2ED02DFFFE6E0EF3	SERIAL	FCW2 20400A1	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.1.23	CONNECTION	COM3	WORK ORDER	No Work Order	UP TIME	1 day ago

Search Neighbors

Neighbor List Table

Neighbor	Neighbor MAC Address
1	00173b05001e0049

Channel	Min Rssi	Avg Rssi	Max Rssi	Error Rate

No content in table

GPS

Timestamp

Etx

Modulation

Noise

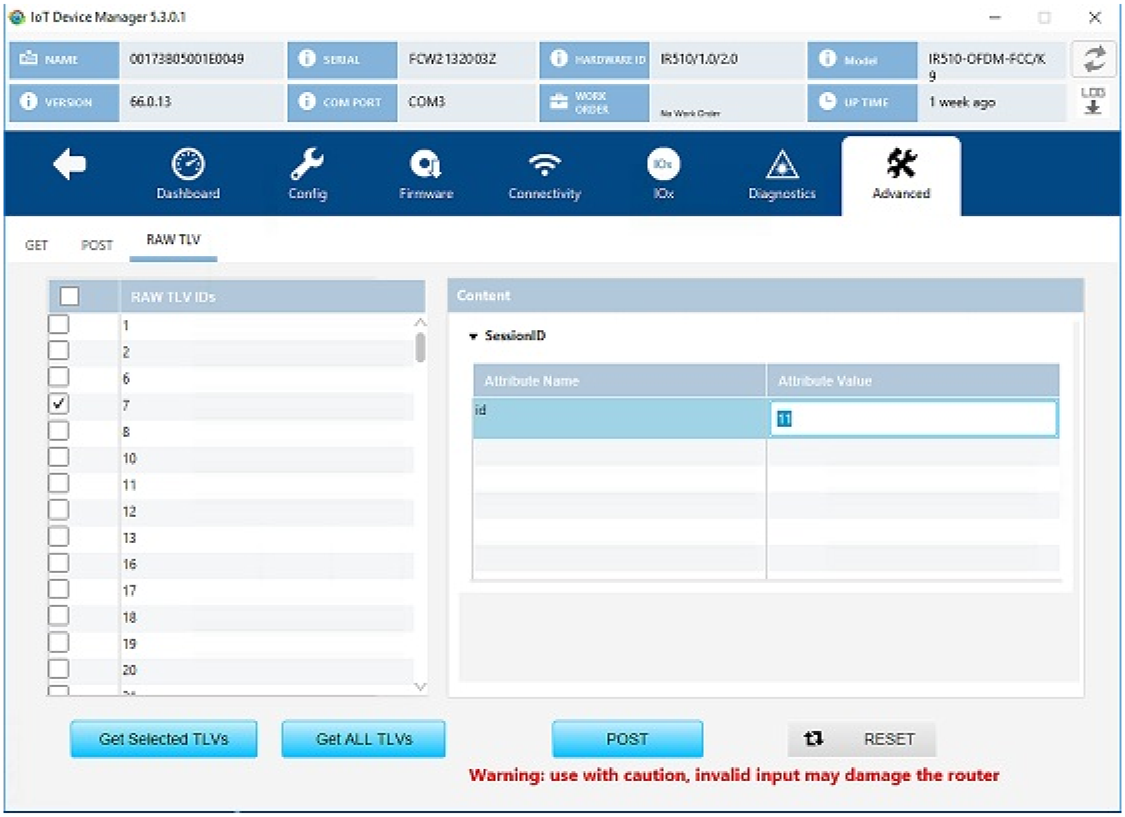
Step 3 (Optional) If you want to search a specific neighbor, enter the physical address in the **Search Neighbours** text box.

The function of searching a specific neighbor is only supported on firmware version CG-Mesh 6.0 and later.

Step 4 After the test is completed, the results are dispalyed for RSSI, Error Rate, ETX, Noise, Modulation, GPS, and Timestamp.

Raw TLV Support on IR510

The RAW TLV tab was introduced for IR510 on the Advanced tab. When you click the **RAW TLV** tab, all TLVs (including newly added TLVs) will be displayed as a list. Select TLVs from the list and click the **Get Selected TLVs** button will display the information about the selected TLVs. Click the **Get ALL TLVs** button will display information of all TLVs in the list. To change the TLV attribute values, click the **POST** button.



