



## **Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1**

August 2016

### **Cisco Systems, Inc.**

[www.cisco.com](http://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](http://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](http://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)

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.

© 2016 Cisco Systems, Inc. All rights reserved.



---

**CHAPTER 1**

<b>Introduction</b>	<b>1-1</b>
Overview	1-1
Application	1-1
Tasks	1-2
Certificates	1-4
Role-based Access Control	1-4
Work Authorization	1-4
Additional Information	1-5

---

**CHAPTER 2**

<b>Installation</b>	<b>2-1</b>
Required Expertise	2-1
System Requirements	2-1
Certificate Installation	2-1
Device Manager Installation	2-2
Device Manager Removal	2-3

---

**CHAPTER 3**

<b>Using the Device Manager</b>	<b>3-1</b>
Overview	3-1
How to Use the Device Manager	3-2
Connect to the CGR 1000	3-3
Setting Operating Mode	3-5
Accessing Work Authorizations	3-9
Enabling Feature on Router	3-10
Downloading Work Authorizations	3-10
Viewing Work Details	3-11
Updating Work Details	3-11
Performing Tasks on the Router	3-11
Test Connectivity	3-12
Add a Device IP Address	3-13
Ping a Device IP Address	3-14
Trace Route a Device IP Address	3-16
Remove a Device IP Address	3-17
Manage Interfaces	3-17

- Bring Up an Interface 3-18
- Shut Down an Interface 3-19
- View Details for an Interface 3-20
- Reload a Module 3-22
- Change Configuration 3-22
  - Add a Configuration File 3-23
  - Update Configuration 3-24
  - Correct a Configuration File 3-25
  - Remove Configuration File 3-25
- Update Image 3-25
  - Upload Image 3-26
  - Replace Image 3-27
  - Remove Image 3-27
- Retrieve Report 3-27
  - Retrieve and Save Reports 3-28
- Manage Modules 3-28
  - Add a Module 3-29
  - Remove a Module 3-31
- Advanced Command 3-33
- Import Certificates 3-35
- Disconnect from the CGR 1000 3-35
- Connection Override 3-36
- Example Log File Output 3-36
- Feature History 3-41

**CHAPTER 4**

**Troubleshooting 4-1**

- Certificate Errors 4-1
- Connection Errors 4-2



# Introduction

---

This chapter provides an overview of the Cisco Connected Grid Device Manager (Device Manager) and includes the following sections:

- [Overview, page 1-1](#)
- [Additional Information, page 1-5](#)

## Overview

This section includes the following topics:

- [Application](#)
- [Tasks](#)
- [Certificates](#)
- [Role-based Access Control](#)
- [Work Authorization](#)

## Application

Cisco Connected Grid Device Manager (Device Manager) is a Windows-based application that field technicians can use to manage the Cisco 1000 Series Connected Grid Routers (CGR 1000) over WiFi or Ethernet.

Cisco Connected Grid Network Management System (Cisco CG-NMS) manages multiple CGR 1000 routers, whereas the Device Manager connects and manages a single CGR 1000 at a time.

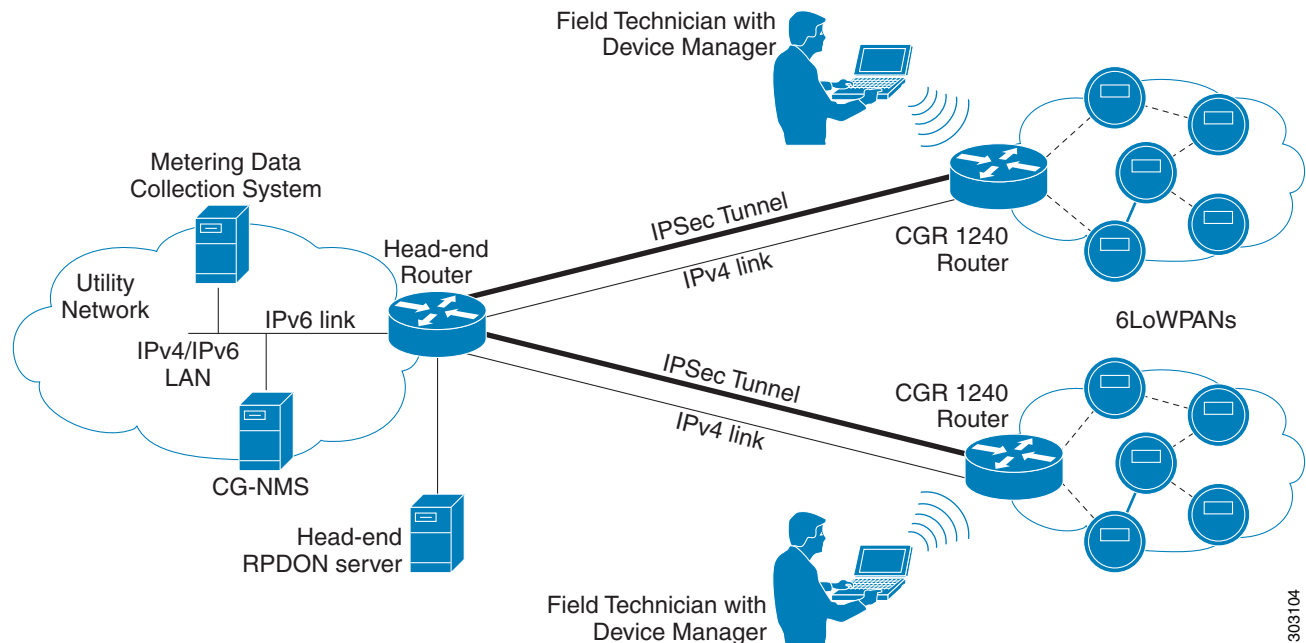
The Device Manager can operate in Connected Grid field deployments operating with or without CG-NMS.

- When operating with CG-NMS (NMS mode), a Device Manager user can retrieve Work Authorizations from the system as well as perform all supported tasks on the At a Glance page (see [Figure 1-2](#)) except as limited by the users assigned roles. (See [Role-based Access Control](#).)
- When operating without CG-NMS (non-NMS mode), the Device Manager user does not have access to Work Authorizations; however, the user can perform all supported tasks on the At a Glance page except as limited by the user's assigned roles.

CGR 1000 routers are multi-service communications platforms designed for use in field area networks. 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.

The 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



303104

## Tasks

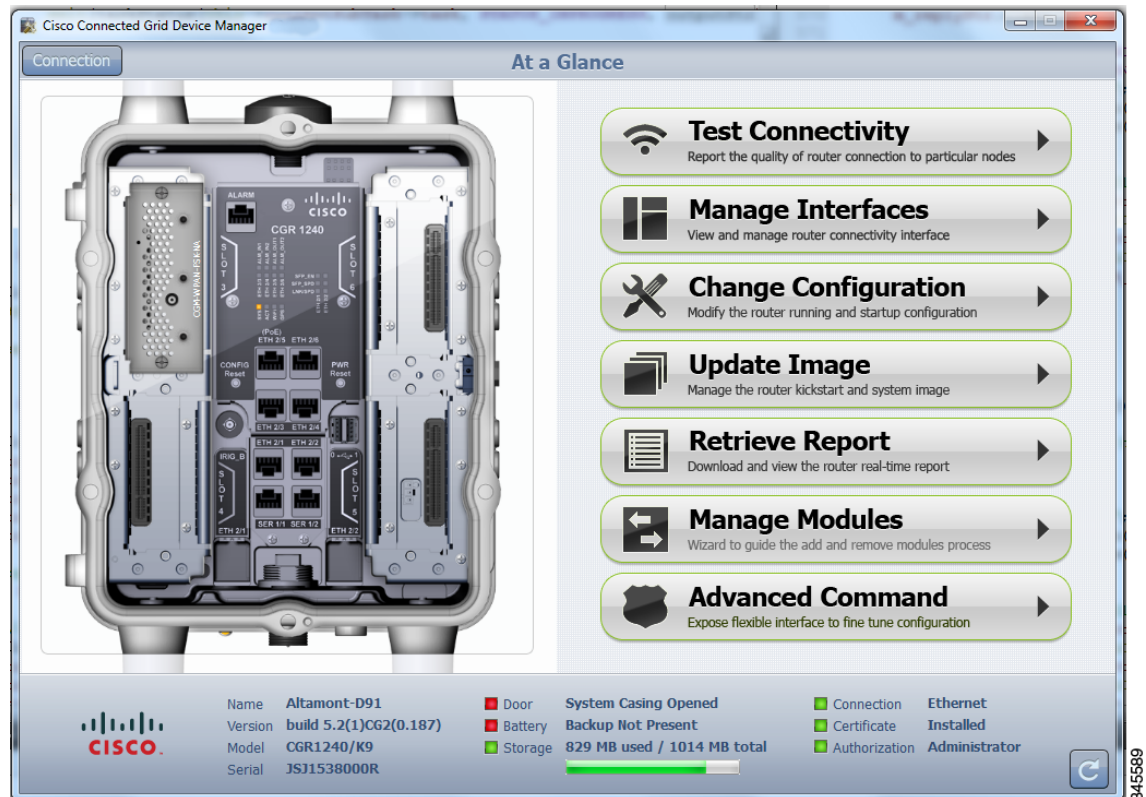
The Device Manager enables you to:

- Troubleshoot connectivity between a CGR 1000 and the devices connected to the router. (See [Test Connectivity](#), page 3-12.)
- Bring up or shut down an CGR 1000 interface. (See [Manage Interfaces](#), page 3-17.)
- Check and update the current CGR 1000 configuration. (See [Change Configuration](#), page 3-22 and [Advanced Command](#), page 3-33.)
- Update the CGR 1000 image on the router. (See [Update Image](#), page 3-25.)
- View real-time CGR 1000 configuration log for troubleshooting. (See [Retrieve Report](#), page 3-27.)
- Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. (See [Manage Modules](#), page 3-28.)
- Use advanced commands to troubleshoot the CGR 1000.

(See [Advanced Command](#), page 3-33.)

You initiate all tasks from the At a Glance page. (See [Figure 1-2](#).)

**Figure 1-2** At a Glance Page for the CGR 1240



In addition to supported tasks (right side), the At a Glance page provides a view of the CGR 1000 router to which the Device Manager is connected (left side).

At the bottom of the page, you can find the following information:

- Name of the router
- Version of the software
- Model number of the CGR 1000
- Serial number of the CGR 1000
- Door status of the system casing, (Opened or Closed) for the router (CGR 1240 only)
- Battery status, when an optional backup battery is installed (CGR 1240 only)
- Slots within the system and modules installed in those slots (CGR 1120 only)
- Storage status, including amount of storage available
- Connection method of the Device Manager to the CGR 1000 (WiFi or Ethernet)
- Certificate status
- Authorization indicates the user role of the connected user

**Tip**

To refresh the At a Glance page, click the **Refresh** icon (lower right side).

## Certificates

You can import certificates through the Device Manager by employing the Setup wizard or by command line. The application launches the Setup wizard when either the user clicks the Setup icon or when the certificate is not detected. (See [Import Certificates](#).)

## Role-based Access Control

As a user, you are assigned roles that manage your access to operational and management functions of the Device Manager, which are summarized on the At a Glance page.

The Device Manager displays or restricts access to tasks based on your assigned role:

- When operating in non-NMS mode, the Device Manager supports four roles (admin, tech, viewer, and upload image). The assigned certificate extension Object ID (OID) manages roles and user access. Your administrator defines certificate extension OIDs for Device Manager roles on the Certificate Authority (CA) server.
  - Admin–User can perform all the supported tasks.
  - Technician–User can perform the following tasks: Test connectivity, manage interfaces, update image, retrieve reports, and manage modules.
  - Viewer–User can perform the following tasks: Test connectivity using predefined targets, view status of interfaces, and retrieve reports.
  - Upload Image–User can perform the following task: Upload an image to the CGR 1000.
- When operating in NMS mode, the Device Manager supports three roles (admin, tech, and viewer). The role that the CG-NMS administrator assigns to a [Work Authorization](#) manages user access.
  - Admin–User can perform all the supported tasks.
  - Technician–User can perform the following tasks: Test connectivity, manage interfaces, update image, retrieve reports, and manage modules.
  - Viewer–User can perform the following tasks: Test connectivity using predefined targets, view status of interfaces, and retrieve reports.

**Note**

In NMS mode, user roles defined in CG-NMS take precedence over certificate-defined roles. For example, if you run Device Manager in non-NMS mode and then start Device Manager in NMS mode, the roles used in non-NMS mode are removed and the roles defined in CG-NMS take effect.

## Work Authorization

The Work Authorization page is the opening page of the Device Manager when configured to operate in NMS mode. On this page, you can view and select work authorizations for CGR 1000 routers and synchronize with the Cisco CG-NMS to download work authorizations. The Device Manager only needs to be connected to CG-NMS to download and update the work authorizations.



