



Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1

First Published: March 2015

Cisco Systems, Inc.

www.cisco.com

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

No combinations are authorized or intended under this document.

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

© 2015 Cisco Systems, Inc. All rights reserved.



CHAPTER 1**Overview of Cisco Connected Grid Device Manager 1-1**

- Application 1-1
- Device Manager and CGR 1000 1-2
 - User Interface 1-3
 - Tasks 1-6
- Device Manager and IR500 1-7
 - User Interface 1-9
 - Tasks 1-11
- Certificates 1-12
- Work Orders 1-12
- User Accounts 1-12
- Additional Information 1-13
- Feature History 1-14

CHAPTER 2**Installation 2-1**

- Required Expertise 2-1
- System Requirements 2-1
- Device Manager Installation 2-2
- Device Manager Removal 2-5

CHAPTER 3**Managing Work Orders 3-1**

- Work Orders 3-2
- Importing Certificates 3-3
- Setting Up the CG-NMS Connection 3-5
- Synchronizing With CG-NMS 3-6
- Updating Work Order Status 3-6
- Override Work Order 3-7

CHAPTER 4**Performing Tasks on the CGR 1000 4-1**

- Connecting to the CGR 1000 4-1
 - Connecting to the Router with a Work Order 4-1

- Manually Connecting to the Router 4-2
- Testing Connectivity 4-3
 - Adding a Device IP Address 4-4
 - Pinging a Device IP Address 4-4
 - Failed Ping 4-5
 - Tracing the Route of a Device IP Address 4-5
 - Deleting or Editing a Device IP Address 4-6
- Managing Interfaces 4-6
 - Resetting an Interface 4-7
 - Viewing Details for an Interface 4-8
 - Bringing Up an Interface 4-9
 - Shutting Down an Interface 4-9
- Changing the Configuration 4-9
 - Adding a Configuration File 4-10
 - Downloading a Configuration File 4-11
 - Replacing a Configuration File 4-11
 - Removing a Configuration File 4-12
- Updating the Firmware Image 4-12
 - Adding an Image 4-13
 - Uploading an Image to the Router 4-14
 - Installing an Image 4-15
 - Removing an Image 4-15
- Retrieving Logs 4-15
 - Retrieving and Saving Logs 4-16
- Managing Modules 4-17
 - Inserting a Module 4-18
 - Removing a Module 4-19
- Executing Commands 4-20
- Disconnecting from the CGR 1000 4-22

CHAPTER 5

Performing Tasks on the IR500 5-1

- Connecting to the IR500 5-1
 - Connecting the Laptop to the IR500 5-2
 - Connecting to the IR500 with a Work Order 5-3
 - Manually Connecting to the IR500 5-4
- Viewing Settings and Status 5-4
 - General Details 5-5
 - MAP-T 5-6

Network Interfaces	5-7
Raw Sockets	5-9
WPAN	5-10
RPL	5-11
Security	5-13
DHCP	5-15
Neighbors	5-16
CG-NMS	5-17
Viewing Interface Details	5-19
Ethernet Interface Details	5-19
Serial Interface Details	5-21
Managing the Ethernet Interface	5-23
Registering with CG-NMS	5-23
Rebooting the IR500	5-23
Changing the Configuration	5-23
Changing General Settings	5-24
Changing MAP-T Settings	5-25
Changing Serial Interface 0 Settings (DCE)	5-26
Changing Serial Interface 1 Settings (DTE)	5-28
Updating the Firmware Image	5-29
Uploading an Image	5-29
Installing an Image	5-30
Setting the Backup	5-31
Testing Connectivity	5-31
Disconnecting from the IR500	5-33



Overview of Cisco Connected Grid Device Manager

This chapter provides an overview of the Cisco Connected Grid Device Manager (Device Manager) for Cisco 1000 Series Connected Grid Routers (CGR 1000 or router) running Cisco IOS and for the Cisco 500 Series WPAN Industrial Routers (IR500).

This chapter includes the following sections:

- [Application, page 1-1](#)
- [Device Manager and CGR 1000, page 1-2](#)
- [Device Manager and IR500, page 1-7](#)
- [Certificates, page 1-12](#)
- [Work Orders, page 1-12](#)
- [User Accounts, page 1-12](#)
- [Additional Information, page 1-13](#)
- [Feature History, page 1-14](#)

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 also supports management of the IR500, 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).

Cisco Connected Grid Network Management System (Cisco CG-NMS) manages multiple CGR 1000 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 CG-NMS:
 - When operating with CG-NMS, a Device Manager user can retrieve work orders from the system as well as perform all supported tasks on the main page (see [Figure 1-2](#)) except as limited by the privilege level that the administrator configures on the router for that user.
 - When operating without CG-NMS, 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.

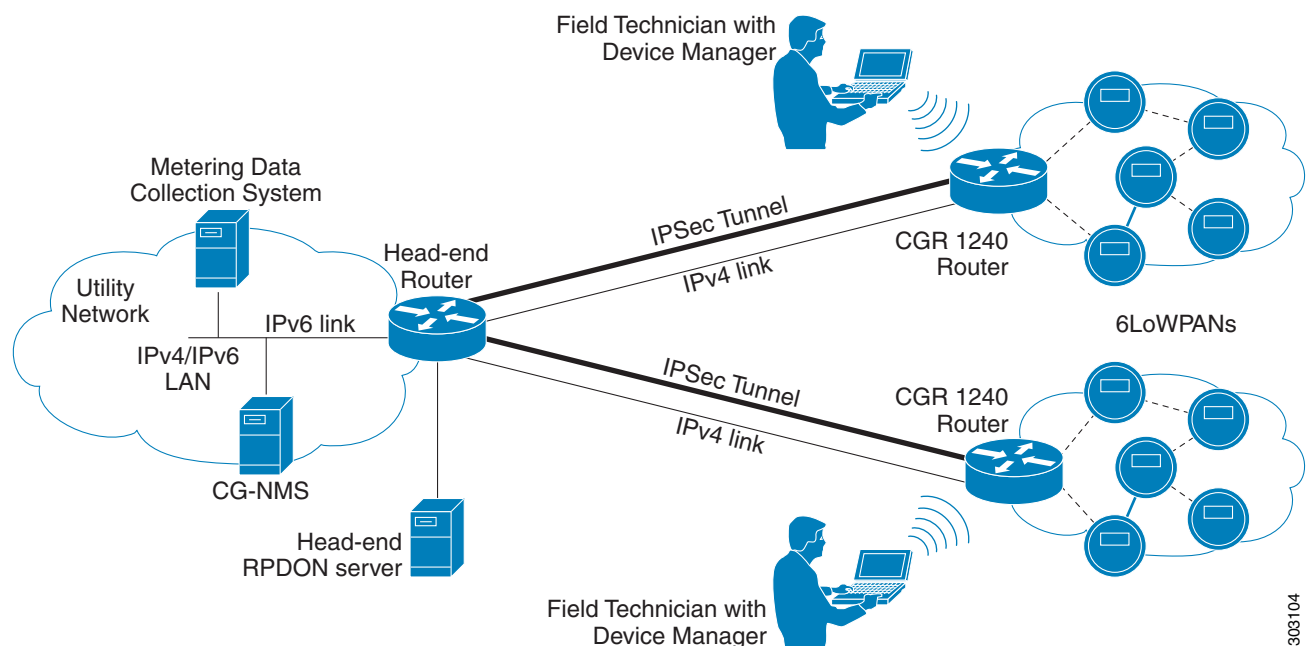
- Device Manager can manage IR500 devices in Connected Grid field deployments operating with or without CG-NMS:
 - When operating with CG-NMS, a Device Manager user can retrieve work orders from the system as well as perform all supported tasks on the main page (see [Figure 1-4](#)).
IR500 devices use CoAP Simple Management Protocol (CSMP) for communicating with CG-NMS. The IR500 regularly reports inventory metrics to CG-NMS using CSMP. CG-NMS stores the reported properties and metrics.
 - When operating without CG-NMS, 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 CG-NMS.

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, Ethernet, and WiFi.

Device Manager connects to the CGR 1000 by using a secure Ethernet or WiFi link. (See [Figure 1-1](#).)

Figure 1-1 Device Manager Application Within a Connected Grid Network



This section covers the following topics:

- [User Interface, page 1-3](#)
- [Tasks, page 1-5](#)

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, page 4-1.](#))

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 1-1.](#)

For an overview of all the tasks that you can perform with Device Manager, refer to [Table 1-2.](#)

[Figure 1-2](#) shows the common page elements and controls for the Device Manager pages.

Figure 1-2 Device Manager Common Page Elements and Controls (CGR 1000)



391537

1	Mini-dashboard	8	Refresh button for mini-dashboard
2	Disconnect from device	9	CG-DM application log file
3	Menu tabs	10	Troubleshooting wizard
4	Power status (CGR 1240 only)	11	Battery information
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



Tip

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 1-2](#)) appears at the top of every Device Manager page, and provides the information listed in [Table 1-1](#).

Table 1-1 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	AC ON or AC OFF (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 (shown if connected to the router using a work order)

Tasks

Device Manager displays the main page (see [Figure 1-2](#)) 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, page 1-12](#) for more information about user accounts and privilege

levels.) [Table 1-2](#) 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 1-2 *Device Manager Tasks (CGR 1000)*

Task	Example of When to Perform Task
<p>Use the Dashboard to check the status of router hardware, such as BBU (optional), power, and modules.</p> <p>(See User Interface, page 1-3.)</p>	<ul style="list-style-type: none"> 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 <i>System Casing Open</i>, 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 <i>System Casing Closed</i>.
<p>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.</p> <p>(See Testing Connectivity, page 4-3.)</p>	<ul style="list-style-type: none"> Devices connected to a CGR 1000 cannot be reached. Start the Device Manager, connect to the router, and then check connectivity to the device.
<p>Bring up or shut down a CGR 1000 interface and view details for an interface.</p> <p>(See Managing Interfaces, page 4-6.)</p>	<ul style="list-style-type: none"> 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.
<p>Update the CGR 1000 configuration with a provided configuration file, and then reboot the router with the new configuration.</p> <p>(See Changing the Configuration, page 4-9.)</p>	<ul style="list-style-type: none"> 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. <p>After you install the configuration file, the router automatically reboots with the new configuration.</p>
<p>Upload a copy of a software image onto the CGR 1000 for immediate installation or for a deferred update of the image.</p> <p>(See Updating the Firmware Image, page 4-12.)</p>	<ul style="list-style-type: none"> 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. <p>The router automatically reboots after you update the software image.</p>
<p>Download and view the CGR 1000 system logs.</p> <p>(See Retrieving Logs, page 4-15.)</p>	<ul style="list-style-type: none"> You need to review the CGR 1000 system logs to troubleshoot the CGR 1000. Start Device Manager and click the Log tab.

Table 1-2 Device Manager Tasks (CGR 1000) (continued)

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 , page 4-17.)	<ul style="list-style-type: none"> A WiMAX 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 , page 4-20.)	<ul style="list-style-type: none"> You need to review the CGR 1000 configuration information to troubleshoot the CGR 1000. Start Device Manager and click the Advanced tab.