NAME	00173805001E0049	SERIAL	FCW2132003Z	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.6.0.13	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	1 week ago

☐	RAW TLV IDs
☐	1
☐	2
☐	6
☑	7
☐	8
☐	10
☐	11
☐	12
☐	13
☐	16
☐	17
☐	18
☐	19
☐	20

Content

▾ SessionID

Attribute Name	Attribute Value
id	11

Warning: use with caution, invalid input may damage the router

Note If you change the field value and click the POST button, the data will be posted to the IR510 device WITHOUT ANY VALIDATION.

Note On the **RAW TLV** tab, every fields of a TLV will be displayed. If some fields are not postable, the post operation will fail.

Disconnecting from the IR500

After finishing your work on the IR500, click the left arrow on the left side of the menu tabs area on the main page to disconnect Device Manager from the IR500. Click **Yes** to confirm that you want to disconnect from the device. Device Manager disconnects and displays the Device Manager opening page.

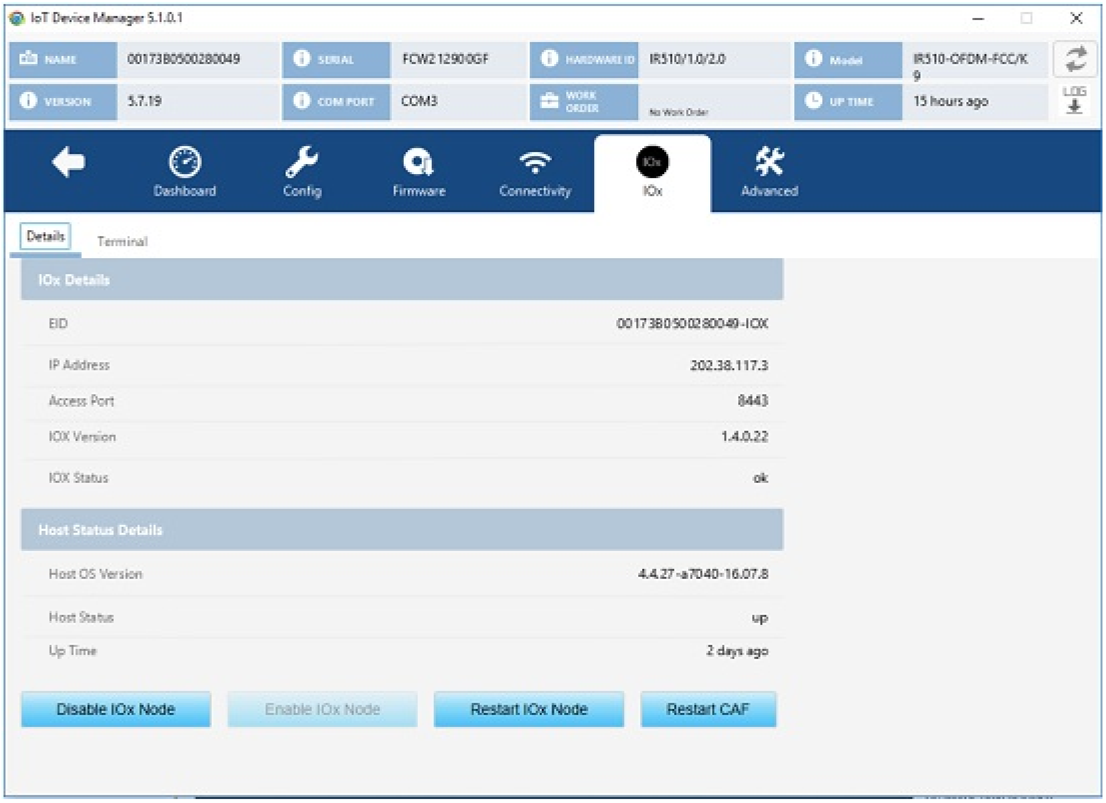
Managing IOx Nodes on IR510

From IoT Device Manager Release 5.2, you can perform management operations on the Linux/IOx nodes on the IR510 device. You can also view the current information of the IOx nodes.