At the CG-NMS, an admin assigns a user role for each of these work authorizations. (See [Role-based Access Control](#).)

**Tip**

---

You must enable Command Authorization on the CGR 1000 to support this functionality on the Device Manager. (See [Enabling Feature on Router](#).)

---

## Additional Information

You can find configuration guides and release notes for Cisco 1000 Series Connected Grid products at: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)





## Installation

---

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

- [Required Expertise, page 2-1](#)
- [System Requirements, page 2-1](#)
- [Certificate Installation, page 2-1](#)
- [Device Manager Installation, page 2-2](#)
- [Device Manager Removal, page 2-3](#)

## Required Expertise

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

## System Requirements

The Device Manager has the following system requirements:

- 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

## Certificate Installation

You can import certificates through the Device Manager by employing the Setup wizard or by command line. (See [Import Certificates, page 3-35](#).)

When the Device Manager cannot locate a valid Certificate Common Name in the registry, the Device Manager launches the Settings page to import a certificate.

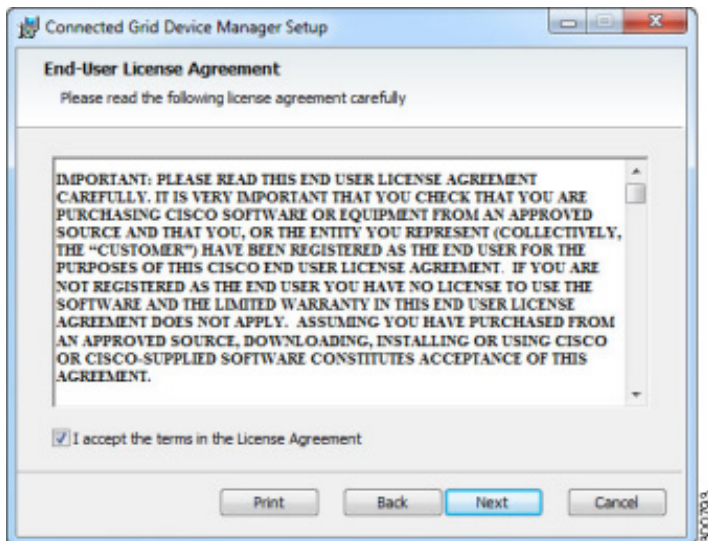
## Device Manager Installation

Follow these steps to install the Device Manager:

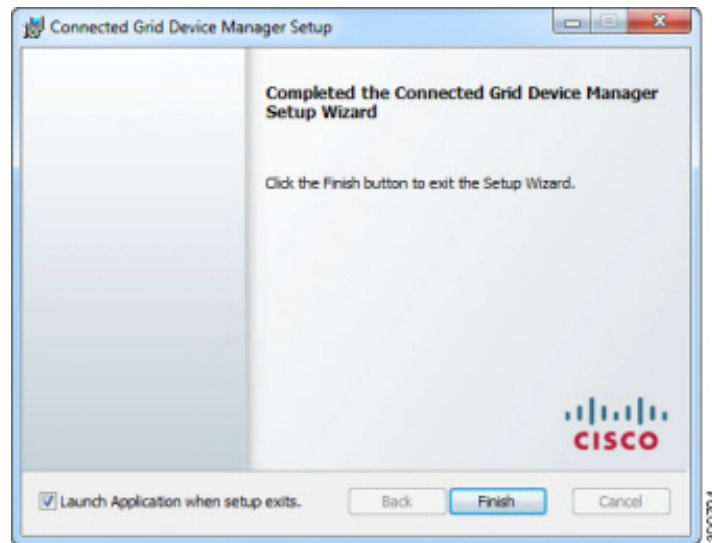
- Step 1** Double-click the CGDManager executable to start installation.
- Step 2** Click **Next**.



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



- Step 4** Click **Finish** to exit the Setup Wizard and launch the Device Manager.



When the Device Manager cannot locate a valid Certificate Common Name in the registry, the Device Manager launches the Settings page to import a certificate.

---

## Device Manager Removal

To remove the Device Manager application, click **Start > All Programs > Cisco CGD Manager > Uninstall Cisco CGD Manager**, or use Add or Remove Programs from the Control Panel.





## Using the Device Manager

---

The chapter explains how to use the Device Manager and contains the following sections:

- [Overview, page 3-1](#)
- [How to Use the Device Manager, page 3-2](#)
- [Connect to the CGR 1000, page 3-3](#)
- [Setting Operating Mode, page 3-5](#)
- [Accessing Work Authorizations, page 3-9](#)
- [Performing Tasks on the Router, page 3-11](#)
- [Import Certificates, page 3-35](#)
- [Disconnect from the CGR 1000, page 3-35](#)
- [Connection Override, page 3-36](#)
- [Example Log File Output, page 3-36](#)
- [Feature History, page 3-41](#)

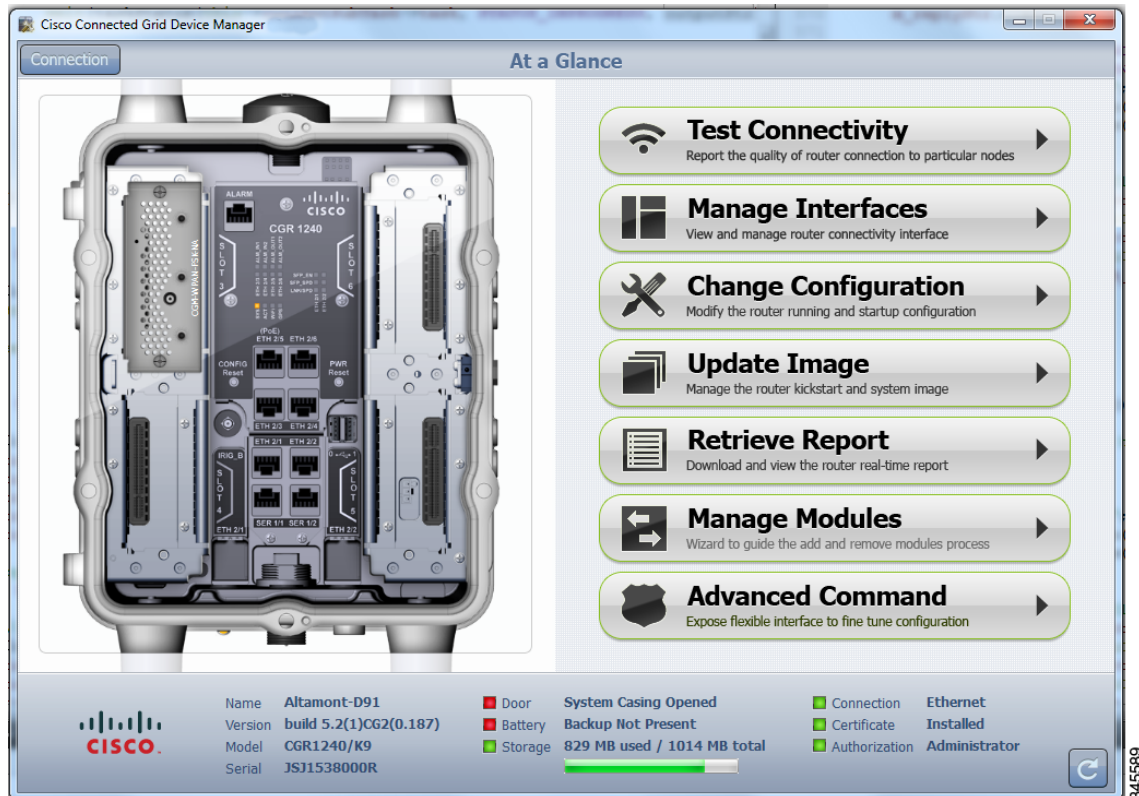
### Overview

Device Manager displays the At a Glance page after securely connecting to the CGR 1000. From this page, you can perform the following tasks as determined by your assigned role. (See [Role-based Access Control, page 1-4.](#))

- **Test Connectivity:** Verify access to a device (IP address) from the CGR 1000 by using ping to check link connectivity and quality, and initiate a traceroute for an inaccessible IP address. (See [Test Connectivity, page 3-12.](#))
- **Manage Interfaces:** Bring up or shut down an CGR 1000 interface, view details for an interface, and reload a module. (See [Manage Interfaces, page 3-17.](#))
- **Change Configuration:** Update the CGR 1000 configuration with a provided configuration file, and then reboot the router with the new configuration. (See [Change Configuration, page 3-22.](#))
- **Update Image:** Upload a copy of a software image onto the CGR 1000 for immediate installation or for a deferred update of the image. (See [Update Image, page 3-25.](#))
- **Retrieve Report:** Download and view the CGR 1000 system logs. (See [Retrieve Report, page 3-27.](#))
- **Manage Modules:** Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. (See [Manage Modules, page 3-28.](#))

- **Advanced Command:** Provides a console-like interface to troubleshoot the CGR 1000 by using CLI commands. 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 [Advanced Command](#), page 3-33.)

Figure 3-1 At a Glance Page for the CGR 1240



The CGR 1000 image that appears on the left side of the At a Glance page provides a view of the CGR 1000 router to which the Device Manager connects. The CGR 1000 image also displays the Connected Grid Modules installed, as well as LEDs that indicate if the modules are operating. You can also view interfaces, available module slots, and other information. The information can be refreshed at any time by clicking the Refresh icon, located on the bottom right-hand corner of the page.

## How to Use the Device Manager

Following are a few examples of how to use the Device Manager:

- Devices connected to a CGR 1000 cannot be reached. Start the Device Manager, connect to the router, and then check connectivity to the device. (See [Test Connectivity](#), page 3-12.)
  - When you reconnect to the devices, review the CGR 1000 configuration information. (See [Advanced Command](#), page 3-33.)



- When the configuration information is incorrect, you can update the configuration (see [Update Configuration, page 3-24](#)) by adding a configuration file to the Device Manager and then updating the CGR 1000 configuration. After you update the configuration (see [Advanced Command, page 3-33](#)) the router automatically resets and restarts with the new configuration.
- A software image update must be uploaded and installed on the CGR 1000. Start the Device Manager, upload the new image file, and then update the router with the new image. The router automatically restarts after you update the software image. (See [Update Image, page 3-25](#).)
- Newly deployed CGR 1000s do not appear in the back-end system. Start the Device Manager and review the router graphic on the At a Glance page. Check the installed modules and their LEDs to verify their operation. When the LEDs are not flashing, check the installation status of the modules. Refer to the configuration guide for the module. (See [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs).)
- (CGR 1240 Only) The door of the CGR 1240 is open. Start the Device Manager and check the status of the door (bottom of the At a Glance page). When the door status indicates a status of *System Casing Open*, you must physically access the CGR 1240 to verify the status of the door. After closing the door, click the Refresh icon (bottom right) on the Device Manager and verify that the door status displays *System Casing Closed*.
- A WiMAX module is being added to a CGR 1240. Start the Device Manager and navigate to the **At a Glance > Manage Module** page. (See [Manage Modules, page 3-28](#).)
- 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), you can use the information on the WiMAX Module Activity page 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. (See [View Details for an Interface, page 3-20](#).)
- A WiMAX module needs to be reloaded in the event of a hardware failure, hang or crash. (See [Reload a Module, page 3-22](#).)

## Connect to the CGR 1000

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

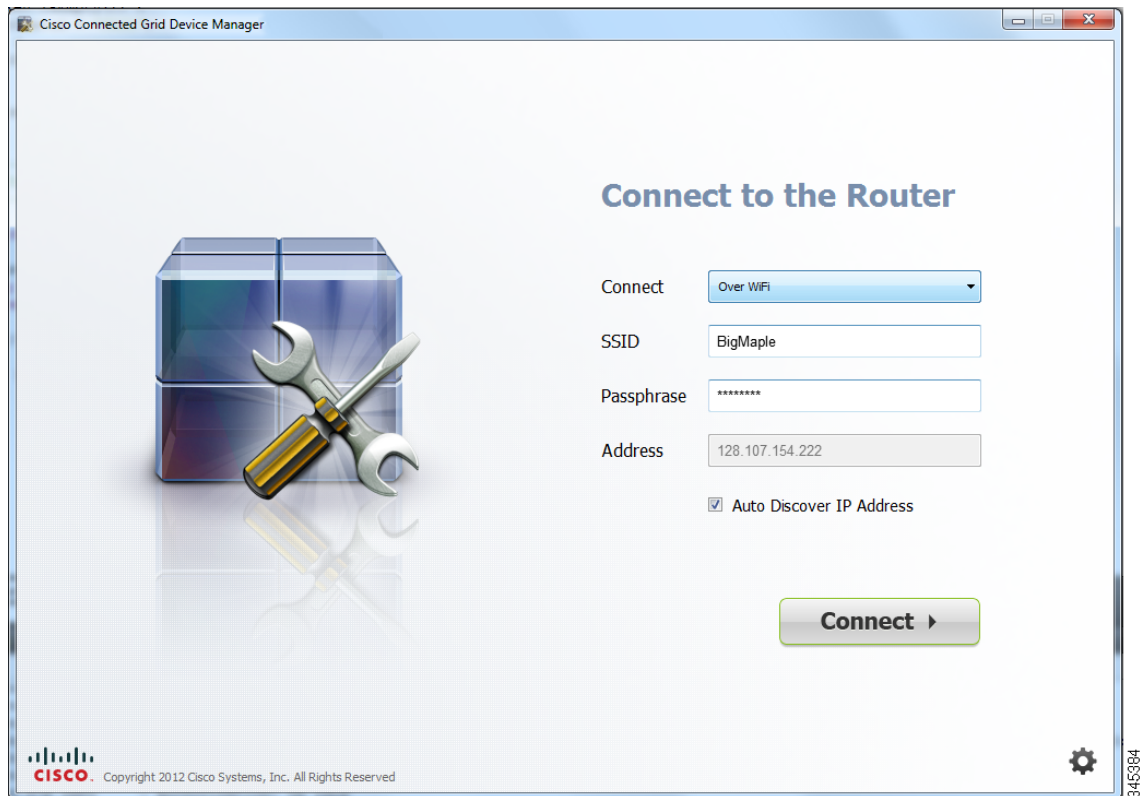
Connect to the Device Manager by employing one of the following methods:

- 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)

Follow these steps to start the Device Manager:

- 
- Step 1** After installing the Device Manager on your laptop, double-click on the **Cisco CGD Manager** icon on your Desktop, or select **Start > All Programs > Cisco CGD Manager**.