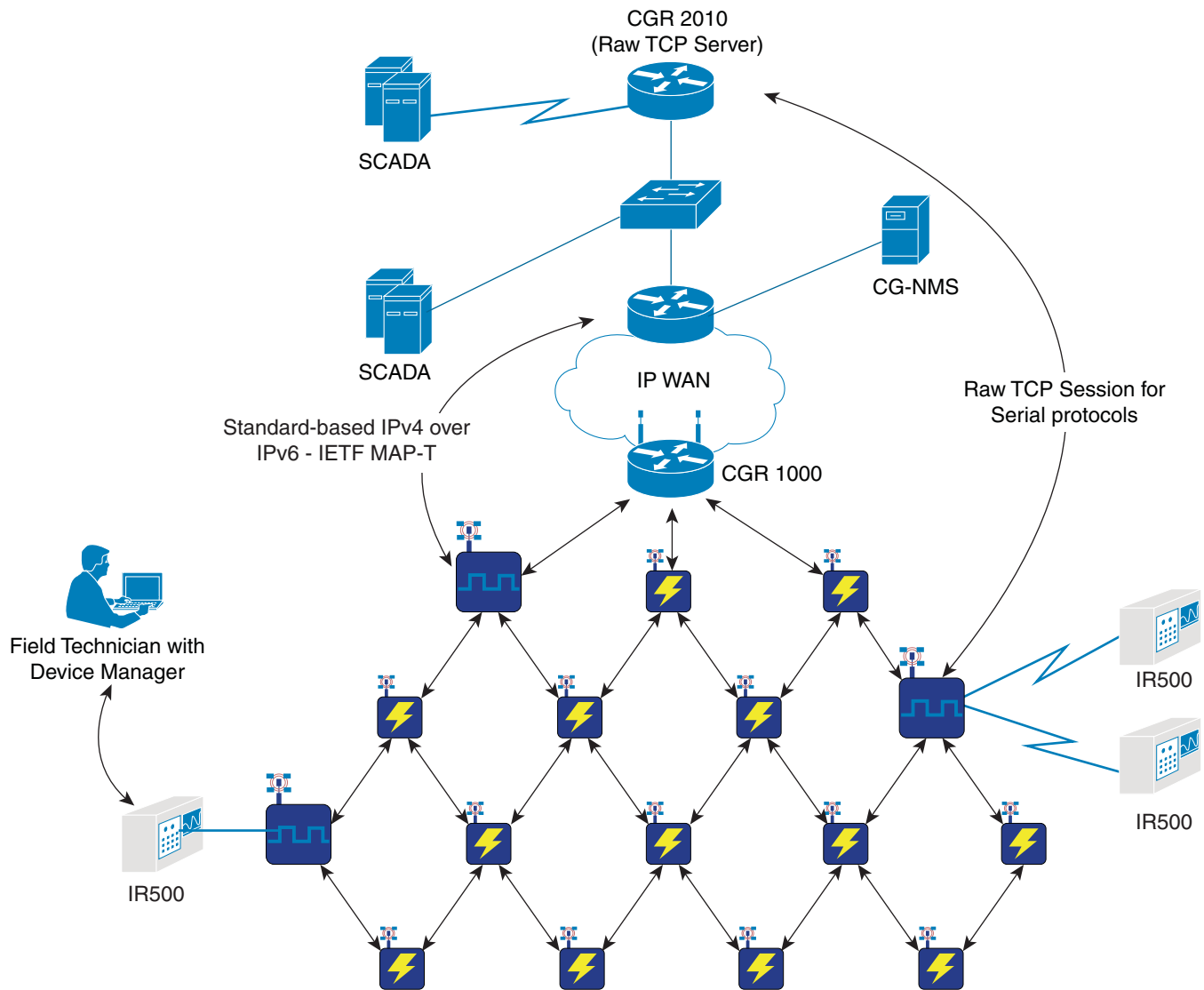
Device Manager and IR500

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 CG-Mesh by transporting serial data over TCP/IP. The IR500 also provides remote connectivity to IPv4 DA devices over the IPv6-based CG-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](#).

Figure 1-3 shows the IR500 in a CG-Mesh deployment.

Figure 1-3 IR500 in a CG-Mesh Network



This section covers the following topics:

- [User Interface](#), page 1-9
- [Tasks](#), page 1-11

353569

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, page 5-1](#)).

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, page 5-4](#)).

At the top of the screen, a mini-dashboard provides additional details on the device as detailed in [Table 1-3](#).

For an overview of all the tasks that you can perform with Device Manager, refer to [Table 1-2](#).

[Figure 1-4](#) shows the common page elements and controls for the Device Manager pages.

Figure 1-4 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 NMS
4	Refresh button for mini-dashboard	10	Pop-up menu
5	CG-DM application log file	11	Front (right) and rear (left) views of device
6	Refresh button for Dashboard		

**Tip**

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 mini-dashboard (see [Figure 1-4](#)) appears at the top of every Device Manager page, and provides the information listed in [Table 1-3](#).

Table 1-3 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 1-4](#)) after securely connecting to the IR500. From the Menu tabs on the main page, you can perform the tasks listed in [Table 1-4](#).

Table 1-4 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, page 1-9 and Viewing Settings and Status, page 5-4 .)	<ul style="list-style-type: none"> 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, page 5-19 .)	<ul style="list-style-type: none"> 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, page 5-23 .)	<ul style="list-style-type: none"> You need to bring up, shutdown, or reset the Ethernet interface.
View details about IR500 settings and status. (See Viewing Settings and Status, page 5-4 .)	<ul style="list-style-type: none"> 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 CG-Mesh network and troubleshoot issues.
Configure or modify general, MAP-T, and serial interface settings. (See Changing the Configuration, page 5-23 .)	<ul style="list-style-type: none"> 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.

Table 1-4 Device Manager Tasks (IR500) (continued)

Task	Example of When to Perform Task
Upload, install, and back up a copy of a software image. (See Updating the Firmware Image , page 5-29.)	<ul style="list-style-type: none"> 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 , page 5-31.)	<ul style="list-style-type: none"> 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 CGR 1000 or to the IR500.

You can import certificates through the Device Manager opening page. (See [Importing Certificates](#), page 3-3.)

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 CGR 1000 routers and IR500 DA gateways and synchronize with Cisco CG-NMS to download work orders. (See [Managing Work Orders](#), page 3-1.) Device Manager needs to be connected to CG-NMS only to download and update the work orders.

User Accounts

The CG-NMS administrator creates user accounts for the field technicians who use Device Manager to download work orders from CG-NMS. 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

Table 1-5 shows the required privilege level for the listed tasks.

Table 1-5 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
IR500	<i>Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide</i>
CG-NMS	<i>Cisco Connected Grid Network Management System User Guide, Release 2.1</i>
WPAN and CG-Mesh	<i>Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)</i>
Raw Socket	<i>Raw Socket Transport Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)</i> <i>Configuring Raw Socket Protocol on the CGR 2010 Router</i>

Feature History

Feature Name	Release	Feature Information
Cisco Connected Grid Device Manager (DM) for Cisco IOS	Cisco CG-DM Release 4.1	Support for Cisco 500 Series WPAN Industrial Routers (IR500) running firmware version 5.5.74 or greater. Note The CGR 1000 must run Cisco IOS Release 15.5(1)T1 to support connectivity to the IR500.
	Cisco CG-DM Release 4.0	Initial support of the feature on the CGR 1000 running Cisco IOS Release 15.4(3)M or greater. Note CG-DM might not work properly with older versions of Cisco IOS on the CGR 1000.



Installation

This chapter explains how to install the Device Manager software and contains the following sections:

- [Required Expertise, page 2-1](#)
- [System Requirements, page 2-1](#)
- [Device Manager Installation, page 2-2](#)
- [Device Manager Removal, page 2-5](#)

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 4.1.

Laptop

The laptop running Device Manager must have the following:

- Microsoft Windows 7 Enterprise
- 2 GHz or faster processor recommended
- 1 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, page 1-14](#) for CGR 1000 software requirements.

IR500

See [Feature History, page 1-14](#) for IR500 firmware requirements.

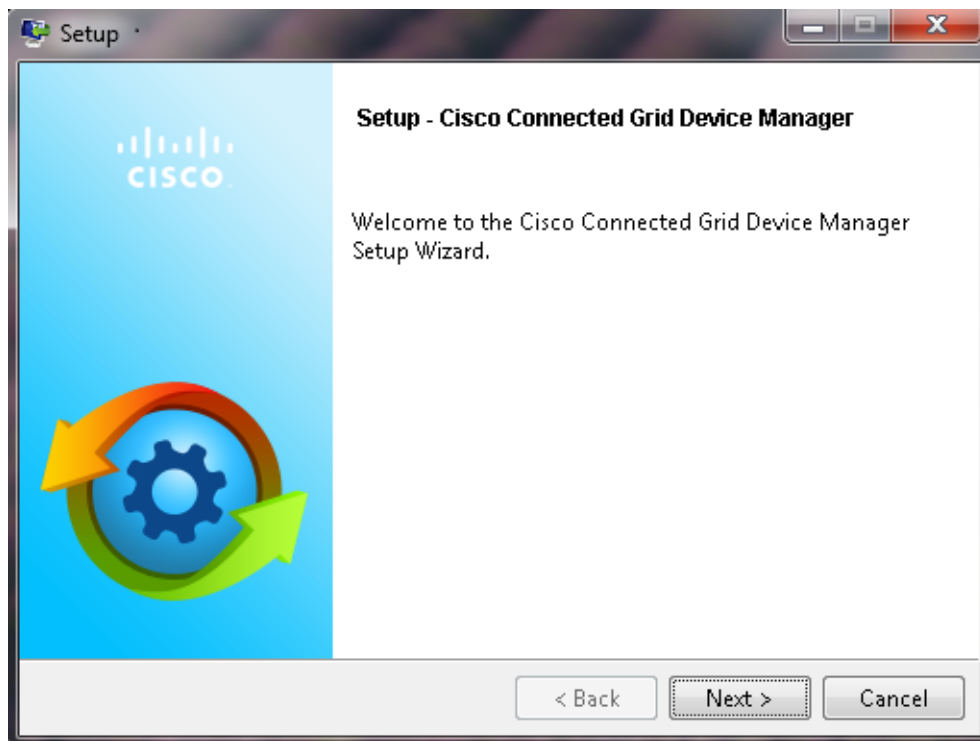
CG-NMS

To work with Device Manager, CG-NMS must be Release 2.1 or greater.