Note The IOx node on IR510 should already have been setup via FND or manually, so that you can perform the management operations on it from IOT-DM.

The following image shows the IOx tab which contains 4 management operation buttons and and a text area showing the details of IOx node in the device.

Figure 11: IOx Tab



NAME 00173B0500280049
SERIAL FCW212900GF
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 5.7.19
COM PORT COM3
WORK ORDER No Work Order
UP TIME 15 hours ago

IOx Details

EID	00173B0500280049-IOX
IP Address	202.38.117.3
Access Port	8443
IOX Version	1.4.0.22
IOX Status	ok

Host Status Details

Host OS Version	4.4.27-a7040-16.07.8
Host Status	up
Up Time	2 days ago

You can perform the following actions

- Enable IOx Node - This operation only takes effect if the IOx Node was in disabled state.

- Disable IOx Node - This operation only takes effect if the IOx Node was in enabled state.
- Restart IOx - This operation only takes effect if the IOx Node was in enabled state.
- Restart CAF - This operation only takes effect if the IOx Node was in enabled state.

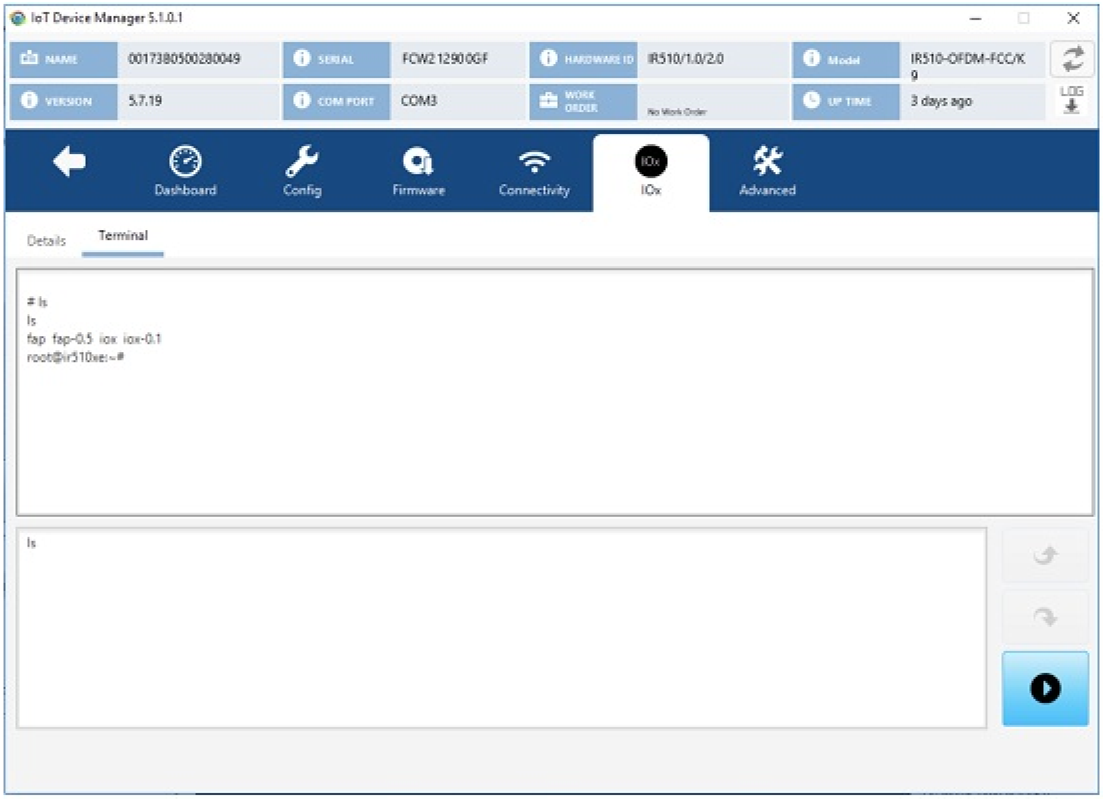
Using the IOx Terminal

You can connect to the Linux/IOx nodes on the IR510 device and execute commands or troubleshoot issues locally by using the IOx terminal on the IOx tab.