The application opens the Connect to the Router page.



- Step 2** On the Connect to the Router page, select the connection method: Ethernet, WiFi, Auto Detect.
- (WiFi only) Enter the SSID and Passphrase.
  - Enter the router IP address, or select the checkbox 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 3** On the Connect to the Router page, do one of the following:
- To set or modify the operating mode (non-NMS or NMS mode) of the Device Manager, click the Settings icon on the bottom-right of the Router page. Non-NMS is the default setting. The Setup Wizard appears. Proceed to [Setting Operating Mode](#).
  - To connect to the router to query the router details (after you set the operating mode), click either **Connect** (non-NMS mode) or **Connect to the Router** (NMS mode). The At a Glance page appears. Proceed to [Performing Tasks on the Router](#).



**Tip** If you have problems connecting to the Device Manager, refer to [Chapter 4, “Troubleshooting”](#) for troubleshooting suggestions.

# Setting Operating Mode

The operating mode of the Device Manager determines what tasks you can access and view from the Device Manager and how it interacts with systems within the Connected Grid network field deployment. (See [Performing Tasks on the Router](#).)

You can configure the Device Manager to operate in one of the following modes:

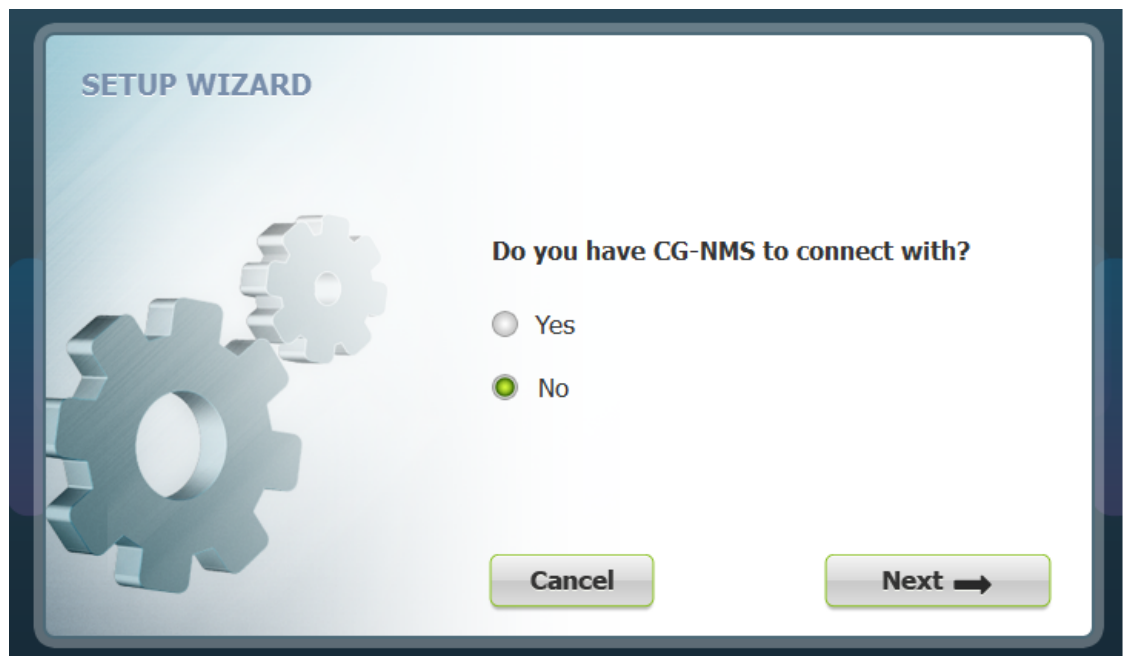
**NMS Mode**—When you have a CG-NMS operating in the network, you can connect to that system with the Device Manager to download and update work authorizations. Work authorizations allow the Device Manager to view status and perform tasks on the CGR 1000. To operate in conjunction with a CG-NMS system, configure the Device Manager to operate in NMS-mode.

**Non-NMS Mode**—When you do not have a CG-NMS operating in the network or do not want to connect to that system, configure the Device Manager to operate in non-NMS mode. In this case, you 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.

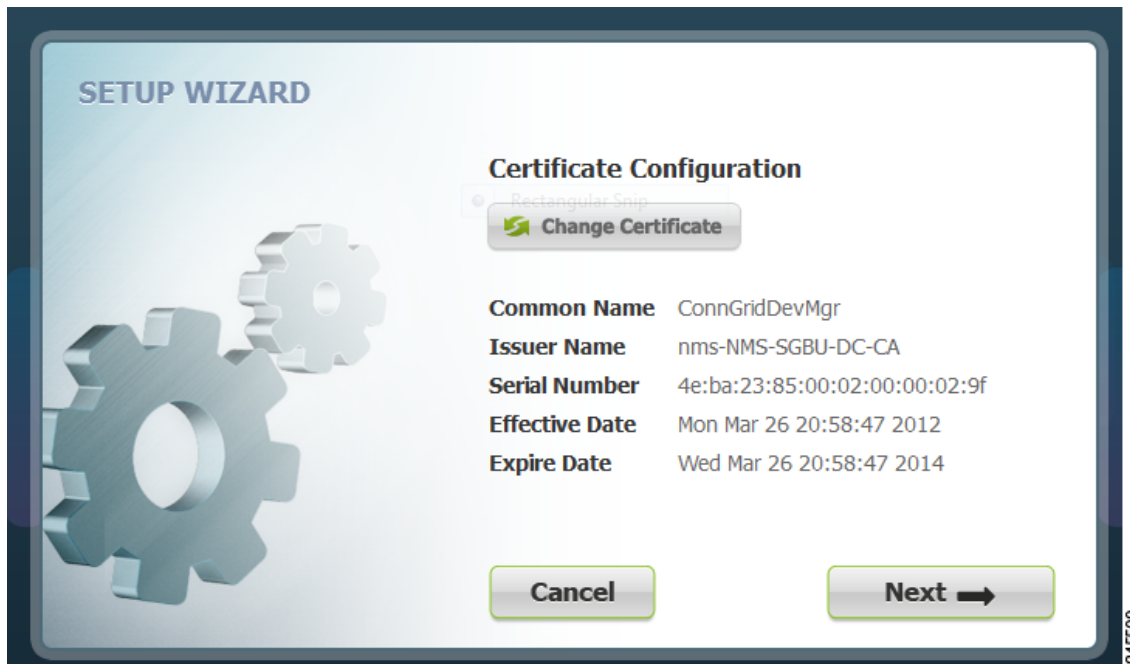
Follow these steps to configure the Device Manager operating mode:

**Step 1** On the Setup Wizard page, select one of the following options:

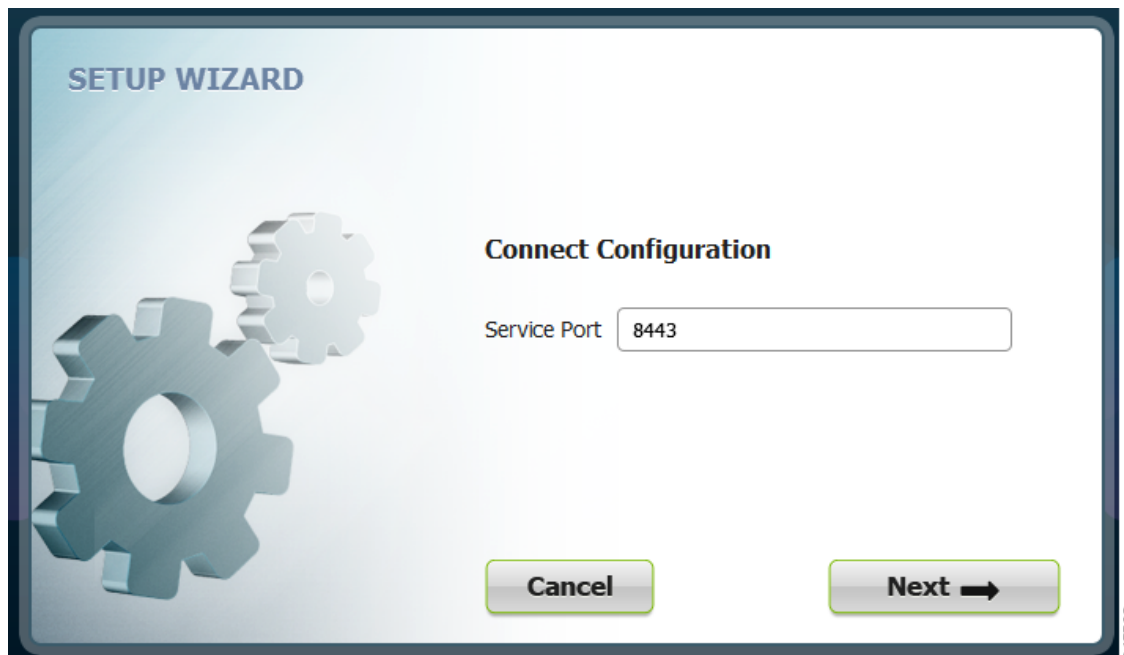
- To have the Device Manager connect to the Router only (non-NMS mode), select the **No** radio button, and then click **Next**. Proceed to [Step 2](#).
- To have the Device Manager operate in conjunction with a CG-NMS system (NMS mode), select the **Yes** radio button, and then click **Next**. Proceed to [Step 3](#).



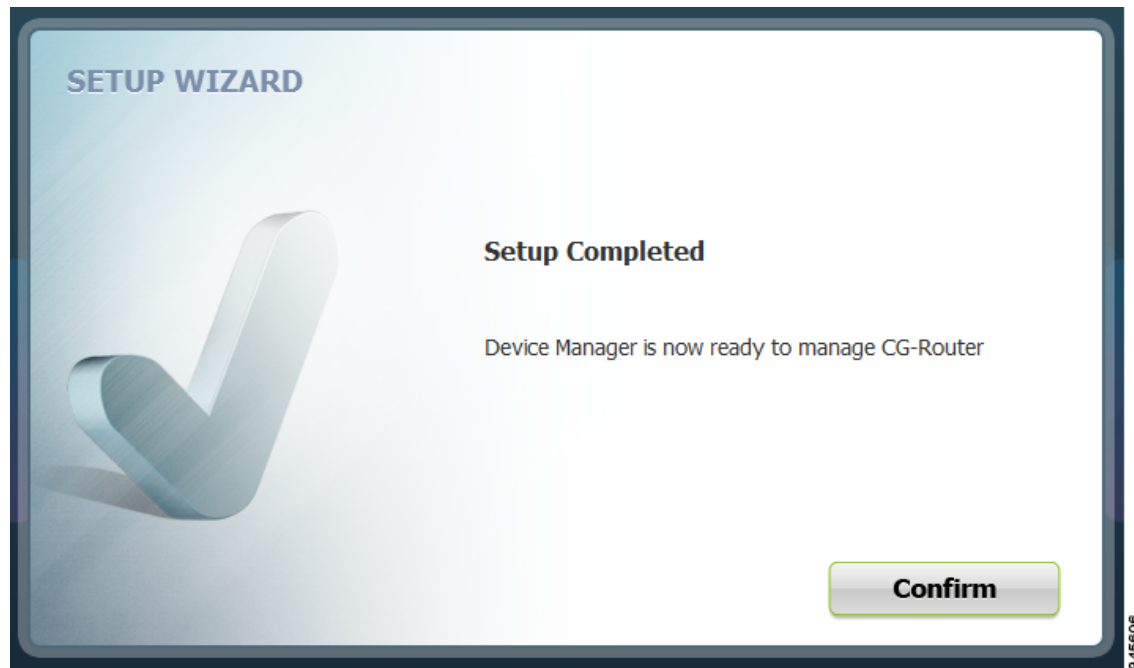
**Step 2** (Non-NMS mode) On the Certificate Configuration page, review the Common Name and the certificate details for accuracy and do the following:



- To accept the current certificate, click **Next**. Proceed to [b](#).
- To select a different certificate, click **Change Certificate**. Proceed to [Import Certificates](#).
- To exit the Setup Wizard, click **Cancel**.