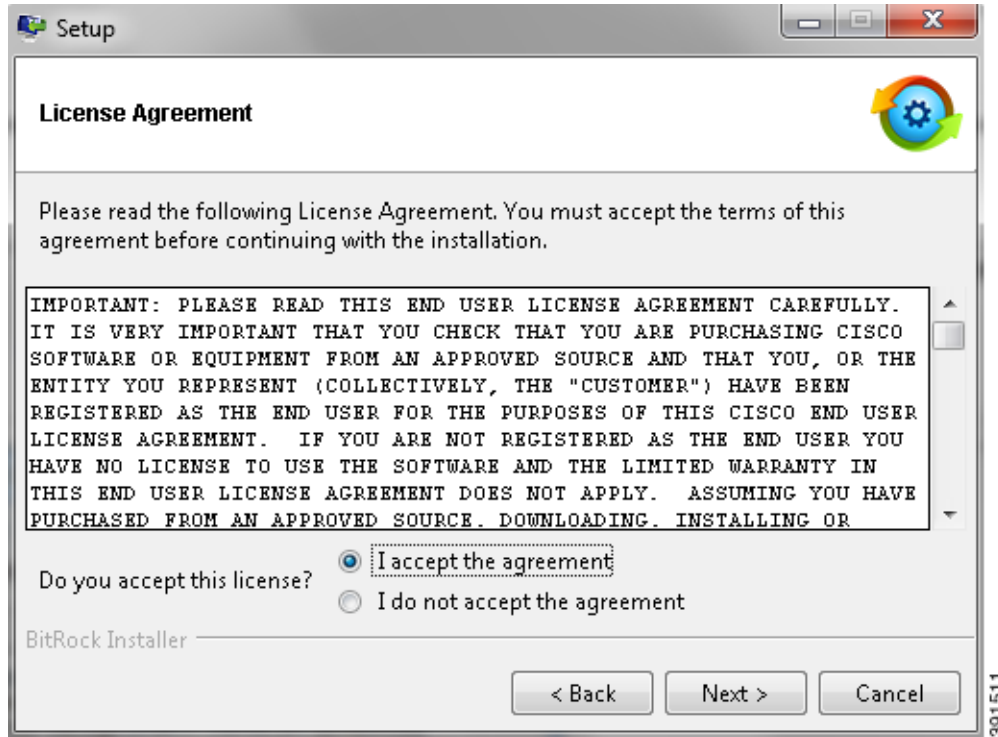
Device Manager Installation

To install the Device Manager:

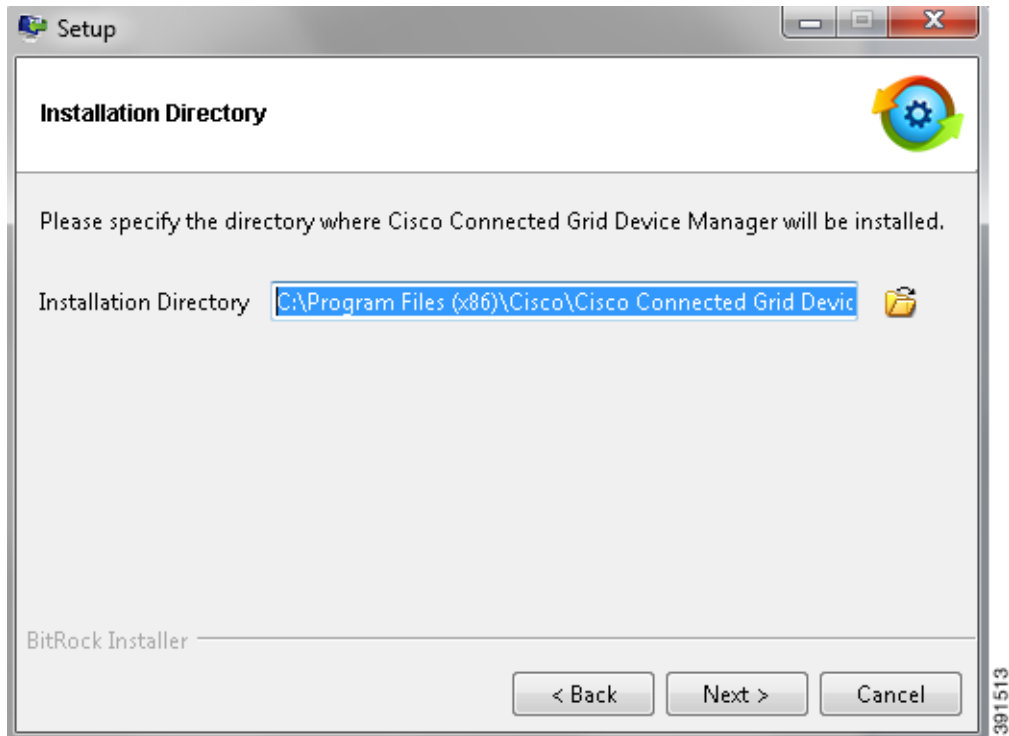
-
- Step 1** Double-click the Device Manager installer executable to start installation.
 - Step 2** Click **Next**.



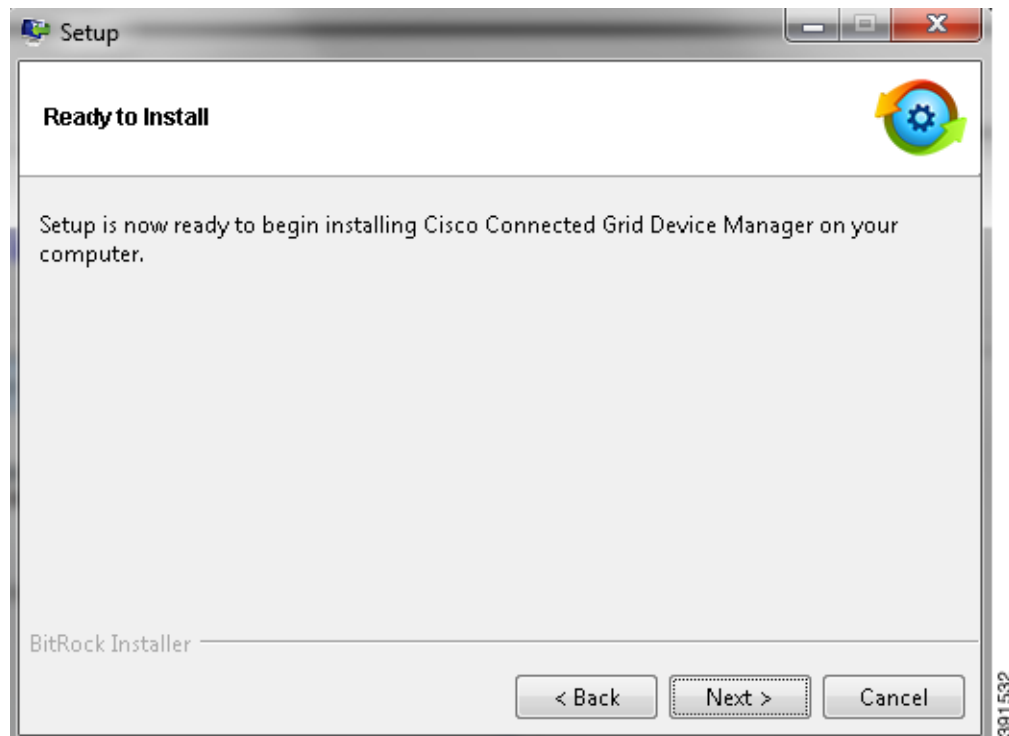
Step 3 Select the check box to accept the terms of the License Agreement, and then click **Next**.



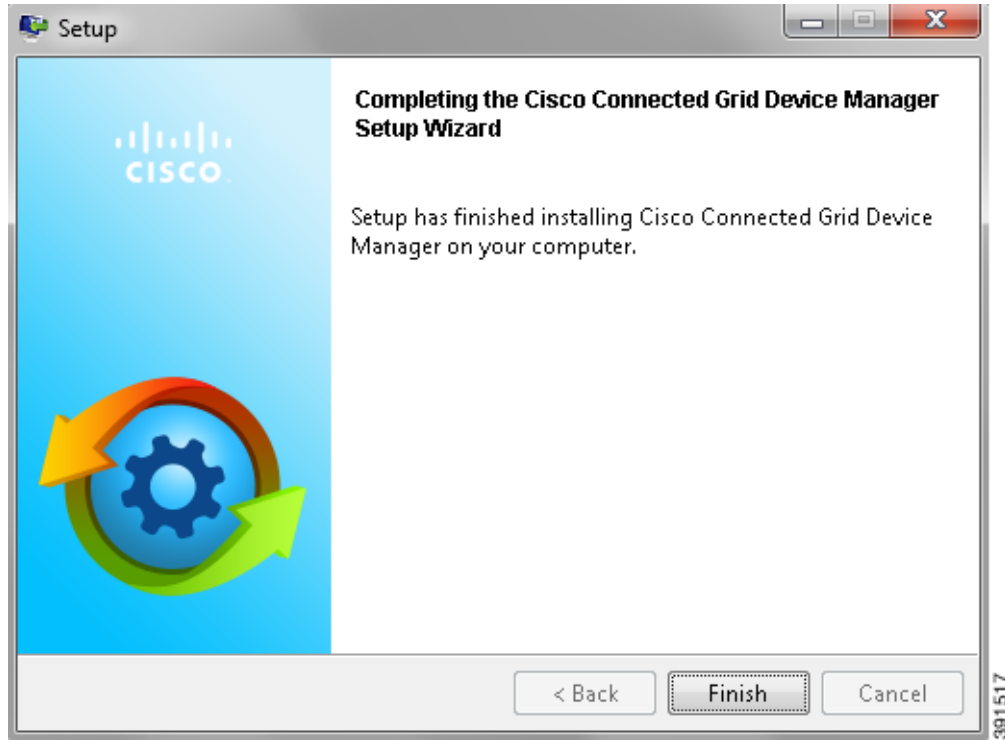
- Step 4** Select an installation directory by clicking the folder icon and browsing to a directory, or click **Next** to accept the default directory.



- Step 5** Click **Next** to begin the installation.



Step 6 Click **Finish** to exit the Setup Wizard and launch the Device Manager.



Device Manager Removal

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



Managing Work Orders

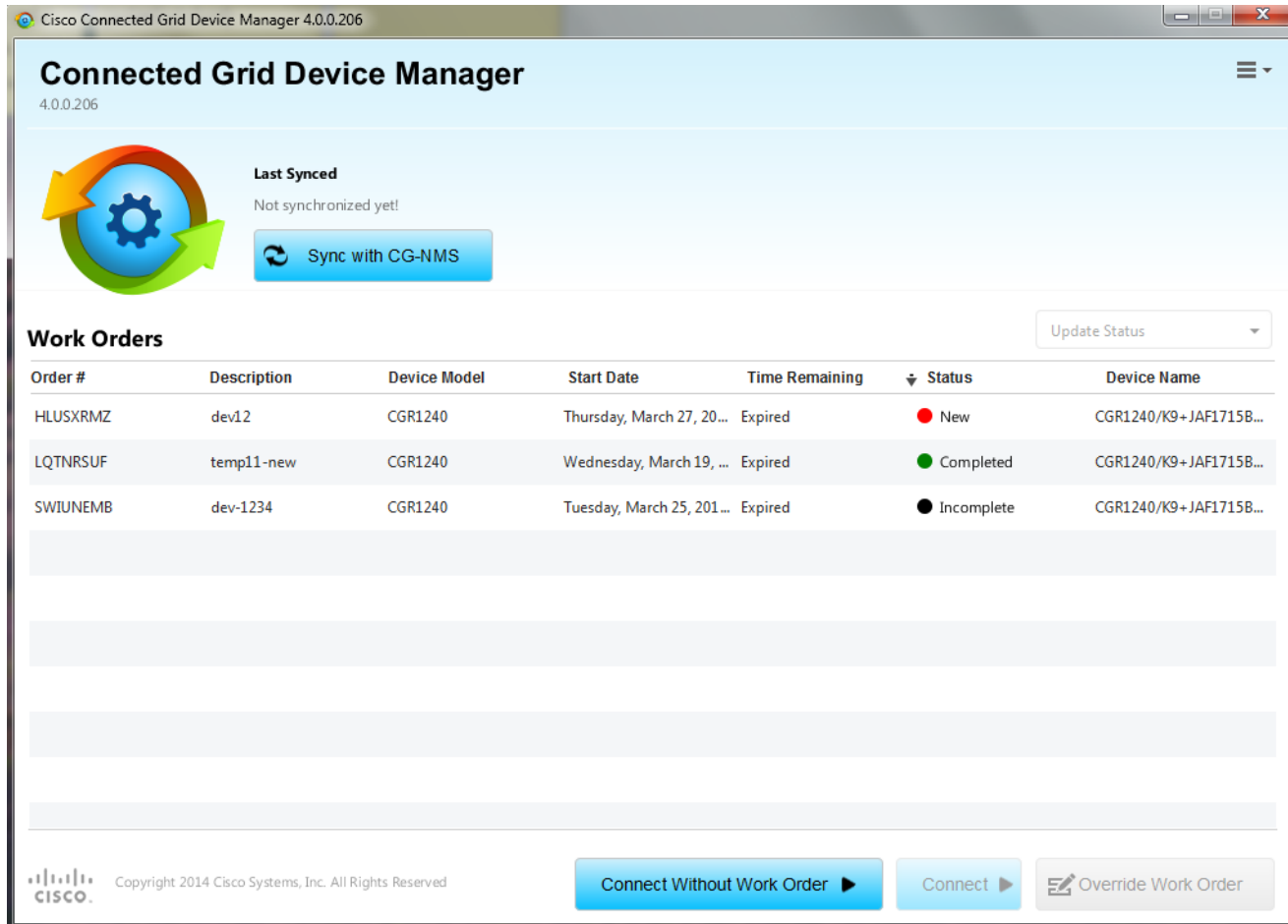
The chapter describes using the Device Manager opening page with the CGR 1000 or IR500 to connect to CG-NMS and manage work orders. This chapter contains the following sections:

