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
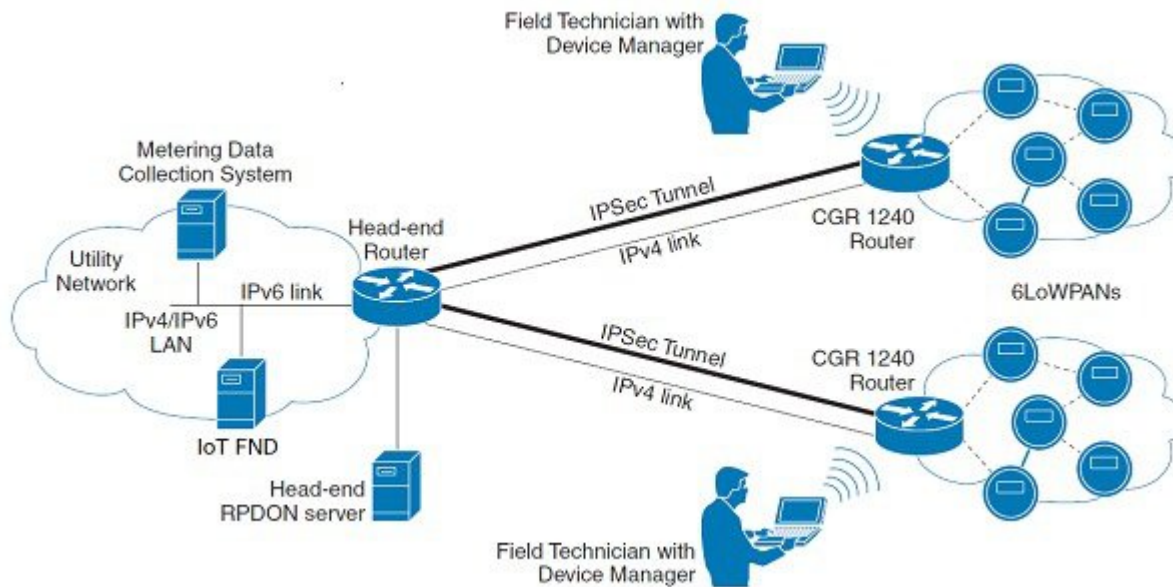
User Interface

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)

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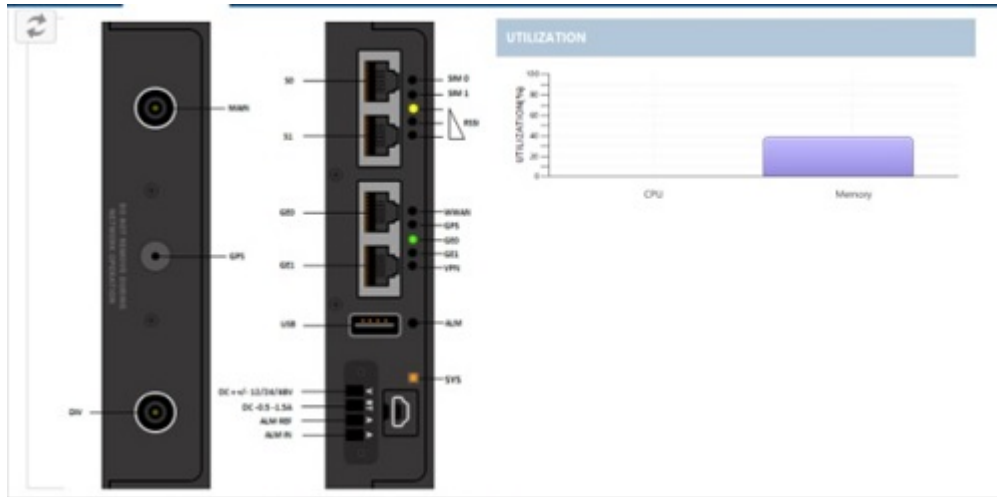
Note   Point to an active LED or port in the front or rear view of the device to display a tooltip. Items on the mini-dashboard also have tooltips.