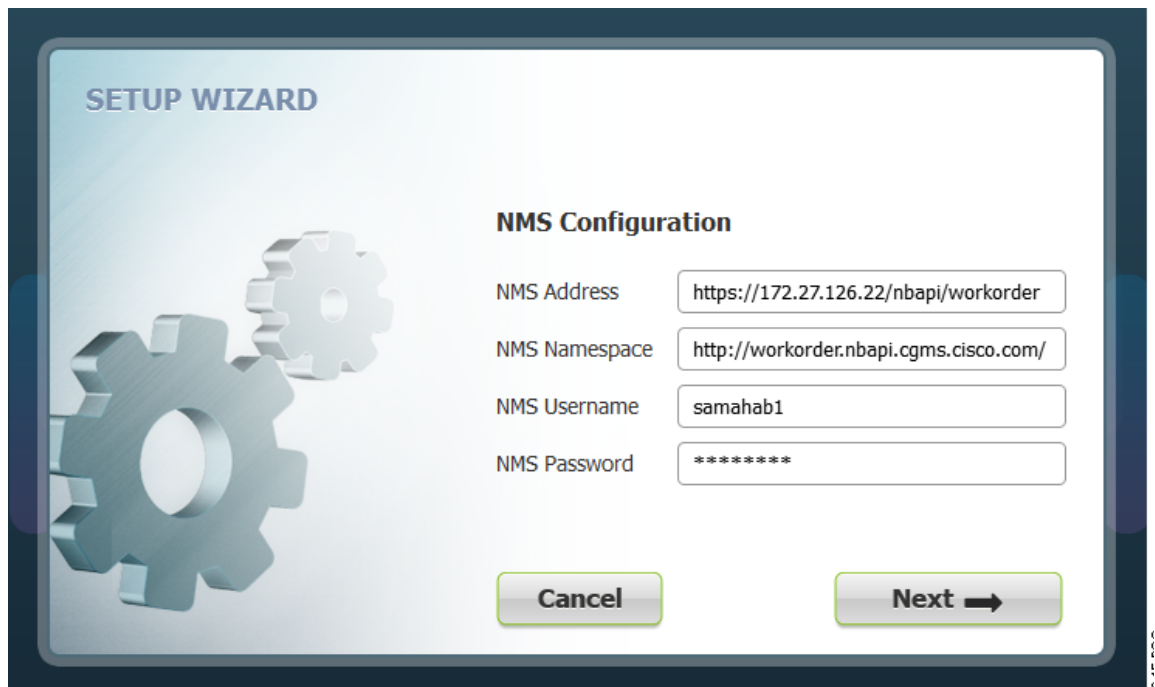
- On the Connect Configuration page, confirm the Service Port and click **Next**.
- On the Setup Completed page, click **Confirm**.



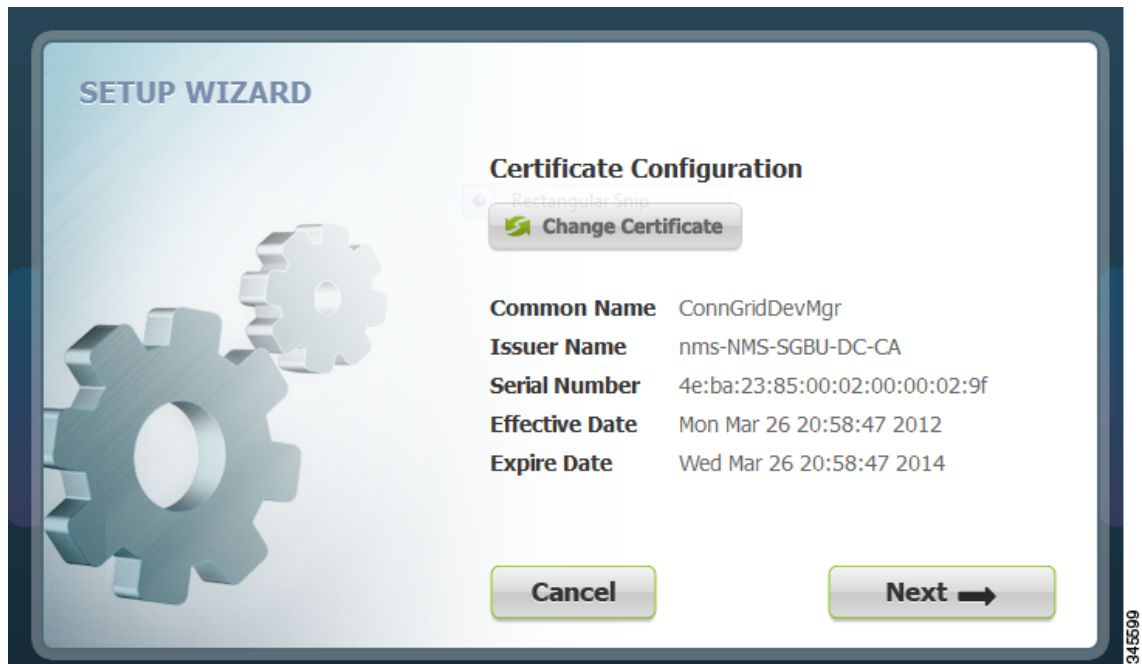
- c. On the Connect to the Router page that appears, click **Connect**.

The At a Glance page appears. Proceed to [Performing Tasks on the Router](#).

- Step 3** (CG-NMS mode) On the NMS Configuration page, do the following:

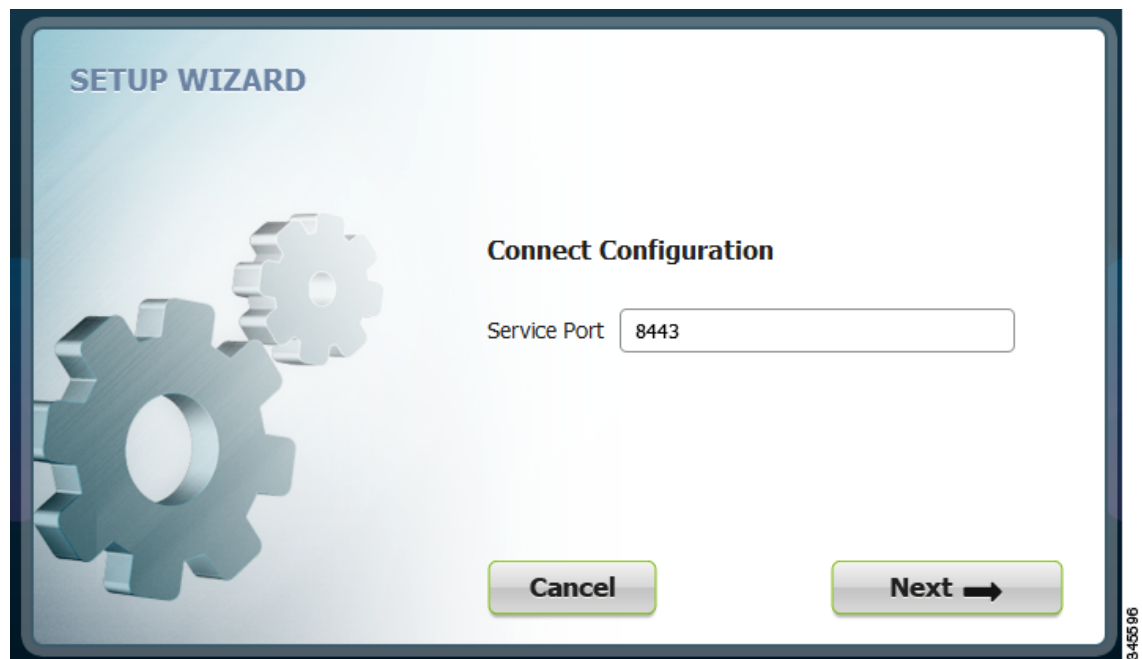


- a. Enter the NMS address (IP address), NMS Namespace, NMS Username and NMS Password for the CG-NMS application server, and then click **Next**.
- b. On the Certificate Configuration page, review the certificate details, and do one of the following:

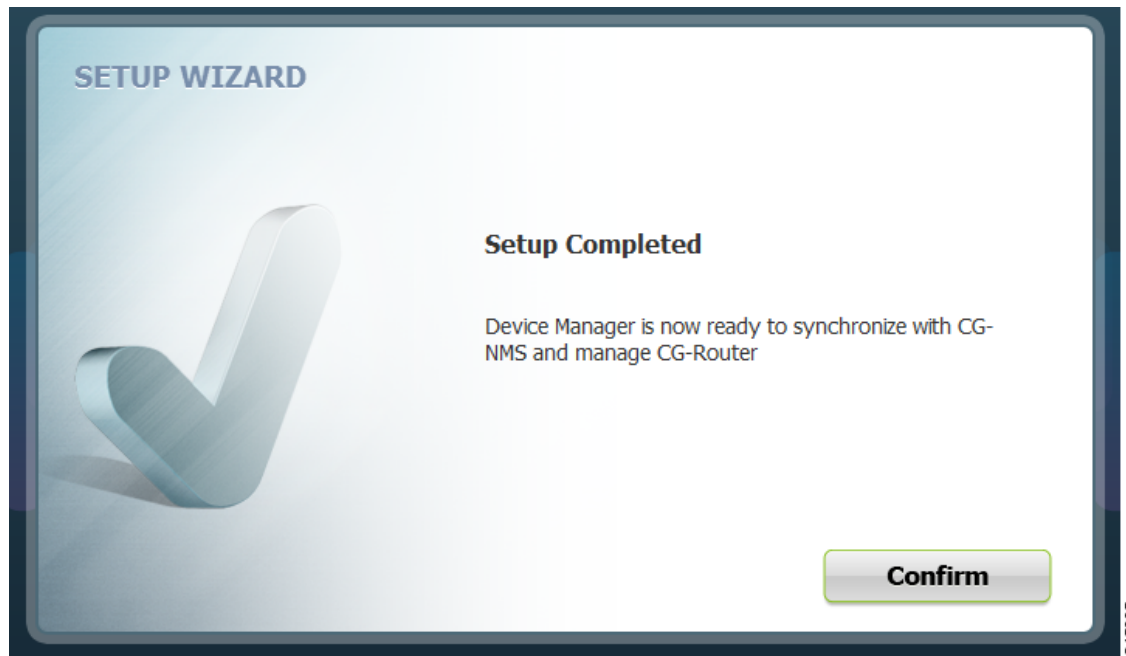


- To accept the current certificate, click **Next**. Proceed to [c](#).
- To select a different certificate, click **Change Certificate**. Proceed to [Import Certificates](#).
- To exit the Setup Wizard, click **Cancel**.

**c.** On the Connect Configuration page, confirm the Service Port and click **Next**.



**d.** On the Setup Completed page, click **Confirm**.



- e. On the Work Authorization page that appears, click **Confirm**. Proceed to [Accessing Work Authorizations](#).