- [Work Orders, page 3-2](#)
- [Importing Certificates, page 3-3](#)
- [Setting Up the CG-NMS Connection, page 3-5](#)
- [Synchronizing With CG-NMS, page 3-6](#)
- [Updating Work Order Status, page 3-6](#)
- [Override Work Order, page 3-7](#)

Work Orders

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

Figure 3-1 Device Manager Opening Page



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

You must synchronize Device Manager with CG-NMS to download the latest work orders from CG-NMS and upload status of the work orders to CG-NMS. See [Synchronizing With CG-NMS, page 3-6](#).

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

Work Orders

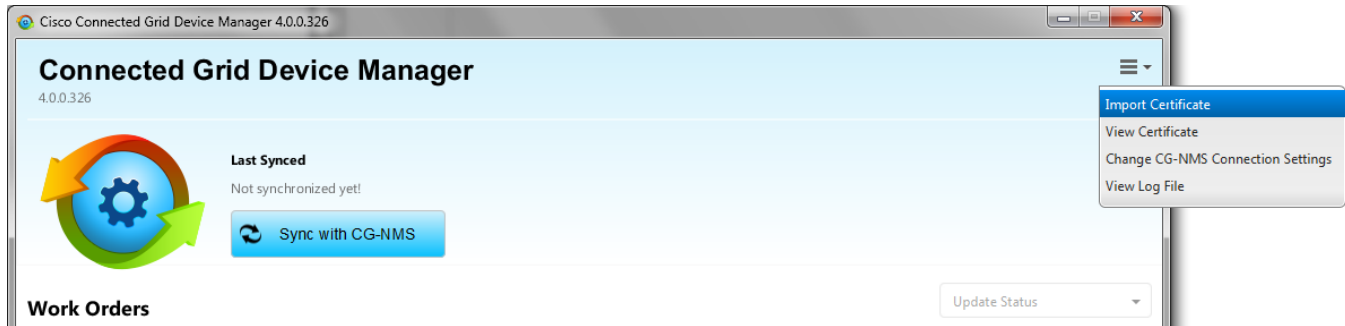
Order #	Description	Device Model	Start Date	Time Remaining	Status	Device Name
ASAUYKSY	qwee	IR500	Thursday, September 11...	6 Day(s)	New	00173b1200470027

Importing Certificates

As admin, you can import certificates through the Device Manager opening page. You need to know the path to the certificate (.pfx) and the certificate password. The certificate password is created when the .pfx file is created. Generally, the admin downloads the .pfx file to the Device Manager laptop.

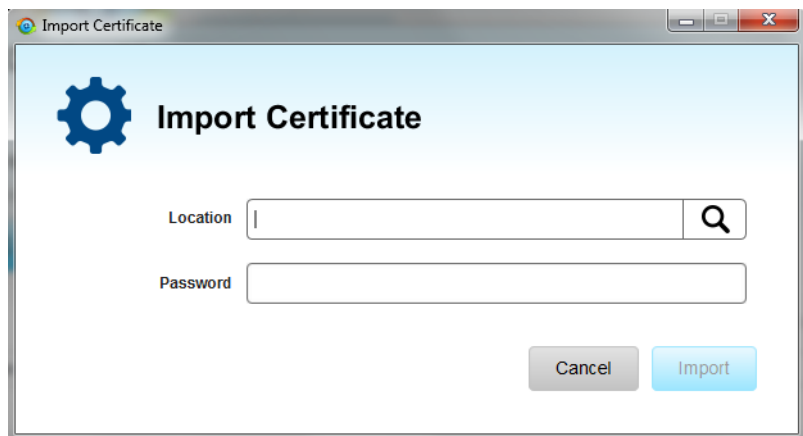
To import a certificate:

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



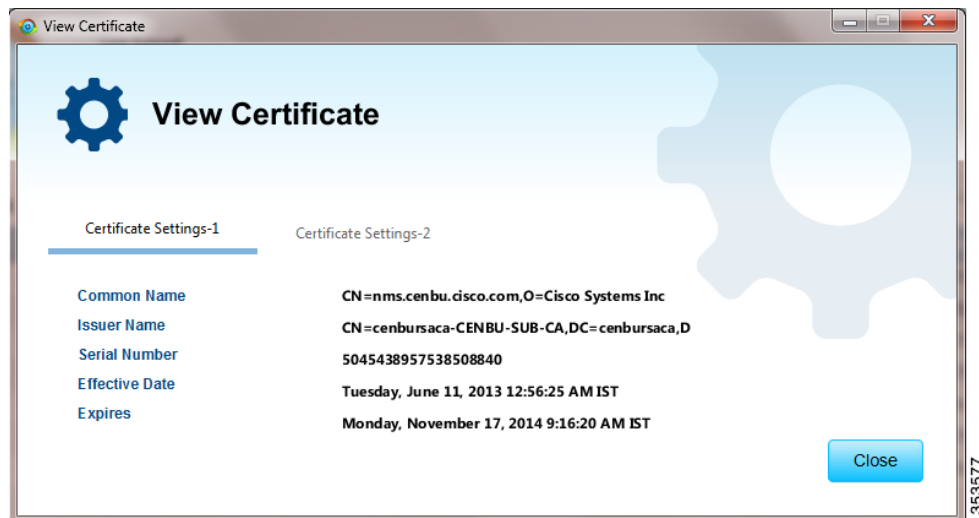
391515

- Step 2** In the Import Certificate dialog box, browse to the location of the certificate file (.pfx) on your laptop.



391514

- Step 3** Enter the certificate password and then click **Import**.
A dialog box displays a success message and informs you to restart Device Manager.
- Step 4** Restart Device Manager.
- Step 5** To view the certificate details, select **View Certificate** from the Device Manager opening page drop-down menu on the upper right.

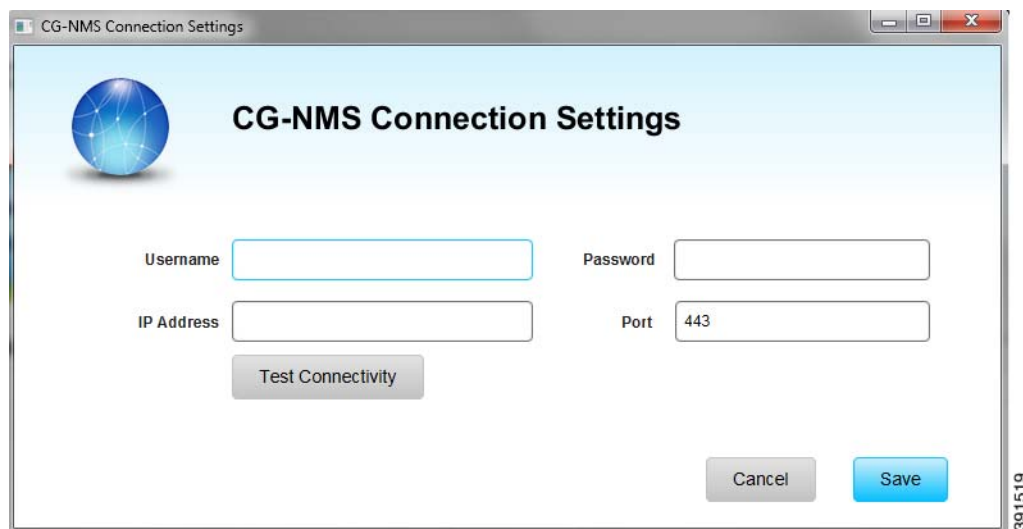


Step 6 Click the tab for the certificate details you want to view.

Setting Up the CG-NMS Connection

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

- Step 1** On the Device Manager opening page, click **Sync with CG-NMS**, or select **Change CG-NMS Connection Settings** from the drop-down menu on the upper right of the page.
- Step 2** In the CG-NMS Connection Settings dialog box, enter the username, password, and IP address for connecting to the CG-NMS application server.



Step 3 Confirm or change the server port number.

- Step 4** Click **Save**.
- Step 5** Click **Test Connectivity** to test connecting to the CG-NMS server.
-

Synchronizing With CG-NMS

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



Note You can only download assigned work orders from CG-NMS.

To download the latest work orders from CG-NMS and upload the status of the work orders to CG-NMS:

- Step 1** On the Device Manager opening page, click **Sync with CG-NMS**.
- Device Manager verifies the authorization for connecting to the CG-NMS 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, page 4-1](#) or [Connecting to the IR500 with a Work Order, page 5-3](#).
-

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 CG-NMS 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 CG-NMS with the changes.

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

To update the status of a work order:

- 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 CG-NMS** to update CG-NMS.

After synchronization with CG-NMS, 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:

-
- Step 1** On the Device Manager opening page, click **Override Work Order**.
 - Step 2** Follow the steps in [Manually Connecting to the Router, page 4-2](#) for the CGR 1000 or [Manually Connecting to the IR500, page 5-4](#) for the IR500.
-



Performing Tasks on the CGR 1000

The chapter explains how to use the Device Manager to perform tasks on the CGR 1000 and contains the following sections:

- [Connecting to the CGR 1000, page 4-1](#)
- [Testing Connectivity, page 4-3](#)
- [Managing Interfaces, page 4-6](#)
- [Changing the Configuration, page 4-9](#)
- [Updating the Firmware Image, page 4-12](#)
- [Retrieving Logs, page 4-15](#)
- [Managing Modules, page 4-17](#)
- [Executing Commands, page 4-20](#)
- [Disconnecting from the CGR 1000, page 4-22](#)

Connecting to the CGR 1000

You can use Device Manager in the following ways:

- **Operating with CG-NMS**—When you have CG-NMS 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 CG-NMS, follow the steps in [Setting Up the CG-NMS Connection, page 3-5](#).
- **Operating without CG-NMS**—When you do not have CG-NMS 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 [Chapter 3, “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**.