Note Linux node on the IR500 device should have UDP server running on 8335 port which will be used to connect via IOT-DM Client over PPP.

To access the IOx Terminal, click the IOx tab and choose Terminal as the following figure shows. An interactive command prompt will display where you can execute the commands on Linux/IOx terminal.

Figure 12: IOx Terminal



NAME	00173805002800049	SERIAL	FCW2 12900GF	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K 9
VERSION	5.7.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	3 days ago

Details Terminal

```
# ls
ls
fap  fap-0.5  iox  iox-0.1
root@ir510xe:~#
```

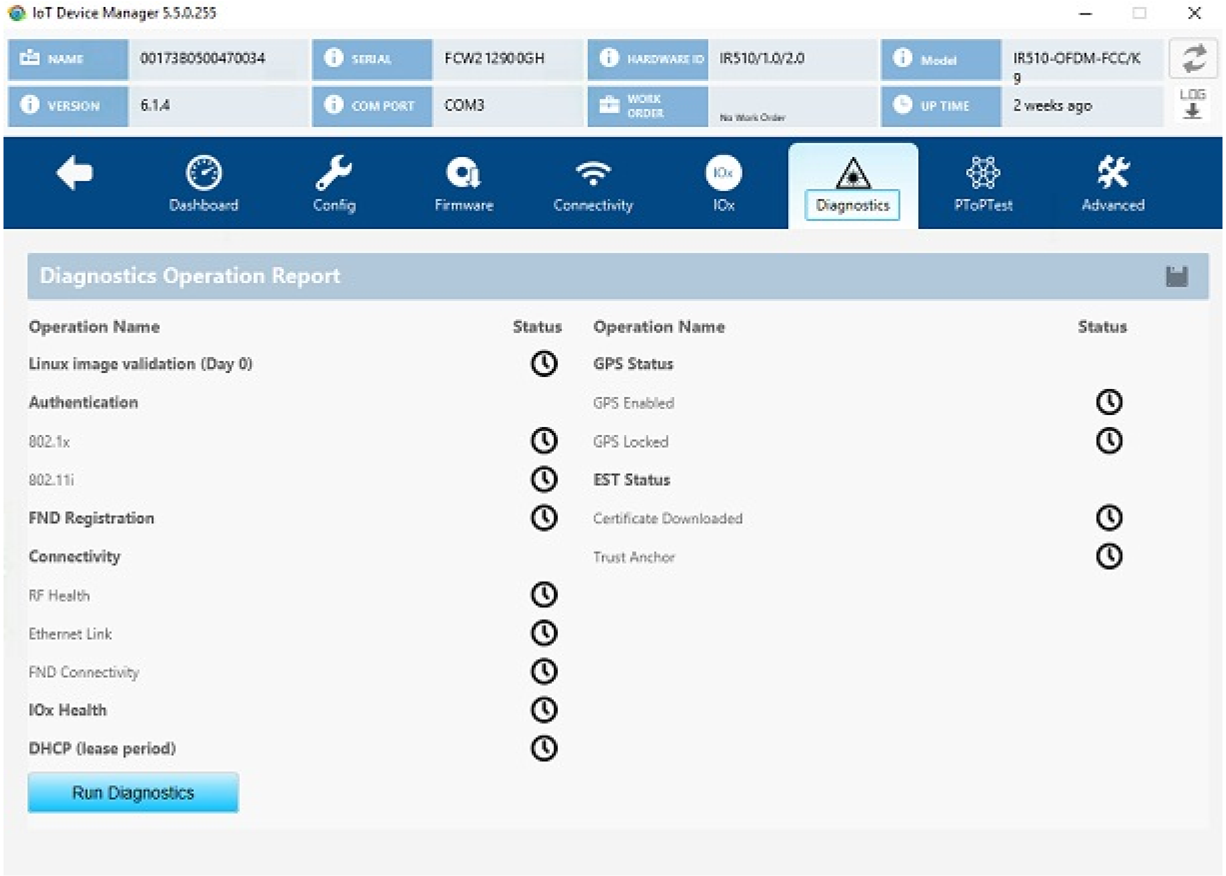
```
ls
```

Diagnostic Operations on IR510

From IoT Device Manager Release 5.3, you can run diagnostic operations on IR510. Once completed, a simple report will be disaplayed to indicate overall health status of the device which includes any issues with the device, suggestions to correct those issues, and possible troubleshooting steps.