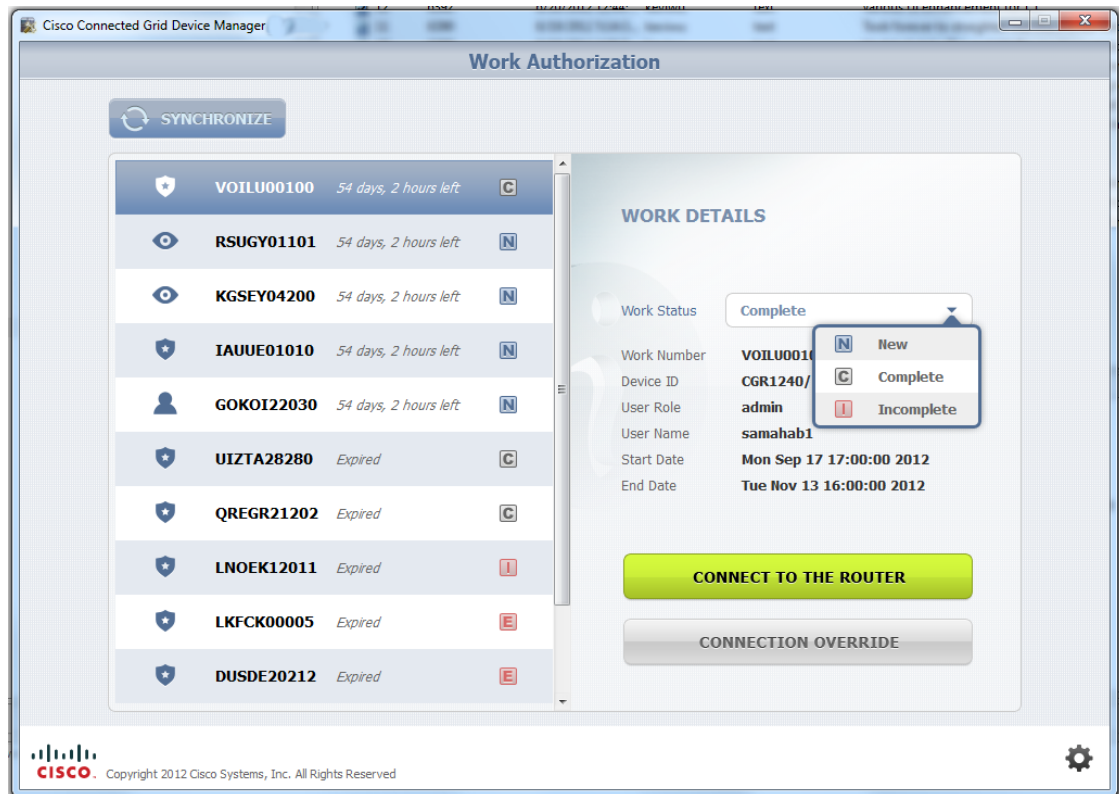
## Accessing Work Authorizations

The Device Manager must be operating in the NMS mode for you to view and download work orders from the CG-NMS to the Work Authorization page. (See [Setting Operating Mode](#).)

The Work Authorization page is the opening page of the Device Manager when operating in NMS mode.

Whenever work or direct inspection of a CGR 1000 is necessary by a field technician, an admin generates a work order on the CG-NMS. Work orders include encrypted WiFi credentials necessary for the technician to connect to the router. In most cases, a work order requires a user with an assigned user role of technician (tech) to access and update the work order. However, a user with a viewer role can retrieve status on a CGR 1000 but not perform tasks on the router.

Each work order has an expected start and end date, which is noted in the Work Details summary (right pane) along with user role and user name and the current state of the work order: New (N), Complete (C), Incomplete (I), or Expired (E).



This section covers the following topics:

- [Enabling Feature on Router](#)
- [Downloading Work Authorizations](#)
- [Viewing Work Details](#)
- [Updating Work Details](#)



Tip

To perform additional tasks on the router, click **Connect to the Router** on the Work Authorization page to launch the At a Glance page. (See [Performing Tasks on the Router](#).)

## Enabling Feature on Router

The following commands must be entered on the CGR 1000 to support communication between the Device Manager and the router when Work Authorization is in use:

```
router# configure terminal
router (config)# cgdm
router (config-cgdm)# command authorization enable
```

## Downloading Work Authorizations

To download the latest work orders from CG-NMS and upload new status of the work orders to CG-NMS, click **Synchronize** on the Work Authorization page.



## Viewing Work Details

The Work Number in the Work Details section (right pane) 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 the 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.

To view work order details, do the following:

- 
- Step 1** On the Work Authorization page, click a work order (left pane).
- Step 2** Using the Work Number that appears (left pane), 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 Work Status drop-down menu.
  - When you are not able to complete the work order, select **Incomplete** from the Work Status drop-down menu.
- The work order (left pane) reflects the status change.
- Step 3** When connected to CG-NMS, click **Synchronize** to update the CG-NMS.
- After synchronization with the CG-NMS, all Completed, Incomplete, and Expired work orders are removed from the Device Manager display.
- 

## Updating Work Details

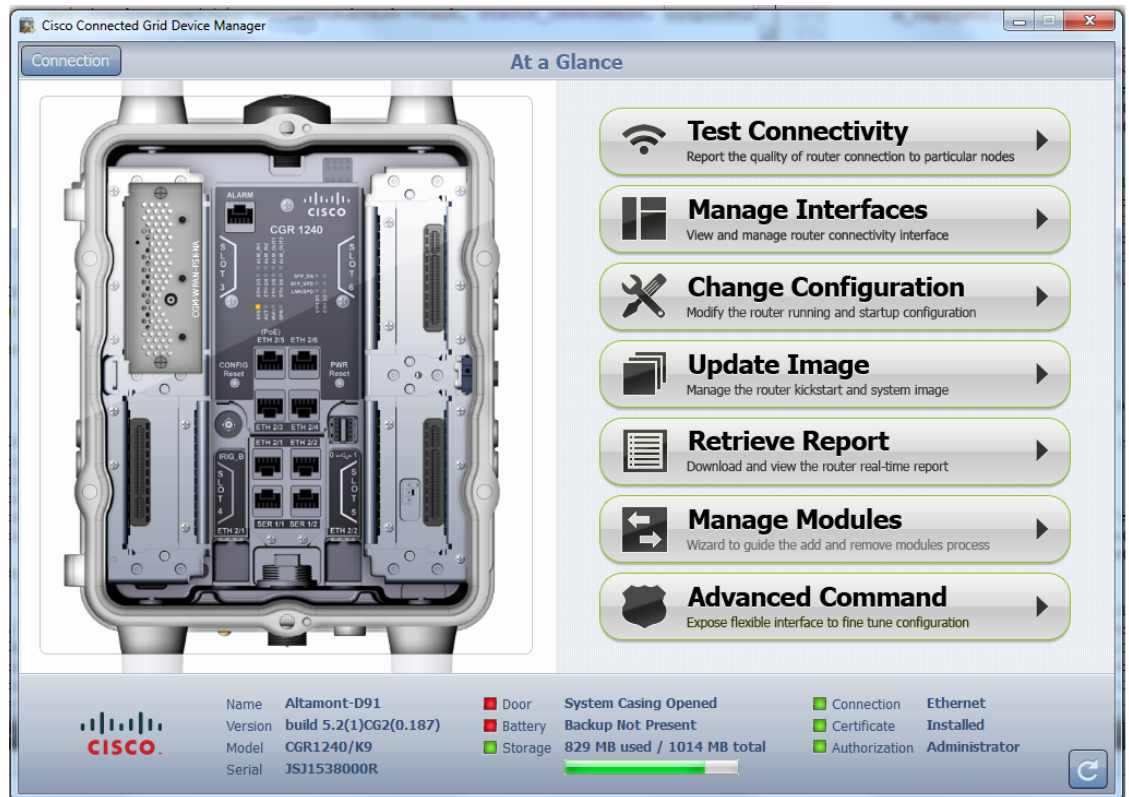
A work order has four possible states: New (N), Complete (C), Incomplete (I), or Expired (E).

To update the status of a work order, do the following:

- 
- Step 1** On the Work Authorization page, select the Work Status drop-down menu (right pane).
- Step 2** Select the current state of the work order.
- The Work Authorization page reflects the new state of the work order (left pane).
- Step 3** To update the CG-NMS database with this change, click **Synchronize**.
- 

## Performing Tasks on the Router

The At a Glance page appears after you click **Connect** from the Connect to the Router page (Non-NMS mode) or click **Connect to the Router** from the Work Authorization page (NMS mode).



Listed below are all the possible tasks that a user can perform. However, your assigned role determines which tasks you can access. The Device Manager displays or restricts tasks based on your assigned role (or roles). The above At a Glance view represents an Admin role. (See [Role-based Access Control](#).)

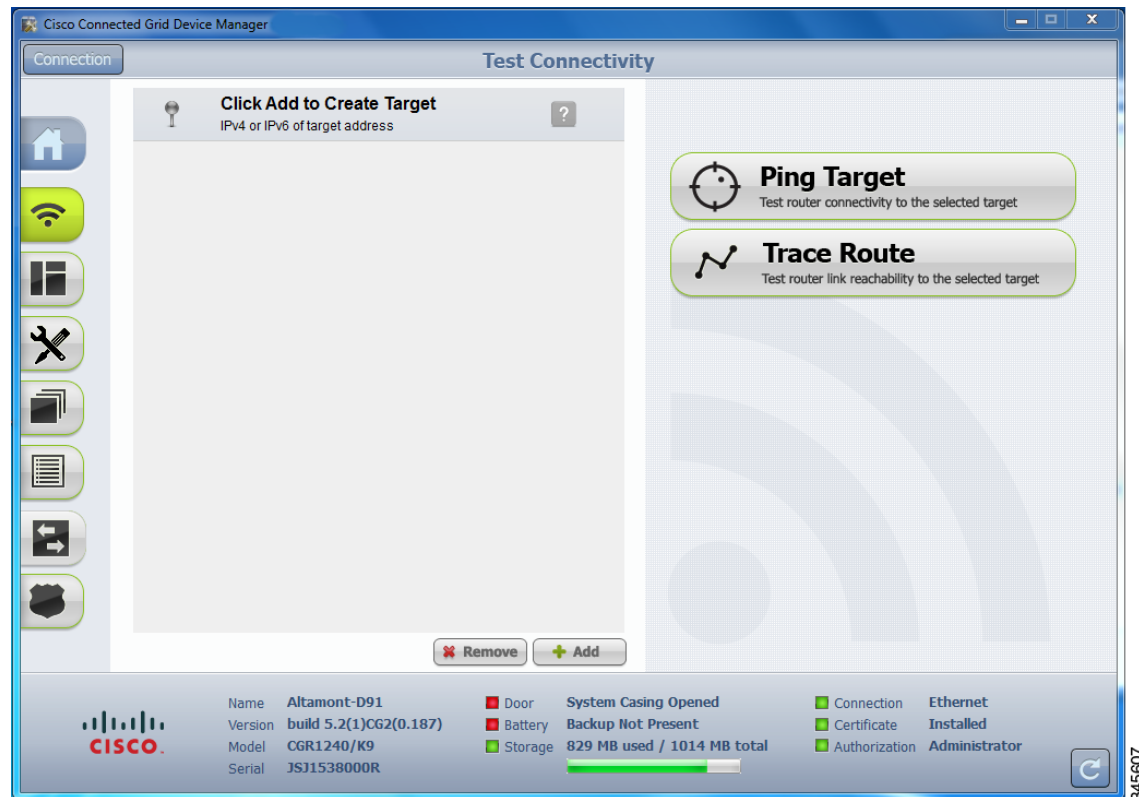
- Troubleshoot connectivity between a CGR 1000 and the devices connected to the router. (See [Test Connectivity](#), page 3-12.)
- Bring up or shut down a CGR 1000 interface. (See [Manage Interfaces](#), page 3-17.)
- Check and update the current CGR 1000 configuration. (See [Change Configuration](#), page 3-22 and [Advanced Command](#), page 3-33.)
- Upload and/or update the CGR 1000 image and reset the router. (See [Update Image](#), page 3-25.)
- View real-time CGR 1000 configuration log for troubleshooting. (See [Retrieve Report](#), page 3-27.)
- Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. (See [Manage Modules](#), page 3-28.)
- View module activity and reload a module (See [View Details for an Interface](#), page 3-20 and [Reload a Module](#), page 3-22.)
- Use advanced commands to troubleshoot the CGR 1000. (See [Advanced Command](#), page 3-33.)

## Test Connectivity

The Test Connectivity task allows you to confirm connectivity to a device from the CGR 1000.

**Tip**

Before you can check a device connection or route to a CGR 1000, you must add the IPv4 or IPv6 address of the device to the Device Manager.



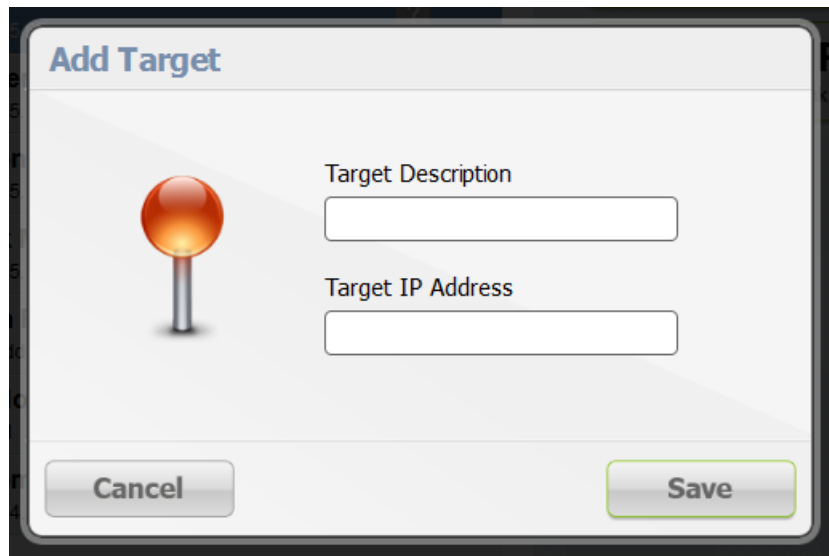
This section covers the following topics:

- [Add a Device IP Address](#)
- [Ping a Device IP Address](#)
- [Trace Route a Device IP Address](#)
- [Remove a Device IP Address](#)

## Add a Device IP Address

Follow these steps to add a device IP address:

- Step 1** From the At a Glance page, click **Test Connectivity**.  
The Test Connectivity page displays the defined sample devices and/or target addresses.
- Step 2** Click **Add** to create a target IP address.