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:

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

The screenshot shows a window titled "Connect To Device" with a blue header and a globe icon. The main content area has a light blue background. At the top right, there's a small image of a CGR 1000 router. Below it, the "Device Type" is set to "CGR1120". The "Connection Type" section has three buttons: "Over WiFi", "Over Ethernet", and "Auto Detect" (which is highlighted in green). The "IP Address" field contains "10.77.245.15" and the "Port" field contains "443". There is a checkbox for "Auto-discover IPv6 Address" which is unchecked. Below these are fields for "WiFi SSID", "WiFi Pass Phrase", "Device User Name" (set to "admin"), and "Device Password". At the bottom right, there are "Cancel" and "Connect" buttons. A vertical number "391520" is visible on the right edge of the dialog box.

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.



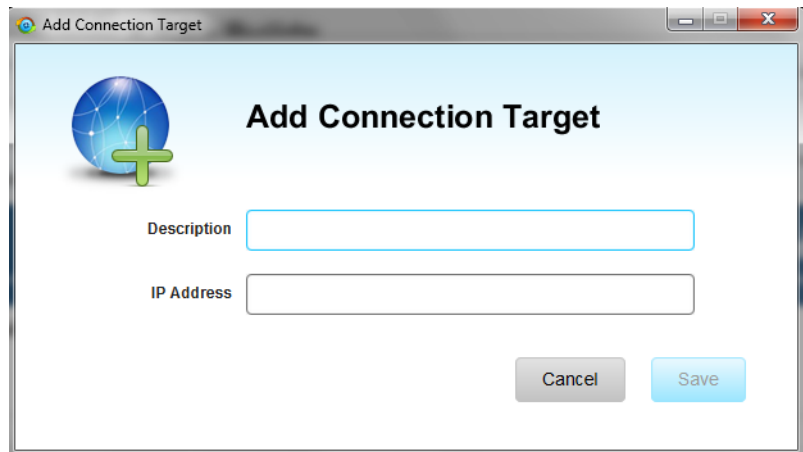
Note To Auto Discover an IPv6 address, the laptop running Device Manager must be directly connected to the CGR 1000 via Ethernet or WiFi. By design, the Auto Discover function works when there is only one active router within the same network.

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

Adding a Device IP Address

To add a device IP address:

- 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**.

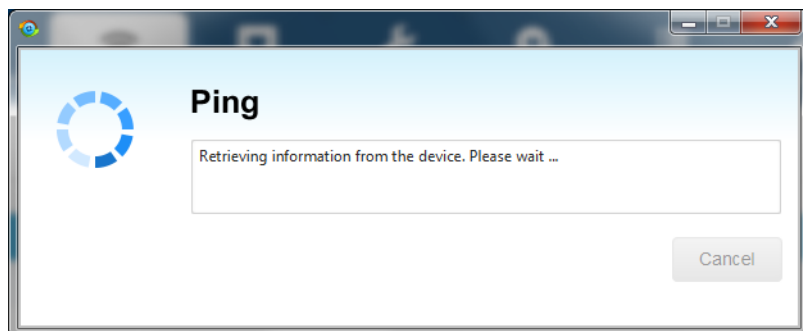
You can now test the connectivity to the device you just added to the Device Manager.

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 CGR 1000 and the device:

- 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.



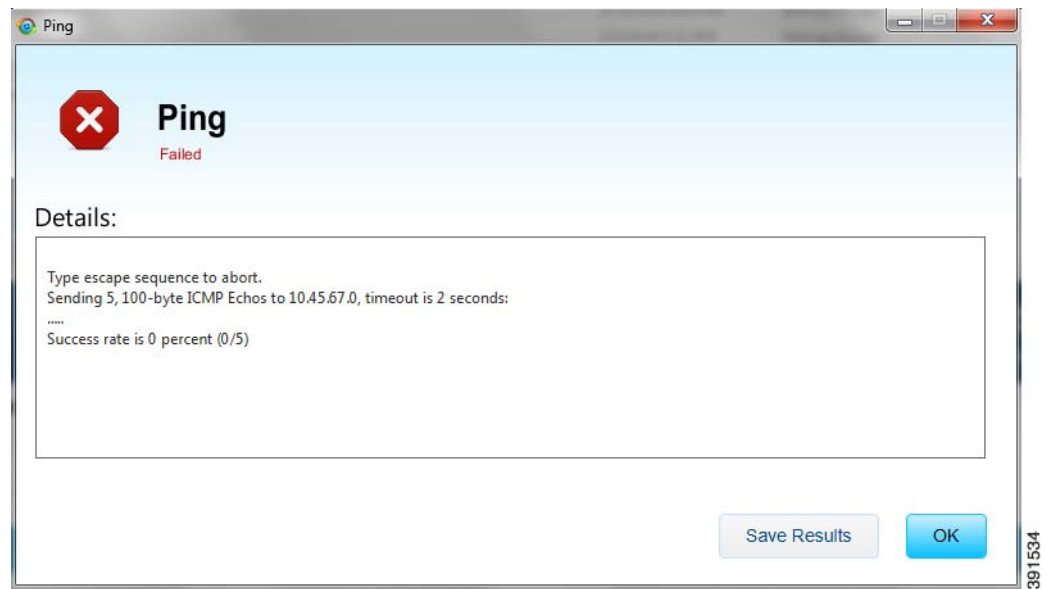
When the system successfully pings the device, a dialog box appears indicating that the ping was successful.

If the system does not successfully ping a device, refer to [Failed Ping, page 4-5](#).

- 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.



- 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, page 4-5](#).

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:

- 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, page 4-6](#).
-

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:

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

All interfaces installed within the CGR 1000 display automatically.

Interface	Description	IP Address	Line Protocol	Administrative Status
Async1/1			✗	✓
Async1/2			✗	✓
Cellular3/1			✗	✓
Dot11Radio2/1		FE80::46A7:CFFF:FED2:F4AE/64	✓	✓
FastEthernet2/3			✗	✗
FastEthernet2/4			✗	✗
FastEthernet2/5			✗	✗
FastEthernet2/6			✗	✗
GigabitEthernet0/1			✓	✓
GigabitEthernet2/1			✗	✗
GigabitEthernet2/2	2/2	10.197.73.200/27 FE80::BE16:65FF:FE31:4ED2/64	✓	✓
Vlan1			✗	✗
Wpan5/1		FE80::207:8108:8E:FB69/64 2015:1111:2222:CAFE::/64	✓	✓

This section covers the following topics:

- [Resetting an Interface](#)
- [Viewing Details for an Interface](#)
- [Shutting Down an Interface](#)
- [Bringing Up an Interface](#)

Resetting an Interface

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

-
- 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 (cellularx/1) and WiMAX (Dot16Radiox/1) interfaces only.

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:

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.

-
- 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:

-
- 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.
-

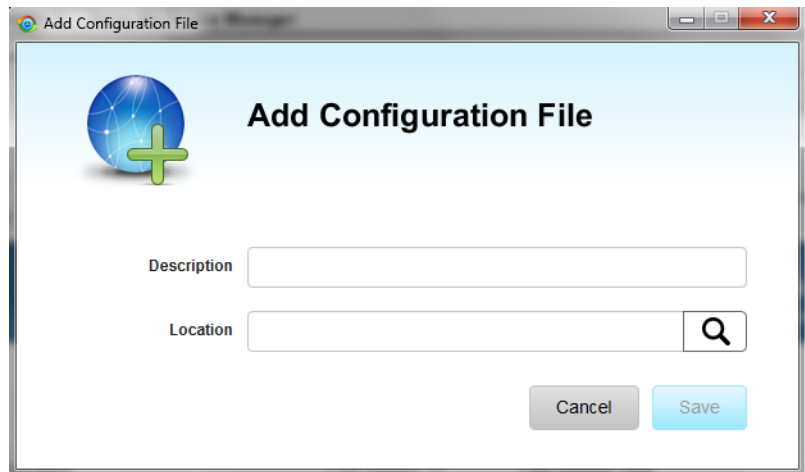
Changing the Configuration


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.



- Step 3** In the Add Configuration File dialog box:
- Enter a description for the configuration file that you are going to upload.
 - Click **Search** () to navigate to the configuration file location and select the file.
 - 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:

- 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](#)), you can find the file name listed on the Config page. You can use the file to update the CGR 1000 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 CGR 1000:

-
- 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 CGR 1000. Proceed to [Removing a Configuration File](#).
-

Removing a Configuration File

After you update the CGR 1000 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:

-
- 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, 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:

<http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/tsd-products-support-general-information.html>

Cisco Connected Grid Device Manager 4.1.0.130

NAME	CGR1240-245-10	SERIAL	JAF1715BJDN	31° C	STORAGE	305 MB / 508 MB
VERSION	15.5(1.1)T	IP ADDRESS	10.197.73.200	Door Opened	UP TIME	4 days, 4 hours, 29 ...
HYPERVISOR VERSION	1.1.1	CONNECTION	Auto Detect	Battery not present	LAST LOGIN	
MODEL	CGR1240/K9	DEVICE USER	admin		WORK ORDER	No Work Order

Navigation: Dashboard, Connectivity, Interfaces, Config, **Firmware**, Log, Modules, Advanced

Buttons: Add Image, Remove Image, Upload to Device, Install on Device

Table: No content in table

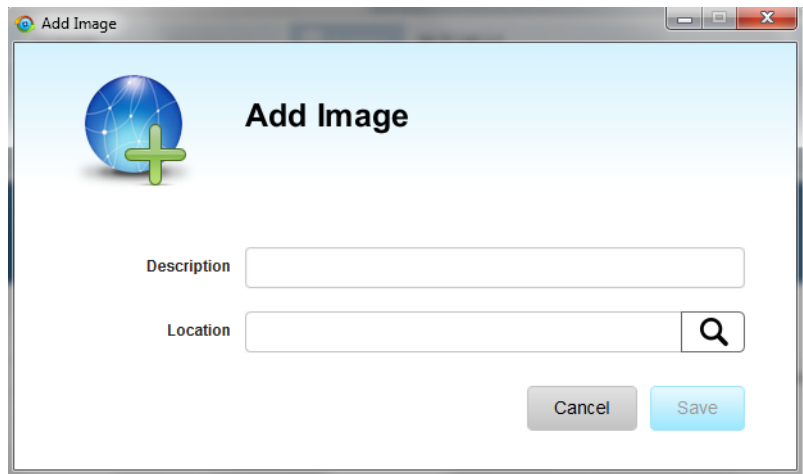
This section covers the following topics:


- [Adding an Image](#)
- [Uploading an Image to the Router](#)
- [Installing an Image](#)
- [Removing an Image](#)

Adding an Image

To add an image file to Device Manager:

- 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 CGR 1000 without initiating an immediate image install. This capability allows operations personnel to use CG-NMS or a utility management tool to install and reboot the CGR 1000 when network conditions allow.

To upload an image to the router:

- 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 CGR 1000 is not listed on the Firmware page, add the image (see [Adding an Image](#)).
- Step 3** On the Firmware page, select the CGR 1000 firmware image that you want to upload and click **Upload to Device**.