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

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.)	• You need to check statistics for the Ethernet and Serial ports.
Use the Ethernet interface popup menu to manage the interface. (See Managing Interfaces.)	• 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.)	• 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.)	• 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
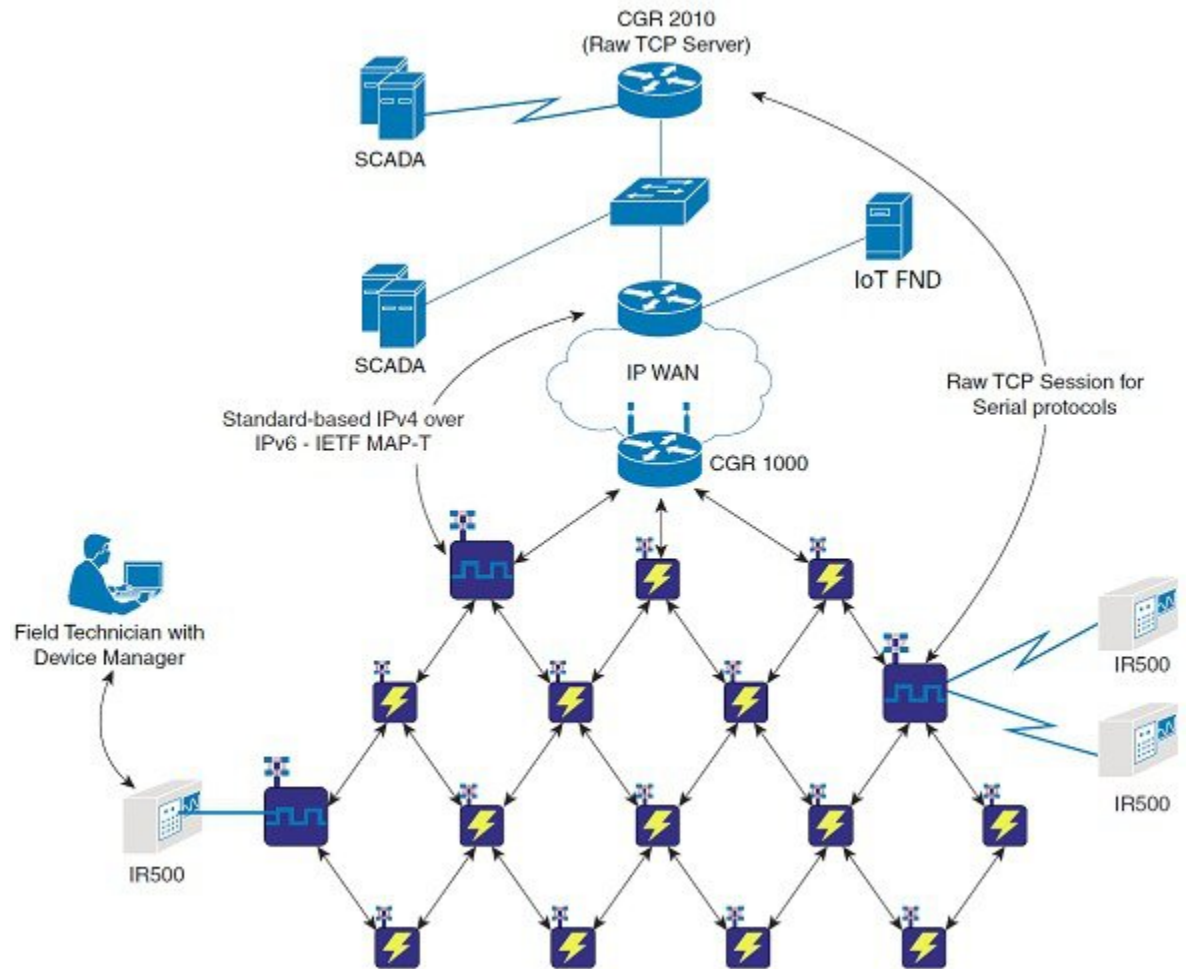
User Interface

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 .