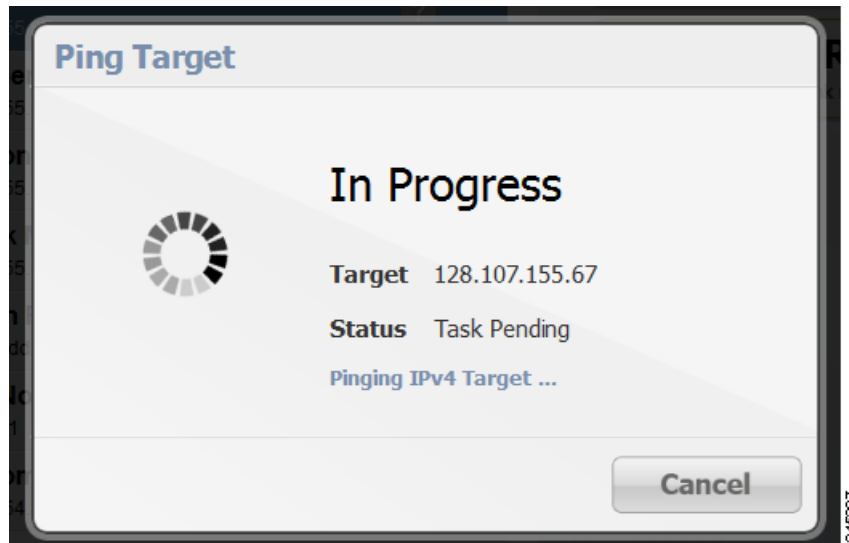


- Step 3** In the Target Description field, enter a description for the device.
- Step 4** In the Target IP Address field, enter the IP address (IPv4 or IPv6) of the device.
- Step 5** Click **OK**.
- You can now test the connectivity to the device you just added to the Device Manager.
- 

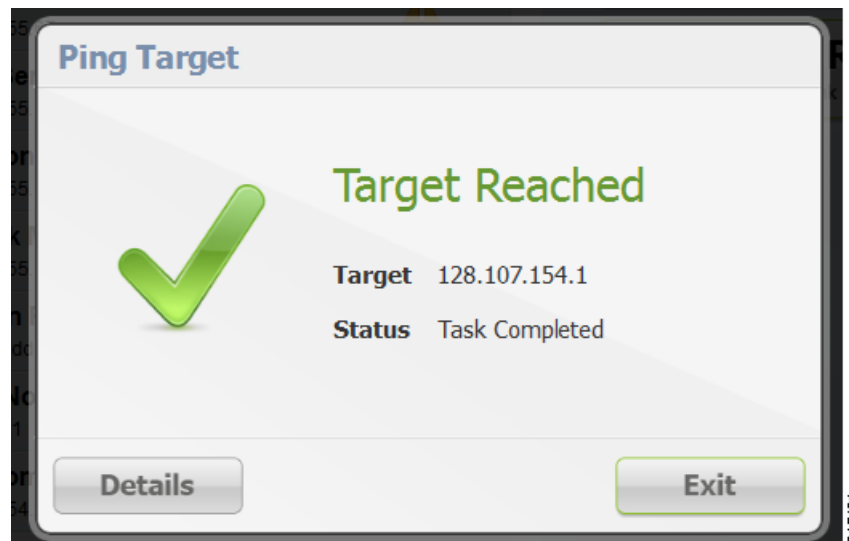
## Ping a Device IP Address

The Ping feature allows you to verify connectivity to a device by querying the target IP address. Follow these steps to test connectivity between the CGR 1000 and the device:

- Step 1** On the Test Connectivity page, click on a target IP address from the listing on the page (left pane).
- Step 2** Click **Ping Target**.
- The In Progress dialog box appears.



When the system successfully pings the device, the Target Reached dialog box appears. If the system does not successfully ping a device, refer to [Failed Ping, page 3-15](#).

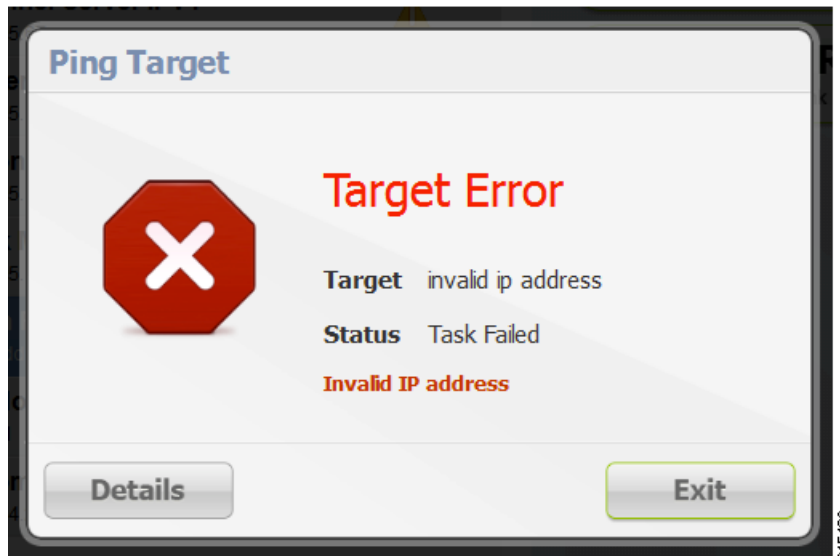
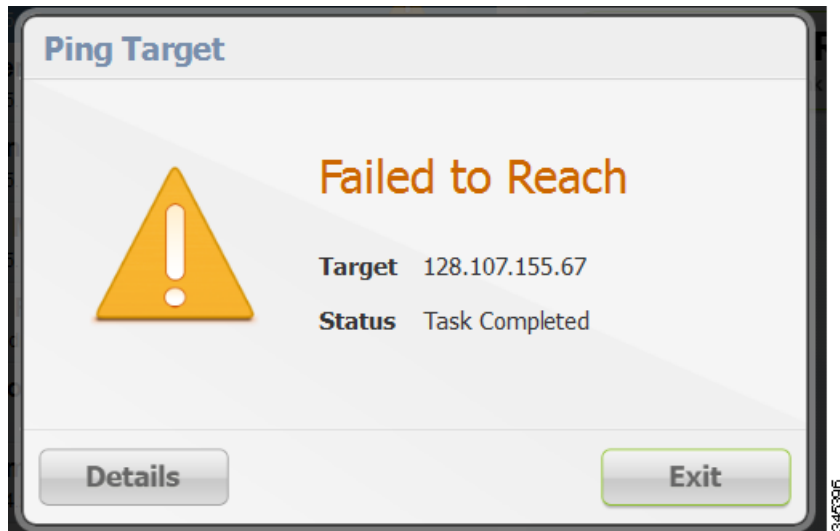


**Step 3** Click **Details** to view details or click **Exit** to close the window.

## Failed Ping

Follow these steps if the ping of the target IP address is unsuccessful:

**Step 1** In the Failed to Reach dialog box, click **Details** to view the reason the system could not reach the IP address.



- Step 2** In the Target Error dialog box, click **Exit** after reviewing the reason for the error. Proceed to [Trace Route a Device IP Address, page 3-16](#).

## Trace Route 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.

Follow these steps to trace the route of the IP address:

- Step 1** On the Test Connectivity page, select the device IP address from the list.
- Step 2** Click **Trace Route**:

- If the trace route is successful, click **Exit** in the Trace Route dialog box.
  - If the trace route is unsuccessful, proceed to [Remove a Device IP Address, page 3-17](#).
- 

## Remove a Device IP Address

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

Follow these steps to remove a target IP address:

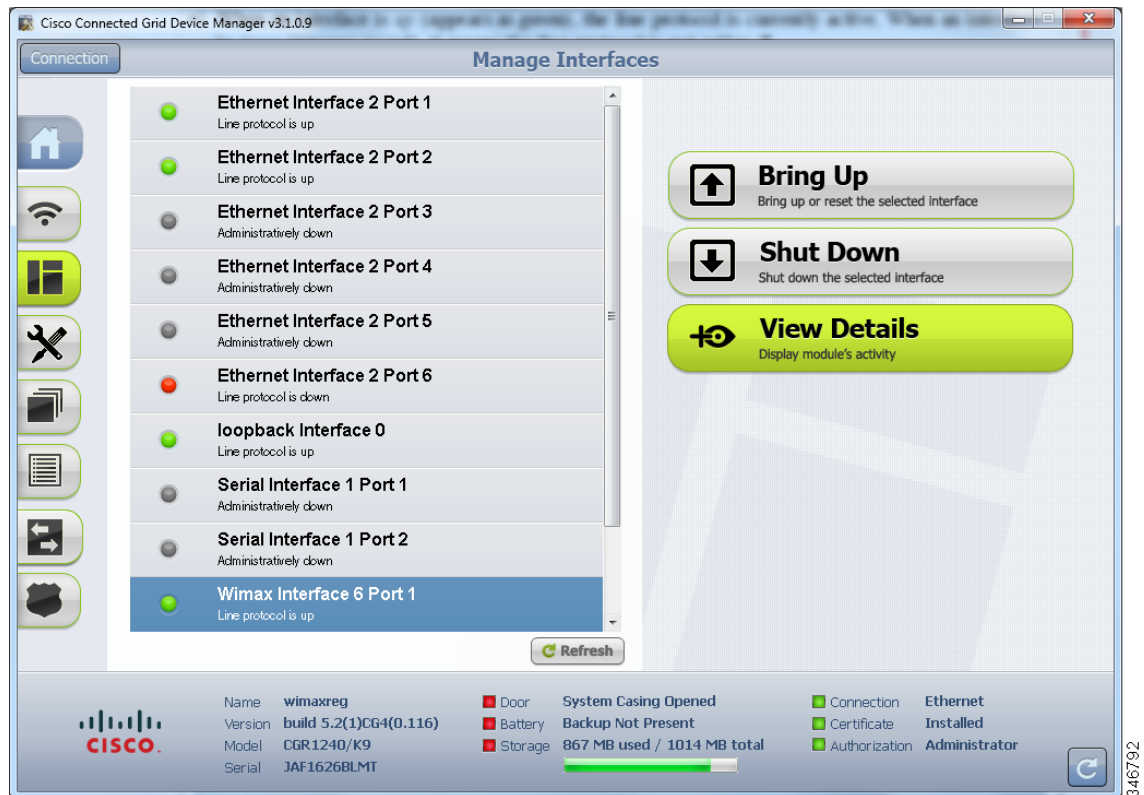
- 
- Step 1** On the Test Connectivity page, select the target IP address from the list.
- Step 2** Click **Remove**.
- 

## Manage Interfaces

You can bring up or shut down an interface on the Manage Interfaces page. You can also view details about a module's activity and reload a module from the Manage Interfaces page.

- When an interface is *up* (appears as green), the line protocol is currently active. When an interface is *down* (appears as red), it means the line protocol is not active.
- When an interface is administratively down (appears as gray), the line interface was taken down by the administrator.

All interfaces installed within the CGR 1000 display automatically.