The new image is stored on the CGR 1000 router until you are ready to install the image on the router. (See [Installing an Image](#).)

Installing an Image

**Caution**

Be careful when using this feature. After this task starts, there is no way to cancel the event. Updating the CGR 1000 firmware image might take awhile to complete and requires a reboot. All connections to the router are unavailable during the image update.

To install an image:

-
- 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.
If you click **Yes**, Guest OS will not be upgraded.
If the CGR 1000 firmware image already exists in the router, you are prompted to confirm reinstalling the same image.
- Step 3** 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:

-
- Step 1** On the Update Image page, select a CGR 1000 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.

Retrieving Logs

The screenshot shows the Cisco Connected Grid Device Manager interface. At the top, there's a header with the device name 'CGR1240-245-10' and various status indicators. Below this is a navigation bar with tabs for Dashboard, Connectivity, Interfaces, Config, Firmware, Log, Modules, and Advanced. The 'Log' tab is selected. In the Log tab, there's a 'Select Task' dropdown menu with 'Fetch Log' selected and a 'Go' button. The main content area displays the output of the 'show logging' command, including details about Syslog logging, Console logging, Monitor logging, Buffer logging, Exception Logging, Count and timestamp logging, Persistent logging, Trap logging, and Log Buffer settings. The output also includes system messages such as interface link-up/down events and system restarts.

Retrieving and Saving Logs

To retrieve real-time log events from the CGR 1000:

- 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 ().

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 OK.



Tip

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



This section covers the following topics:

- [Inserting a Module](#)
- [Removing a Module](#)

**Tip**

- 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:

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



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.



359572

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:

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.