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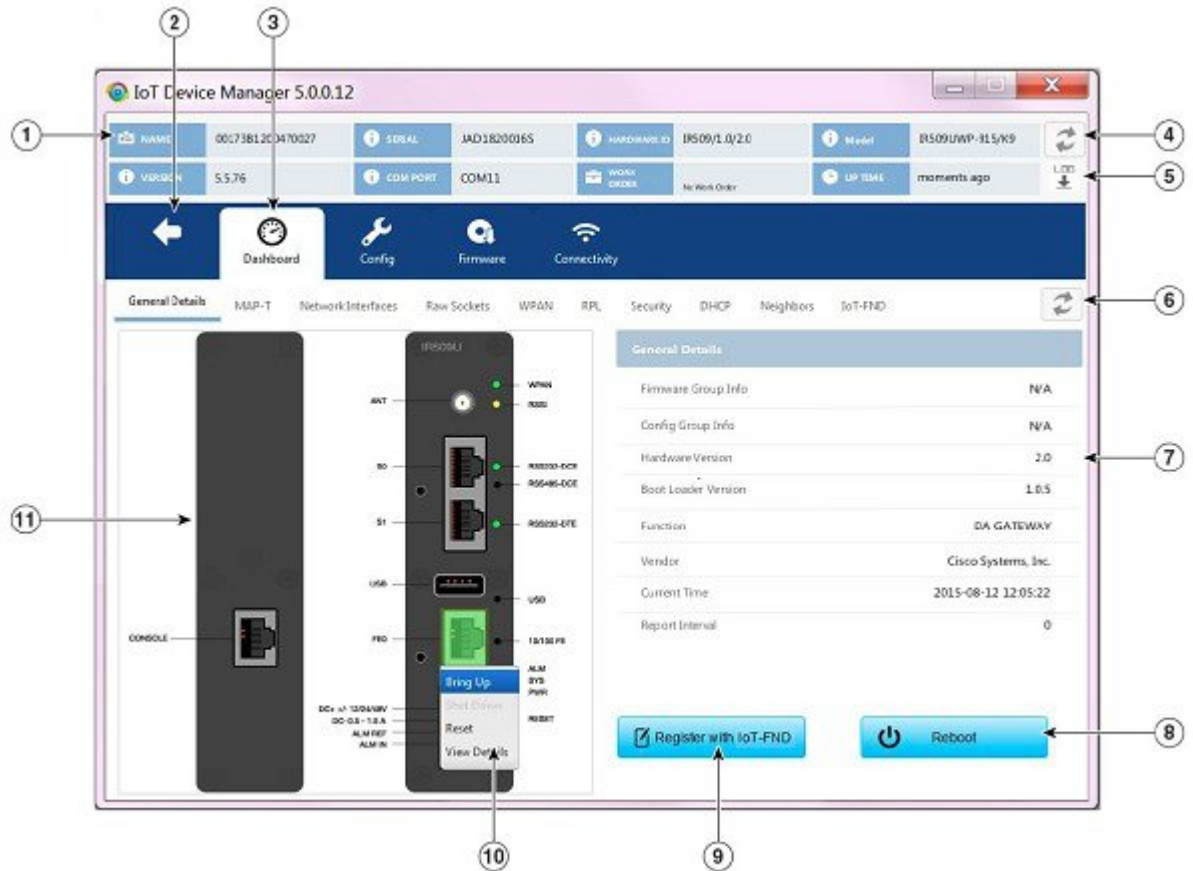
1	Mini-dashboard	7	Details area
2	Disconnect from device	8	Reboot device
3	Menu tabs	9	Register with IoT-FND
4	Refresh button for mini-dashboard	10	Pop-up menu
5	IoT-DM application log file	11	Front (right) and rear (left) views of device
6	Refresh button for Dashboard		

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-home
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.