This section covers the following topics:

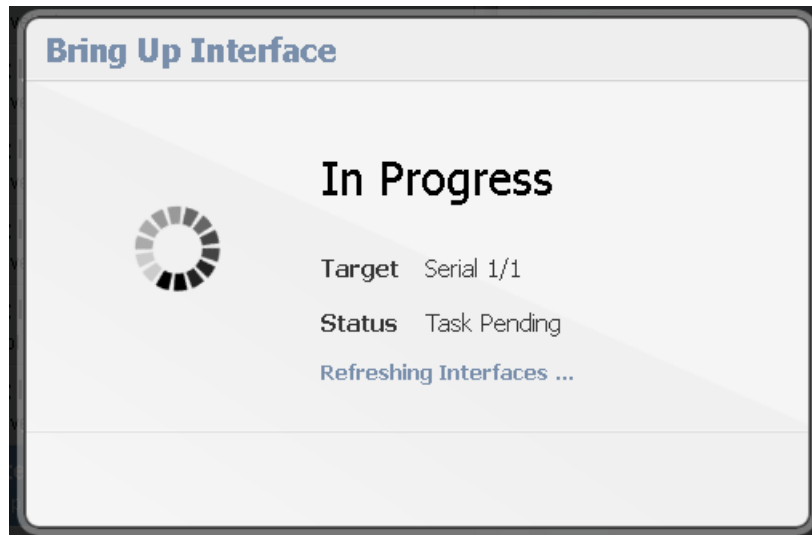
- [Bring Up an Interface](#)
- [Shut Down an Interface](#)
- [View Details for an Interface](#)
- [Reload a Module](#)

## Bring Up an Interface

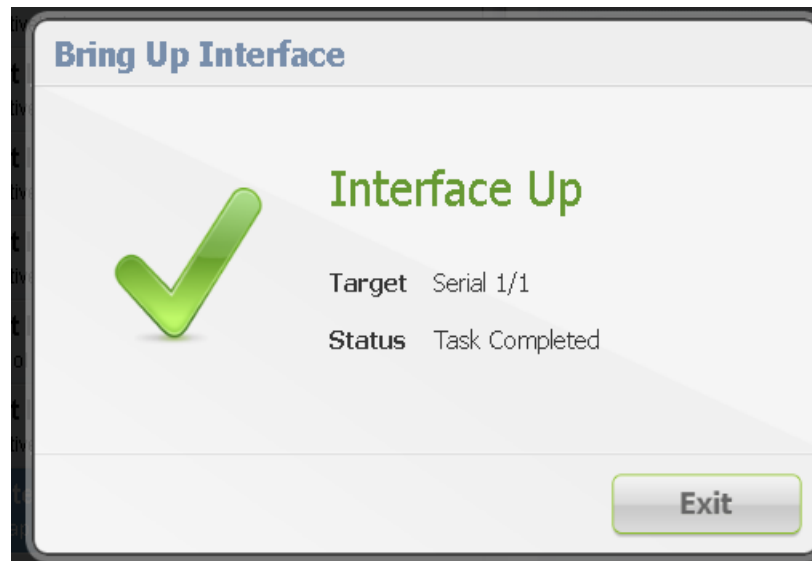
When an interface is shut down for any reason, you can attempt to bring up the interface by doing the following:

- 
- Step 1** From the At a Glance page, click **Manage Interfaces**.
- Step 2** On the Manage Interfaces page, select an interface and then click **Bring Up Interface**.  
The In Progress message appears. When the interface is up, the Interface Up dialog box appears.





345395



345394

## Shut Down an Interface

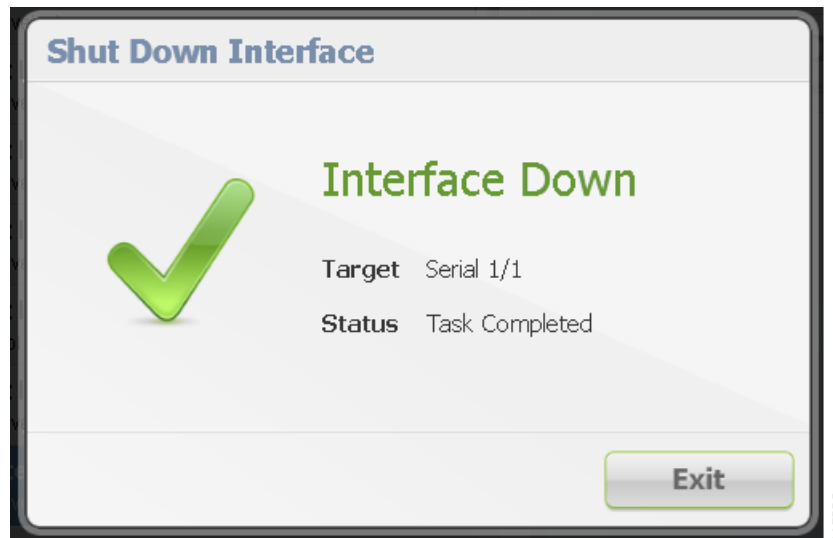
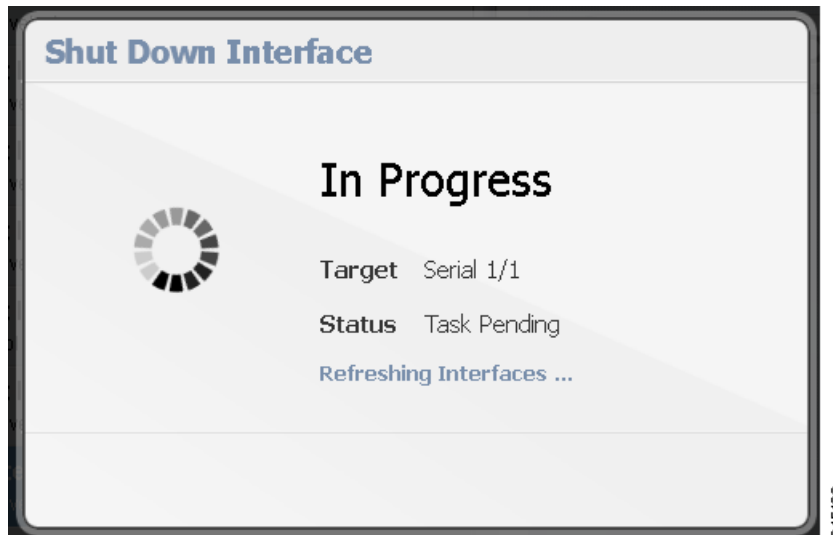


### Caution

Do not shut down the interface on which the Device Manager communicates with the CGR 1000 or the connection will be lost.

Follow these steps to shut down an interface:

- Step 1** From the At a Glance page, click **Manage Interfaces**.
- Step 2** On the Manage Interfaces page, select an interface and then click **Shut Down**.  
The In Progress message appears. When the process completes, the Interface Down dialog box appears.



## View Details for an Interface

The View Details feature allows you to display information for the selected interface and related module, including interface status, model number, MAC and IP addresses, and dynamic statistics. The information is updated every 10 seconds.



### Note

In this release, details are available for the WiMAX module only.

Follow these steps to view details for a module:

- Step 1** From the At a Glance page, click **Manage Interfaces**.

- Step 2** On the Manage Interfaces page, select an interface and then click **View Details**.  
The Module Activity page appears.



## WiMAX Details

The following information is displayed for the WiMAX module:

- Slot in which module is inserted
- Model number
- MAC address
- IP address
- Physical layer state (indicates Connected, Disconnected, Scanning, or Authenticating)
- BSID (ID of the base station to which the WiMAX module is connected)
- Frequency of transmission of the WiMAX module
- Channel bandwidth (bandwidth supported by the WiMAX module)
- RSSI (Received Signal Strength Indication measured in dBm)
- CINR (Carrier to Interference Noise Ratio measured in dB. A higher value indicates better signal strength)
- Packets in (number of incoming packets)
- Packets out (number of outgoing packets)

- DL Bad CRC Packets (number of bad packets during download - ideally 0)
- Hardware version
- Board version

## Reload a Module

Reloading a module shuts off power to the module then powers it on again.



### Note

In this release, the Reload Module feature is available for the WiMAX module only.

Follow these steps to reload a module:

- 
- Step 1** From the At a Glance page, click **Manage Interfaces**.
- Step 2** On the Manage Interfaces page, select an interface and then click **View Details**.  
The Module Activity page appears.
- Step 3** Click **Reload Module**.

The message *Reloading module...* appears in the Updates area (bottom of left pane). When reloading is complete, the message *Module reloaded successfully* appears in the Updates area, and it takes 3-4 minutes for WiMAX module base station connectivity to be reestablished.

---

## Change Configuration

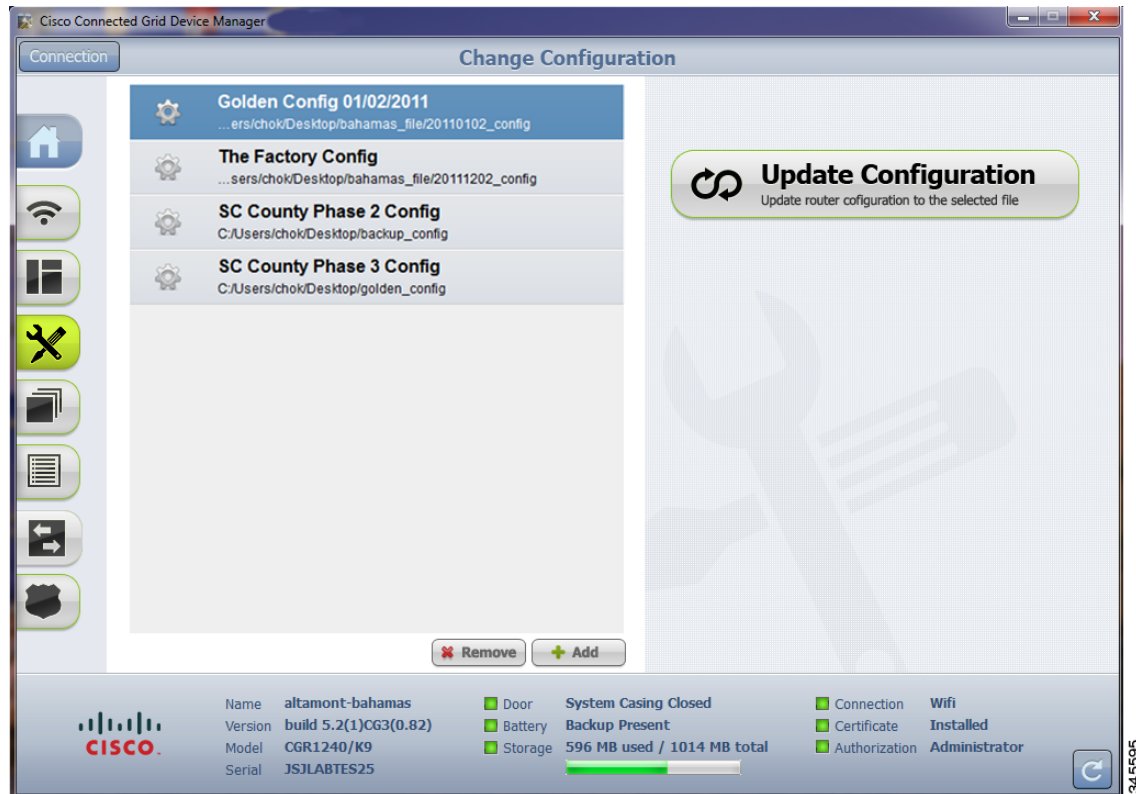
The Change Configuration task allows you to upload a configuration file to the Device Manager and then use that file to update the configuration of the CGR 1000. The configuration file information must include version, username and password, Ethernet and WiFi interfaces, and Device Manager (CGDM) and IP HTTPS configurations.



### Note

The configuration file must be a complete and valid CGR 1000 configuration. When the configuration file contains missing fields, the Device Manager stops the file upload and warns that the configuration file is incomplete. When you receive an error while updating the configuration file, check the configuration file for missing information.

---



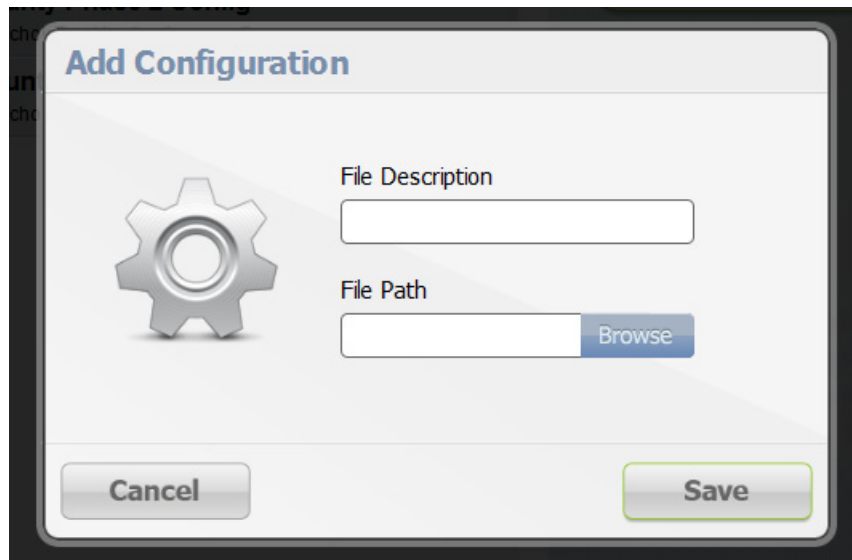
This section covers the following topics:

- [Add a Configuration File](#)
- [Update Configuration](#)
- [Correct a Configuration File](#)
- [Remove Configuration File](#)

## Add a Configuration File

Follow these steps to add a configuration file to the Device Manager:

- 
- Step 1** From the At a Glance page, click **Change Configuration**.
- Step 2** Click **Add**.



- Step 3** In the Add Configuration dialog box:
- a. Enter a file description for the configuration file that you are going to upload.
  - b. Click **Browse** to navigate to the configuration file location and select the file.
  - c. Click **Save**.

## Update Configuration

After uploading the configuration file to Device Manager, you can use the file to update the CGR 1000 configuration.



### Caution

Updating the configuration 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.