The following figure shows the Diagnostics tab.

Figure 13: Diagnostics Tab



IoT Device Manager 5.5.0.255

NAME	0017380500470034	SERIAL	FCW2 12900GH	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.1.4	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	2 weeks ago

Diagnostics Operation Report

Operation Name	Status	Operation Name	Status
Linux image validation (Day 0)	◷	GPS Status	
Authentication		GPS Enabled	◷
802.1x	◷	GPS Locked	◷
802.11i	◷	EST Status	
FND Registration	◷	Certificate Downloaded	◷
Connectivity		Trust Anchor	◷
RF Health	◷		
Ethernet Link	◷		
FND Connectivity	◷		
IOx Health	◷		
DHCP (lease period)	◷		

To run diagnostics, click the **Diagnostics** tab. Then click the **Run Diagnostics** button, a message dialog box showing "*Diagnostic operation is under progress, please wait.*" will be displayed. Other operations will not be allowed until the diagnostic operation is completed.

After all diagnostics are completed, successful operations will be shown as green and failed ones will be shown as red. Failed operation will have the suggestions shown when a mouse is hovered on it.

The following diagnostic operations are supported:

- Image Validation - Identifies whether the image (ROMMON or LINUX) installed on the device is in a good state.

  Error messages:

  - LINUX image is either not installed or it is corrupt. Please re-install LINUX image and try again.

- ROMMON is up and running. Please load LINUX and try again.

- Authentication Check - Checks if the device has completed 802.1x and 802.11i authentications in the network.
  - 802.1x

    Error message: Seems like 802.1x is disabled. Please follow the instructions to configure 802.1x authentication correctly.
  - 802.11i

    Error messages:
    - 802.11i is disabled. Please follow the instructions to configure 802.11i authentication correctly.
    - Seems like pmkId is not set. Please carryout 802.1x authentication.
    - Device should have at least one gtkId to participate in 802.11i authentication process.
    - gtkid is expired. Please renew it.

- DHCP Check - Verifies whether the device has the DHCP lease period and got IPV6 address assigned.

  Error message: DHCP lease is expired. Please renew it.

- FND Registration Check - Identifies whether the device is successfully registered with FND server. The following checks will be performed:
  - Time synchronization issue - IoT-DM compares the time of IR510 with the time of FND to check if the time is synchronized. If their is a time sync issue then below error message is shown:

    Error message: Device time is not synched properly. Please correct the device time and try again.
  - Registration process issue - Displays the registration failure cause.

    Error message: There seems to be issue with registration process. Error Code: xxx.
  - Certificate validity

    Error message: NMS Certificate is invalid. Please load the valid NMS certificate and try again.

  Default message: Check if the device is added in FND DB.

  Note As part of the FND registration diagnostic operation , there will be an FND API call to get the Current Time. Credentials will be taken from the CGMS Settings page if field technician had entered it before. If not, a seperate screen would be shown to you to enter the details of FND Server with which the time sync operation will be performed. You may choose to skip it if you do not want to enter the details of the FND server. In that case, the Time synchronization check will be ignored while performing diagnostic operations.

- Connectivity Diagnostic operations - Identifies whether the device connectivity is up to the mark with other interfaces on the field.
  - RF Health Check - Status of WPAN LED will be displayed.

  - Ethernet Link Check - Status of Ethernet will be displayed.
  - FND connectivity Check
- IOx Health Check - Performs the diagnostic operations on the IOx module installed in the device.
  - IOx Host Status - The status of the host on which IOx runs will be displayed.
  - IOx Status - The status of IOx process will be displayed.
- GPS Status Check
  - GPS enabled or not
  - GPS locked or not
- EST Status Check
  - Certificate downloaded or not
  - Trust anchor present or not