- 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

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:

```
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 CG-NMS
- Trigger Tunnel Provisioning Request to CG-NMS


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 ().

Disconnecting from the CGR 1000

After finishing your work on the CGR 1000, click  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.



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) and contains the following sections:

- [Connecting to the IR500, page 5-1](#)
- [Viewing Settings and Status, page 5-4](#)
- [Viewing Interface Details, page 5-19](#)
- [Managing the Ethernet Interface, page 5-23](#)
- [Registering with CG-NMS, page 5-23](#)
- [Rebooting the IR500, page 5-23](#)
- [Changing the Configuration, page 5-23](#)
- [Updating the Firmware Image, page 5-29](#)
- [Testing Connectivity, page 5-31](#)
- [Disconnecting from the IR500, page 5-33](#)

Connecting to the IR500

You can use Device Manager in the following ways:

- **Operating with CG-NMS**—When you have CG-NMS 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 CG-NMS, follow the steps in [Setting Up the CG-NMS Connection, page 3-5](#).
- **Operating without CG-NMS**—When you do not have CG-NMS 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 CG-NMS.



Note

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

This section covers the following topics:

- [Connecting the Laptop to the IR500](#), page 5-2
- [Connecting to the IR500 with a Work Order](#), page 5-3
- [Manually Connecting to the IR500](#), page 5-4

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 [Chapter 2, “Installation.”](#)
- You are familiar with the information in [Chapter 3, “Managing Work Orders.”](#)
- You have a valid work order if you plan on changing any IR500 settings.

To connect the laptop to the IR500:

Step 1 Attach a serial-to-USB adapter to a serial cable.



Note

The serial-to-USB adapter and serial cable are not supplied with the IR500.

Figure 5-1 Serial-to-USB Adapter Cable



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

Figure 5-2 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 CG-DM 4.1.0.

Step 5 Connect to the IR500 as described in [Connecting to the IR500 with a Work Order, page 5-3](#) or [Manually Connecting to the IR500, page 5-4](#).

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 [Chapter 3, “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**.

Manually Connecting to the IR500

To connect to the IR500 manually:

- 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 COM port or **Auto Detect**.

- 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 following subtabs of the Dashboard:

- [General Details](#)
- [MAP-T](#)
- [Network Interfaces](#)
- [Raw Sockets](#)
- [WPAN](#)

- [RPL](#)
- [Security](#)
- [DHCP](#)
- [Neighbors](#)
- [CG-NMS](#)

General Details

To view General Details:

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

The screenshot shows the Cisco Connected Grid Device Manager 4.1.0.130 interface. At the top, there is a header with navigation tabs: Dashboard, Config, Firmware, and Connectivity. Below this is a sub-tab menu with options: General Details, MAP-T, Network Interfaces, Raw Sockets, WPAN, RPL, Security, DHCP, Neighbors, and CG-NMS. The main content area is divided into two sections. On the left is a hardware diagram of the IR509U device with labels for various ports: ANT, S0, S1, USB, FED, DC+ +/- 12/24/48V, DC- 0.5 - 1.5 A, ALM REF, ALM IN, WPAN, RSSI, RSS232-DCE, RSS485-DCE, RSS232-DTE, USB, 10/100 FE, ALM, SYS, PWR, and RESET. On the right is a 'General Details' table with the following data:

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	2014-09-26 03:39:44
Report Interval	0

At the bottom of the right section, there are two buttons: 'Register with NMS' and 'Reboot'.

- Step 2** View the General Details:

- **Firmware Group Info:** The name of the firmware group that CG-NMS uses to upload and install firmware images on member devices.
- **Config Group Info:** The configuration group that CG-NMS 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 CG-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 CG-NMS every 28,800 seconds (8 hours).

MAP-T

To view MAP-T information:

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

The screenshot displays the Cisco Connected Grid Device Manager 4.1.0.130 interface. At the top, a status bar shows device details: NAME (00173B12002B003B), SERIAL (JMX1803X00M), HARDWARE ID (IR509/1.0/2.0), Model (IR509UWP-915/K9), VERSION (0.0.0), COM PORT (COM4), WORK ORDER (No Work Order), and UP TIME (28 minutes ago). Below this is a navigation menu with icons for Dashboard, Config, Firmware, and Connectivity. The main content area shows a tabbed interface with 'MAP-T' selected. Under the 'MAP-T' tab, the following information is displayed:

MAP-T	
MAP-T IPv6 Address	0:0:0:0:0:100:0
MAP-T PSID	0
Number of IPv6 to IPv4 Transactions	0
MAP-T IPv4 Address	0.0.0.1
Number of IPv4 to IPv6 Transactions	0

Step 2 View the MAP-T settings and statistics:

- MAP-T IPv6 Address: Contains the IPv6 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:

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

The screenshot shows the Cisco Connected Grid Device Manager interface. The top navigation bar includes Dashboard, Config, Firmware, and Connectivity. The main content area is titled 'Network Interfaces' and contains the following tables:

Index	Interface	IP Address	Administrative Status	Line Protocol	Tx Speed	Rx Speed
1	lo	0.0.0.1 0:0:0:0:0:0:1	✓	✓	N/A	N/A
2	lowpan		✓	✗	N/A	N/A
3	ppp	fe80:0:0:0:0:0:1	✓	✓	N/A	N/A

Route Index	Route Destination Type	Route Destination	RoutePfxLen	Route Next Hop Type	Route Next Hop	Route Interface ...	Route Type
1	2	0:0:0:0:0:100:0	128	2	4	0:0:0:0:0:0:0	4

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:

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

The screenshot shows the Cisco Connected Grid Device Manager 4.1.0.130 interface. The top navigation bar includes Dashboard, Config, Firmware, and Connectivity. The main content area is titled "Raw Sockets" and contains a table with the following data:

Session Index	Status	Uptime	Peer Address	Peer Port	Local Port	Serial Interface	Tx Bytes	Rx Bytes	Connect Attempts	Reset
0	LISTEN	0	0.0.0.0:0:0:0:0	20000	20000	serial0	0	0	0	↻
1	LISTEN	0	0.0.0.0:0:0:0:0	20000	20000	serial0	0	0	0	↻

- 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:

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

The screenshot shows the Cisco Connected Grid Device Manager interface. The top navigation bar includes 'Dashboard', 'Config', 'Firmware', and 'Connectivity'. The 'WPAN' sub-tab is selected. Below the navigation bar, there are several tabs: 'General Details', 'MAP-T', 'Network Interfaces', 'Raw Sockets', 'WPAN', 'RPL', 'Security', 'DHCP', 'Neighbors', and 'CG-NMS'. The 'WPAN Status' section displays a table with the following data:

Interface Index	SSID	PAN ID	Master	Dot1xEnabled	Security Level	Rank	Beacon Valid	Beacon Version
2	cisco	65535	No	No	1	65535	No	0

The 'WPAN Settings' section displays a table with the following data:

Interface In...	PAN ID	Short Address	Broadcast Slot Size	Broadcast Period	Neighbor Probe Rate	Back Off Timer	SSID	Mo
2	65535	0	125000	500000	300	0	cisco	0

- 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.
- Dot1xEnabled: Whether the 802.1x protocol is enabled.
- Security Level: Level of security corresponding to the protection offered.
- 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:
- Dwell: Dwell window in IEEE802.15.4g protocol.
- Notch: List of disabled channels.

RPL

To view information about RPL:

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

The screenshot shows the Cisco Connected Grid Device Manager interface for a device named 00173B12002B003B. The device details include SERIAL JMX1803X00M, HARDWARE ID IR509/1.0/2.0, Model IR509UWP-915/K9, VERSION 0.0.0, COM PORT COM4, WORK ORDER No Work Order, and UP TIME 55 minutes ago. The navigation menu includes Dashboard, Config, Firmware, and Connectivity. The RPL settings are displayed under the RPL tab.

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

Pare...	Instance Index	Route Index	IPv6 Address Local	IPv6 Address Global	Do Dag VersionNo	PathEtx	LinkEtx	RSSI Forward	RSSI R
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:

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

The screenshot displays the Cisco Connected Grid Device Manager interface. At the top, there is a header bar with navigation icons for Dashboard, Config, Firmware, and Connectivity. Below this is a sub-header with tabs for General Details, MAP-T, Network Interfaces, Raw Sockets, WPAN, RPL, Security (selected), DHCP, Neighbors, and CG-NMS. The main content area is divided into three sections: Ieee8021x Status, Ieee8021x Settings, and Ieee802.11i Status.

Ieee8021x Status

Index	Enabled	Identity	State	PMK Id	Client Cert Valid	CA Cert Valid	Private K...	Rly Pan Id	Rly Address	Rly LastHeard
2	No	host/SM1-3B...	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	0000000000000000...	0000000000000000...	0	No	0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000...	0	N/A
2	No	0000000000000000...	0000000000000000...	0	No	0000000000000000... 0000000000000000... 0000000000000000... 0000000000000000...	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:

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

The screenshot shows the Cisco Connected Grid Device Manager 4.1.0.130 interface. At the top, there is a header with device information: NAME (00173B12002B003B), SERIAL (JMX1803X00M), HARDWARE ID (IR509/1.0/2.0), Model (IR509UWP-915/K9), VERSION (0.0.0), COM PORT (COM4), WORK ORDER (No Work Order), and UP TIME (55 minutes ago). Below the header is a navigation bar with tabs for Dashboard, Config, Firmware, and Connectivity. The main content area shows the DHCP Client Status page, which includes a table with the following data:

Index	anaIAID	anaT1	anaT2
2	0	0	0

Step 2 View the DHCP Client Status:

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

Neighbors

To view 802.15.4g neighbor information:

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

Cisco Connected Grid Device Manager 4.1.0.1

NAME	00173B15002E001D	SERIAL	JAD1820015W	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.68	COM PORT	COM25	WORK ORDER	No Work Order	UP TIME	2 hours ago

Dashboard | Config | Firmware | Connectivity

General Details | MAP-T | Network Interfaces | Raw Sockets | DHCP | **Neighbors** | Security | CG-NMS

Neighbor802154G

Neighbor Index	Physical Address	Last Changed	RSSI Forward	RSSI Reverse	LQI Forward	LQI Reverse
1		332	-128	-106	255	20

- 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.

CG-NMS

To view information about CG-NMS:

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

NAME	00173B15002E001D	SERIAL	JAD182001SW	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.68	COM PORT	COM25	WORK ORDER	No Work Order	UP TIME	2 hours ago

Dashboard | Config | Firmware | Connectivity

General Details | MAP-T | Network Interfaces | Raw Sockets | DHCP | Neighbors | Security | **CG-NMS**

CGMS Notification

Code: 0

CGMS Status

Registered	NMSAddr	NMSAddrOrigin	LastReg	LastRegReason	NextReg	NMSCertValid
No	0:0:0:0:0:0:0:0	0	2 hours ago	1		Yes

CGMS Stats

SigOk	SigBadA...	SigBadValidity	SigNo Sync	Reg Succeed	RegAttempts	RegHolds	RegFails	NmsErrors
0	0	0	0	0	0	0	0	0

Signature Cert

CertSubj	CertValidNotBefore	CertValidNotAfter	CertFingerprint
SSM_CSMP	Jul 22 2014	Jul 21 2044	[B@710c1593

Signature Settings

ReqSign...	ReqV...	ReqTimeS...	ReqSecLo...	ReqSignedResp	ReqValidCh...	ReqTimeSyncResp	ReqSecLocalResp	Cert
No	No	No	No	No	No	No	No	

353555

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.

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:

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

The screenshot shows the Cisco Connected Grid Device Manager interface. At the top, a metadata table provides the following information:

NAME	00173B1200470027	SERIAL	JAD1820016S	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.71	COM PORT	COM4	WORK ORDER	No Work Order	UP TIME	2 days ago

The main navigation bar includes Dashboard, Config, Firmware, and Connectivity. The 'General Details' tab is active, showing a physical diagram of the IR509U device. A context menu is open over the FE0 port, with the following options:

- Bring Up
- Shut Down
- Reset
- View Details

To the right of the diagram, a 'General Details' table lists the following information:

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	2014-10-13 16:07:57
Report Interval	0

At the bottom of the interface, there are two buttons: 'Register with NMS' and 'Reboot'.

The View Details window displays the Ethernet metrics.

Metrics		eth
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):

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

Viewing Interface Details

The screenshot shows the Cisco Connected Grid Device Manager interface. At the top, there is a header with device information: NAME (0017381200470027), SERIAL (JAD1820016S), HARDWARE ID (IR509/1.0/2.0), Model (IR509UWP-915/K9), VERSION (5.5.71), COM PORT (COM4), WORK ORDER (No Work Order), and UP TIME (2 days ago). Below the header is a navigation bar with icons for Dashboard, Config, Firmware, and Connectivity. The main content area is divided into several tabs: General Details, MAP-T, Network Interfaces, Raw Sockets, WPAN, RPL, Security, DHCP, Neighbors, and CG-NMS. The General Details tab is active, showing a diagram of the IR509U device with various ports and indicators labeled. A 'View Details' button is overlaid on the diagram, pointing to the S0/S1 network interface. To the right of the diagram is a 'General Details' table with the following data:

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	2014-10-13 16:09:03
Report Interval	0

Below the table are two buttons: 'Register with NMS' and 'Reboot'. The diagram on the left shows the following components: ANT, S0, S1, USB, FE0, DC+ +/- 12/24/48V, DC- 0.5 - 1.5 A, ALM REF, ALM IN, WPAN, RSSI, RSS232-DCE, RSS485-DCE, RSS232-DTE, USB, 10/100 FE, ALM, SYS, PWR, and RESET.

The View Details window displays the DCE or DTE metrics.

The screenshot shows the 'View Details' window with the 'Serial Dev Metrics' section selected. The metrics are displayed for 'DCE' mode. The metrics and their values are:

Serial Dev Metrics	
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:

-
- 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 CG-NMS

When you connect to the IR500 with a work order, the IR500 registers with CG-NMS. Registration notifies CG-NMS 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 CG-NMS for load balancing or delegation to specific sites. In this case, CG-NMS redirects the IR500 to re-register with an alternate CG-NMS.

To register with CG-NMS, on the Device Manager main page (Dashboard), click **Register with NMS**. 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:

- General Settings such as Report interval, Config Group Info and NAT44 settings
- MAP-T settings
- Serial Interface 0 settings (DCE)
- Serial Interface 1 settings (DTE)

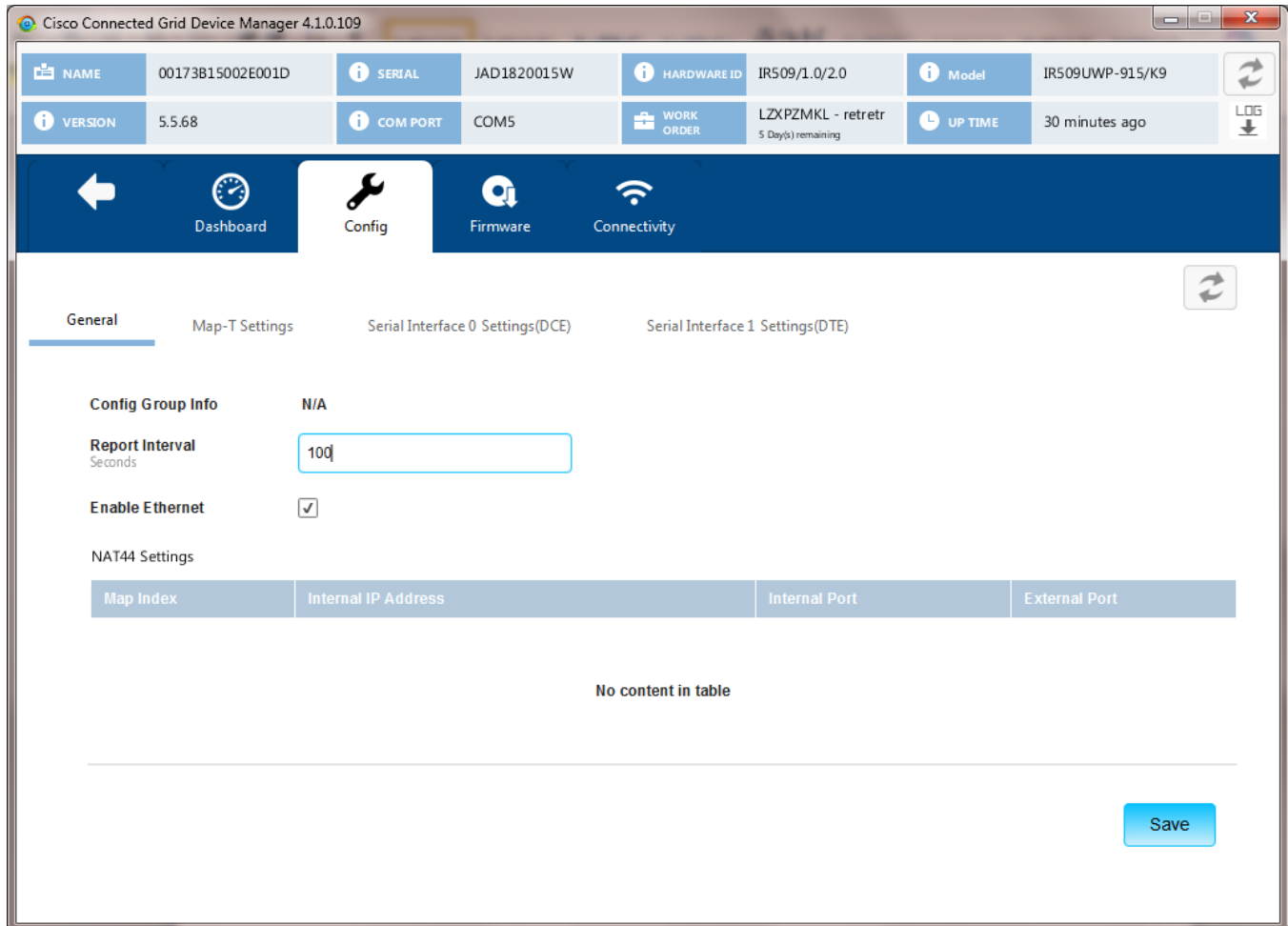
**Note**

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:

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



Step 2 View or modify General settings:

- **Config Group Info:** The configuration group that CG-NMS 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 CG-NMS 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.

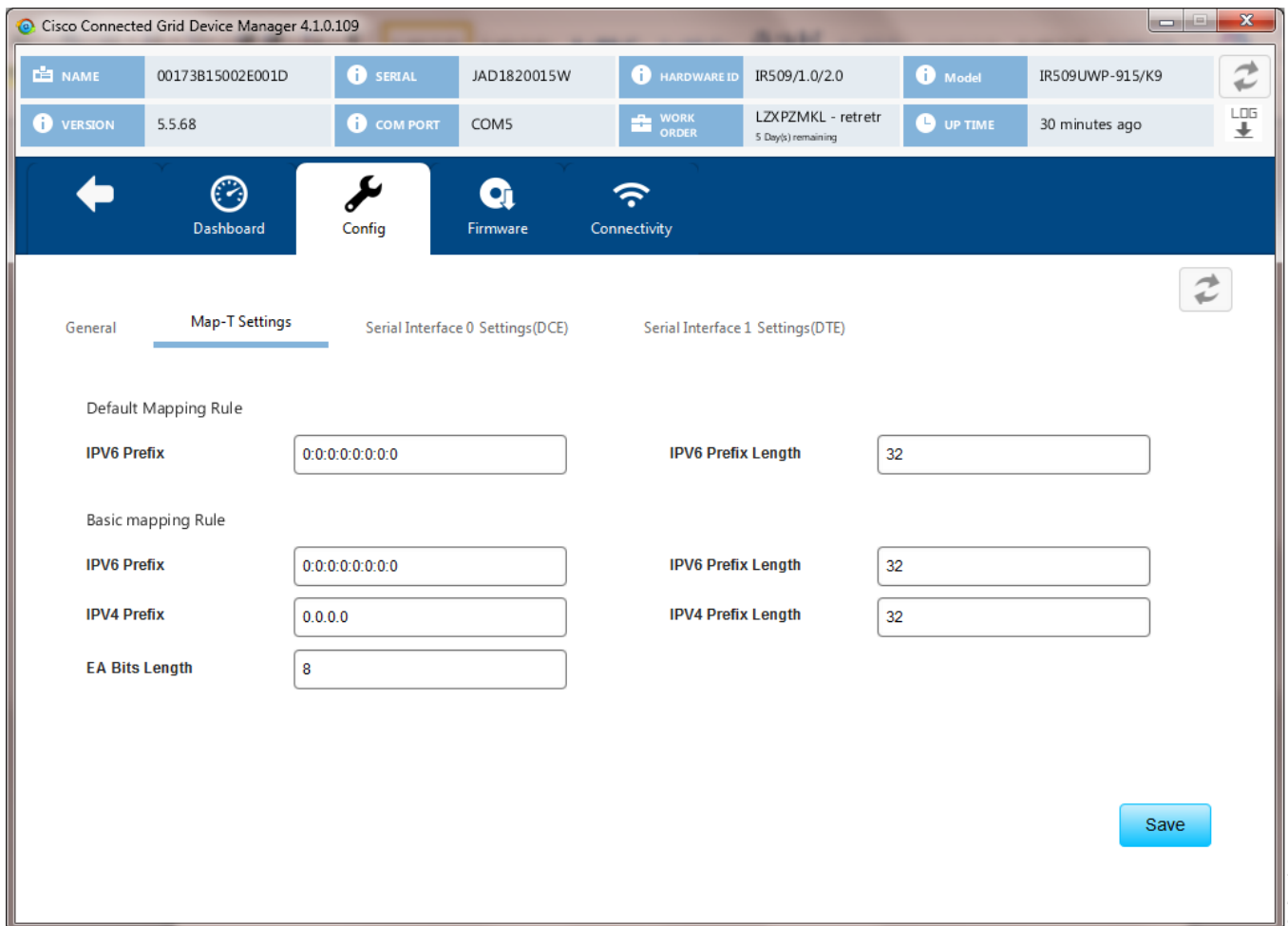
- External Port: The external port number of the NAT 44 configured device.

Step 3 Click **Save**.

Changing MAP-T Settings

To view or change MAP-T configuration settings:

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



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):

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

Cisco Connected Grid Device Manager 4.1.0.109

NAME	00173B15002E001D	SERIAL	JAD1820015W	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.68	COM PORT	COM5	WORK ORDER	LZXPMKL - retrer 5 Day(s) remaining	UP TIME	30 minutes ago

Dashboard | Config | Firmware | Connectivity

General | Map-T Settings | **Serial Interface 0 Settings(DCE)** | Serial Interface 1 Settings(DTE)

Media Type: RS232

Data Bits: 8

Parity: Odd

Flow Control: None

Baud Rate: 115200

Stop Bit: 4

TCP Raw Socket Sessions

TCP Idle Time Out	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Le...	Packet Timert(...)	Special Character	Initiator
0	0	2001:a:b:c:0:0:face	20000	20000	512	500	0	No

Save

353652

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):

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

Cisco Connected Grid Device Manager 4.1.0.109

NAME	00173B15002E001D	SERIAL	JAD1820015W	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.68	COM PORT	COM5	WORK ORDER	LZXPZMKL - retrertr 5 Day(s) remaining	UP TIME	30 minutes ago

Dashboard | **Config** | Firmware | Connectivity

General | Map-T Settings | Serial Interface 0 Settings(DCE) | **Serial Interface 1 Settings(DTE)**

Media Type: RS232

Data Bits: 8

Parity: Odd

Flow Control: None

Baud Rate: 115200

Stop Bit: 4

TCP Raw Socket Sessions

TCP Idle Time ...	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Length	Packet Timer(ms)	Special Character	Initiator
0	0	2001:a:b:c:0:0:0:face	20001	20001	512	500	0	No

Save

- 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**.
-

Updating the Firmware Image

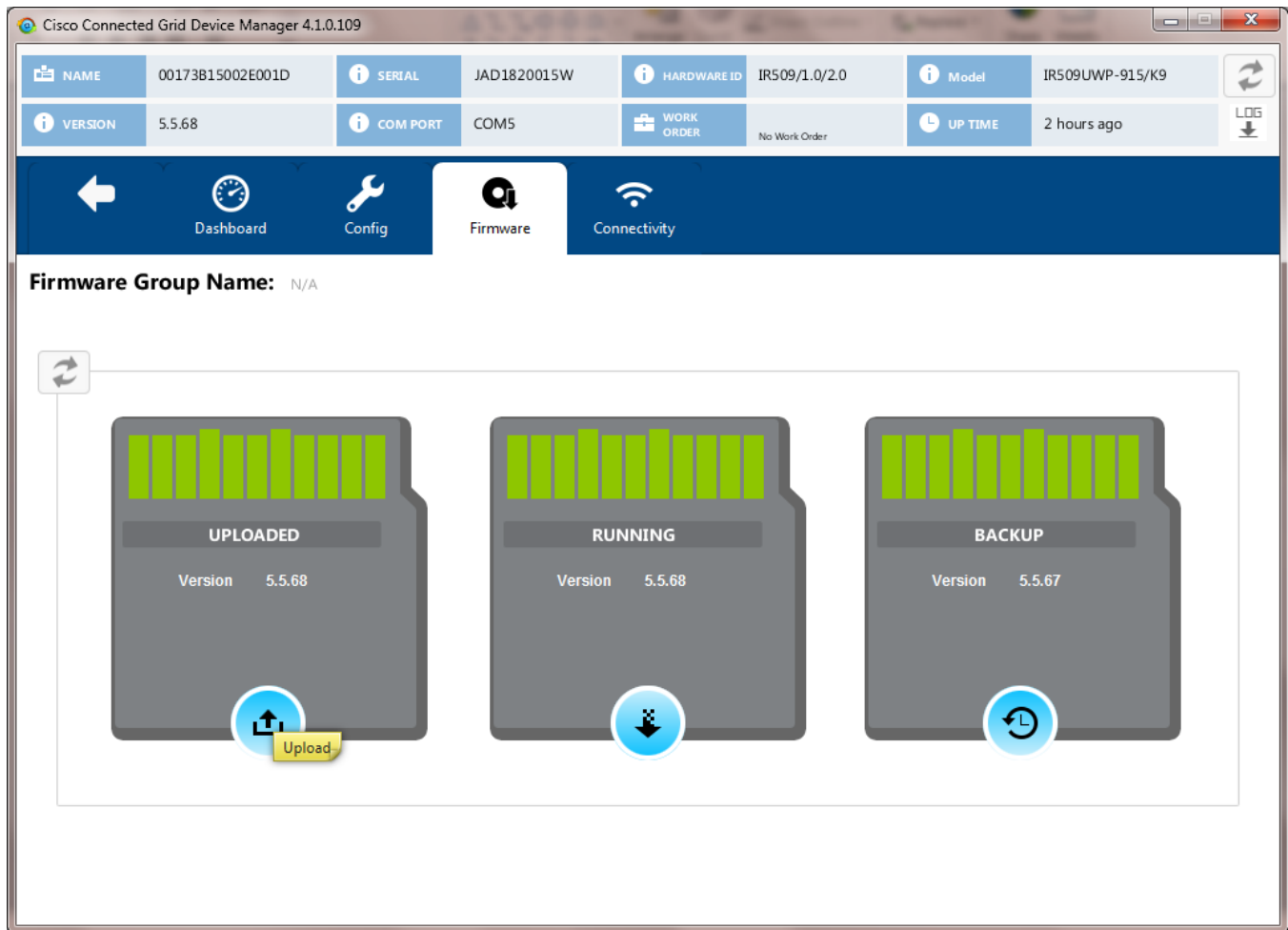
Use the Firmware page to perform these tasks:

- [Uploading an Image, page 5-29](#)
- [Installing an Image, page 5-30](#)
- [Setting the Backup, page 5-31](#)

Uploading an Image

To upload an image to the IR500:

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



- 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](#).)
- 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:

- 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:

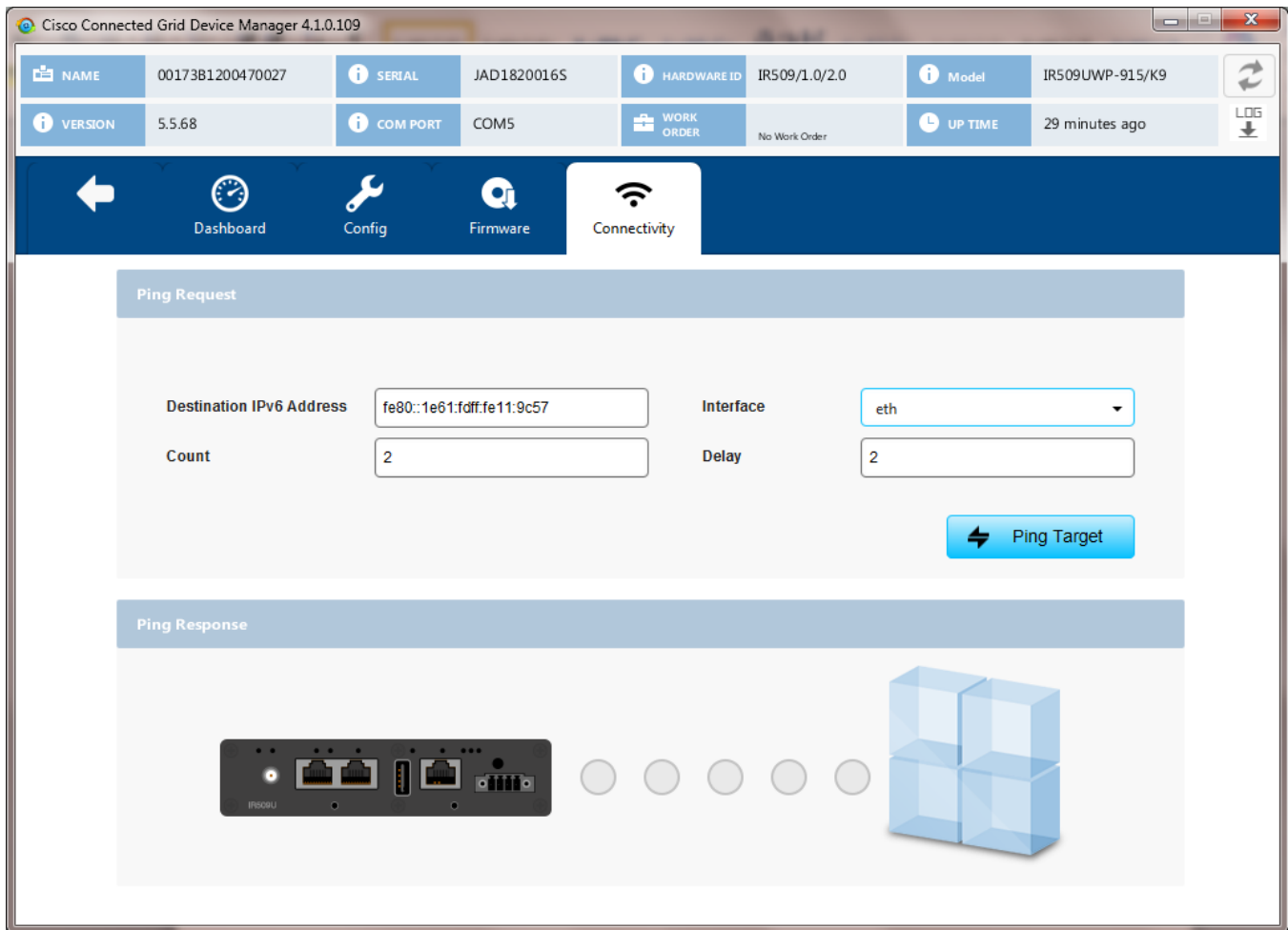
-
- Step 1** On the Device Manager main page, click the **Firmware** tab.
- Step 2** On the right of the Firmware page, click the Set Backup icon.
- Step 3** In the dialog box that appears, click **Yes**.
-

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:

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



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.

Disconnecting from the IR500

After finishing your work on the CGR 1000, click  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.