Follow these steps to update the configuration file on the CGR 1000:

- Step 1** On the Change Configuration page, select the desired configuration file (left pane).
- Step 2** Click **Update Configuration**.
- If a confirmation dialog box appears, click **Confirm** to verify that you would like to change the router configuration.
  - If an error message appears, the file did not upload to the CGR 1000.  
Proceed to [Correct a Configuration File](#).

## Correct a Configuration File

A configuration file upload fails because the configuration file has missing fields such as version, username and password, Ethernet and WiFi interfaces, and Device Manager (CGDM) and IP HTTPS details.

To correct a configuration file error:

- 
- Step 1** Check the configuration file for errors. If errors or missing information exist, make corrections.
  - Step 2** Remove the current configuration file from the Device Manager. (See [Remove Configuration File, page 3-25](#).)
  - Step 3** Add the updated configuration file to Device Manager. (See [Add a Configuration File](#).)
  - Step 4** Update the configuration file. (See [Update Configuration](#).)
- 

## Remove Configuration File

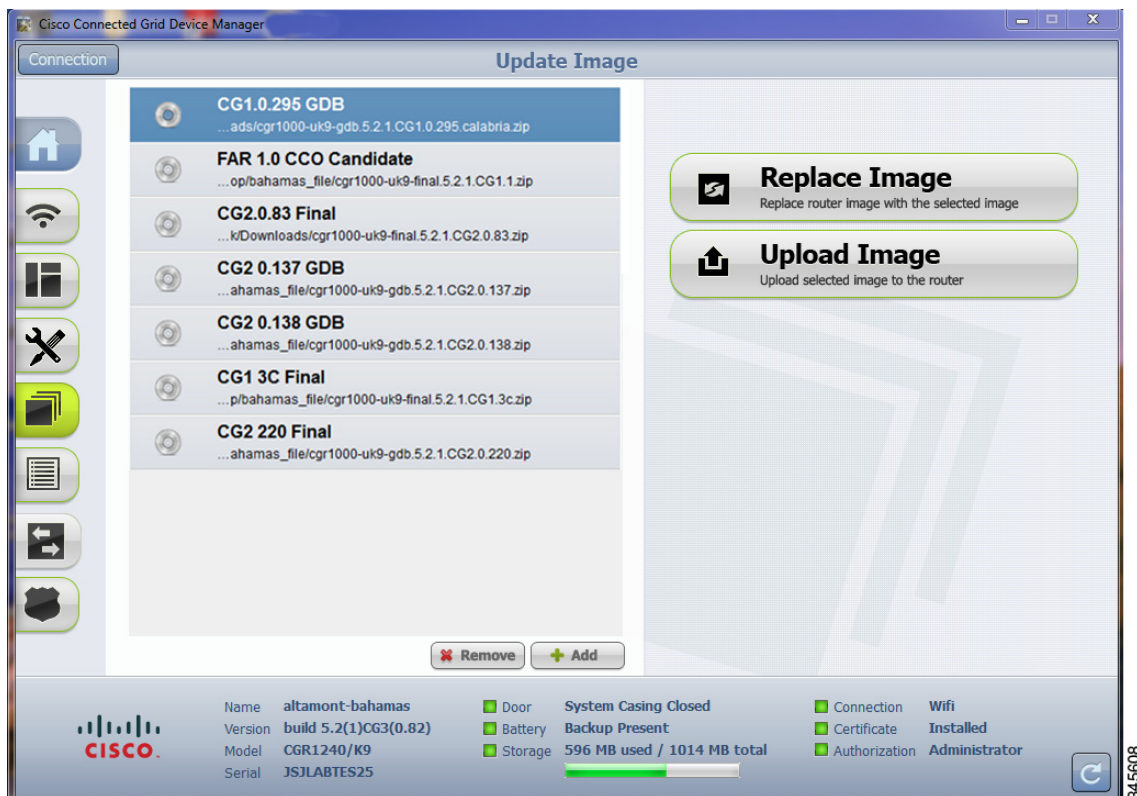
After you update the CGR 1000 with the new configuration file, you can remove the file from Device Manager. You can also use this function to remove unwanted or duplicate configuration files.

Follow these steps to remove a configuration file:

- 
- Step 1** On the Change Configuration page, select the configuration file you want to remove from the list.
  - Step 2** Click **Remove**.
- 

## Update 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.



This section covers the following topics:

- [Upload Image](#)
- [Replace Image](#)
- [Remove Image](#)

## Upload Image

Before you can update an image on the CGR 1000, you must upload the image to the Device Manager.

The Upload Image option allows you to upload and store a copy of a software 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.

Follow these steps to upload a image:

- 
- Step 1** From the At a Glance page, click **Update Image**.
- Step 2** On the Update Image page, select the CGR 1000 software image that you want to upload.



**Note** If the software image that you want to install on the CGR 1000 is not listed, click **Add** and browse to the image, and then click **OK** to upload the image.

---

- Step 3** Click **Upload Image**.



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

---

## Replace Image



### Caution

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

---

Follow these steps to replace an image:

- Step 1** On the Update Image page, select an CGR 1000 image.
  - Step 2** Click **Replace Image**.  
A confirmation dialog box appears.
  - Step 3** To begin the replace image process, click **Confirm**.
  - Step 4** After the router software update completes, the router restarts.
- 

## Remove Image

After you update an image, you can remove the image file from the Device Manager. You can also use the Remove image option to remove a image file you added mistakenly.

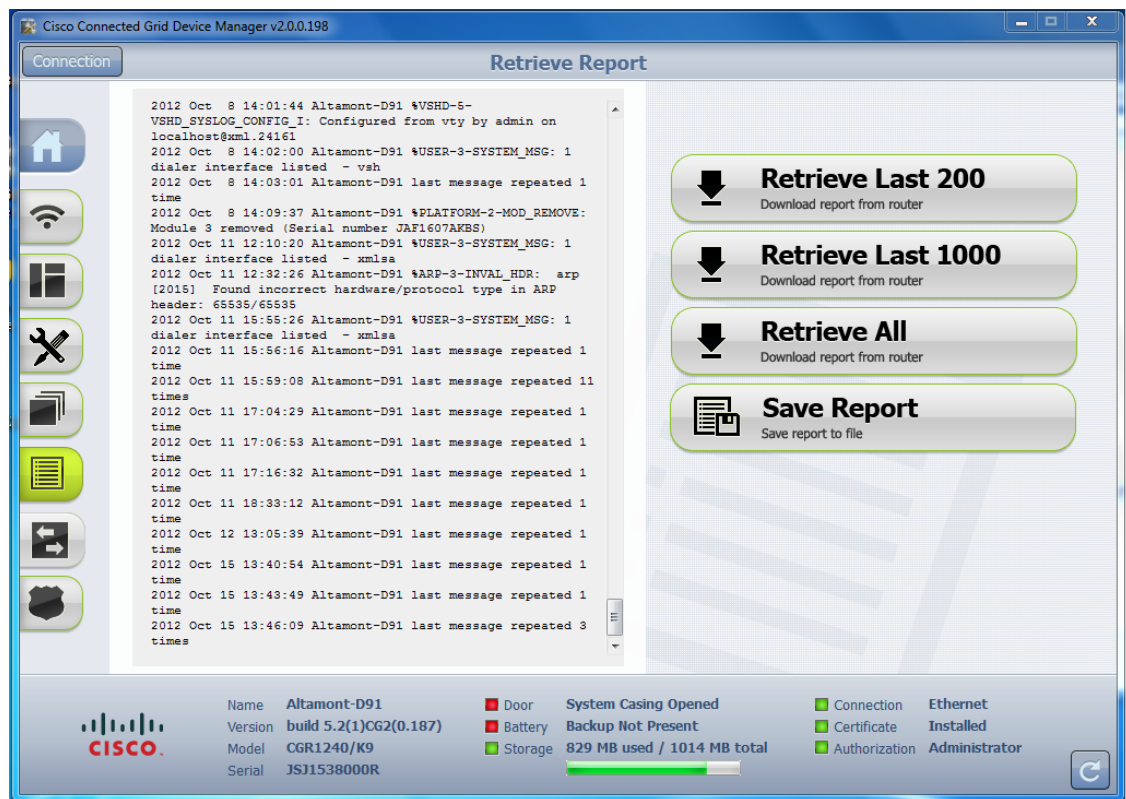
Follow these steps to remove an image:

- Step 1** On the Update Image page, select an CGR 1000 image.
  - Step 2** Click the **Remove** button (bottom of page).
- 

## Retrieve Report

You can retrieve real-time reports of log events from the CGR 1000 and view them on the Retrieve Report page or save the information to a *.txt* file.

- You can specify that you want to retrieve and view all CGR 1000 log events (Retrieve All) or view a specified number of log events (200 or 1000)
- You can specify that you want to save a copy of the log events that display on the Retrieve Report page to your laptop (Save Report)



## Retrieve and Save Reports

Follow these steps to retrieve real-time reports from the CGR 1000:

- 
- Step 1** From the At a Glance page, click **Retrieve Report**.
- Step 2** On the Retrieve Report page, click the type of report that you want to view or save:
- Retrieve Last 200—Displays the last 200 log events of the CGR 1000.
  - Retrieve Last 1000—Displays the last 1000 log events of the CGR 1000.
  - Retrieve All—Displays all current log events of the CGR 1000.
  - Save Report—Saves a copy of the retrieved log events (displayed on the page) to a default file, *systemlog.txt*. By default, the application saves this file in the Documents folder. However, you can specify the destination for the file. See [SYSTEMLOG.TXT SAMPLE](#) for example output.
- 

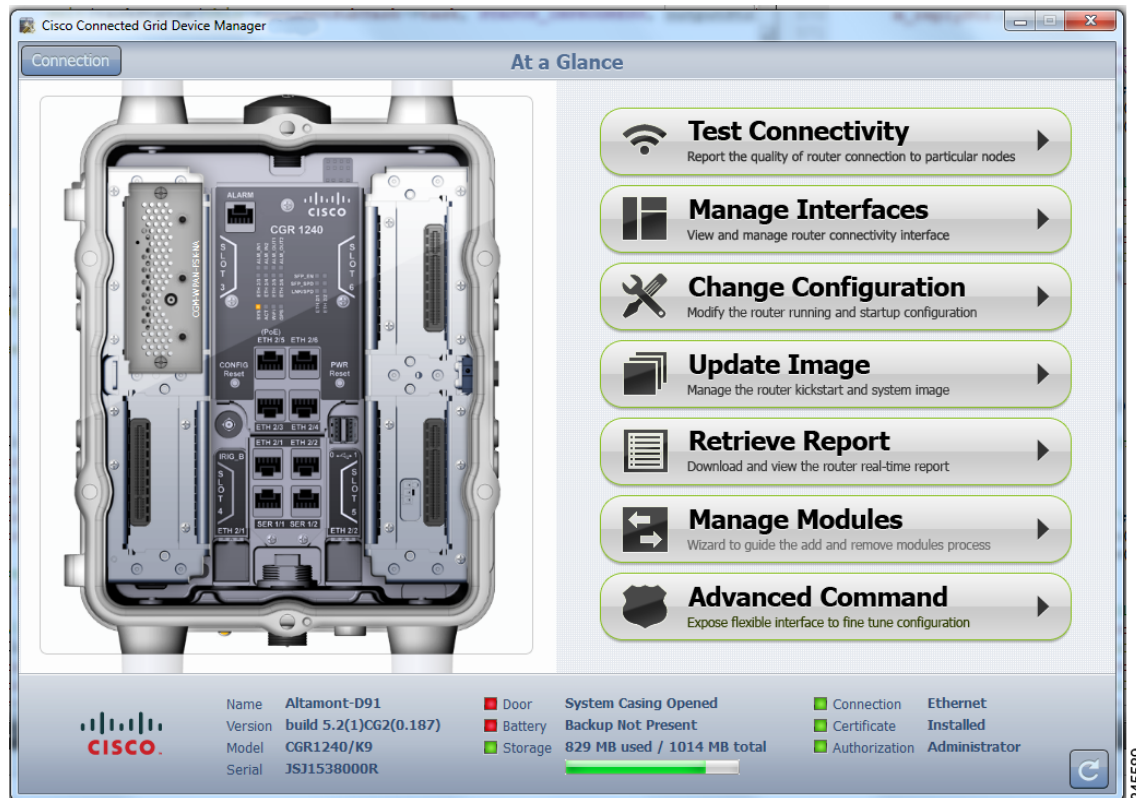
## Manage Modules

The Manage Modules page provides a wizard that guides you through the process of adding or removing 3G and WiMAX modules.

The Device Manager updates the configuration file and reloads the CGR 1000 after you add or remove a module.

The plus sign (+) indicates an available slot.

The minus sign (-) indicates an occupied slot.



This section covers the following topics:

- [Add a Module](#)
- [Remove 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* at: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)
- For details on installing a specific module, refer to the Installation and Configuration Guide for that module at: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)

## Add a Module

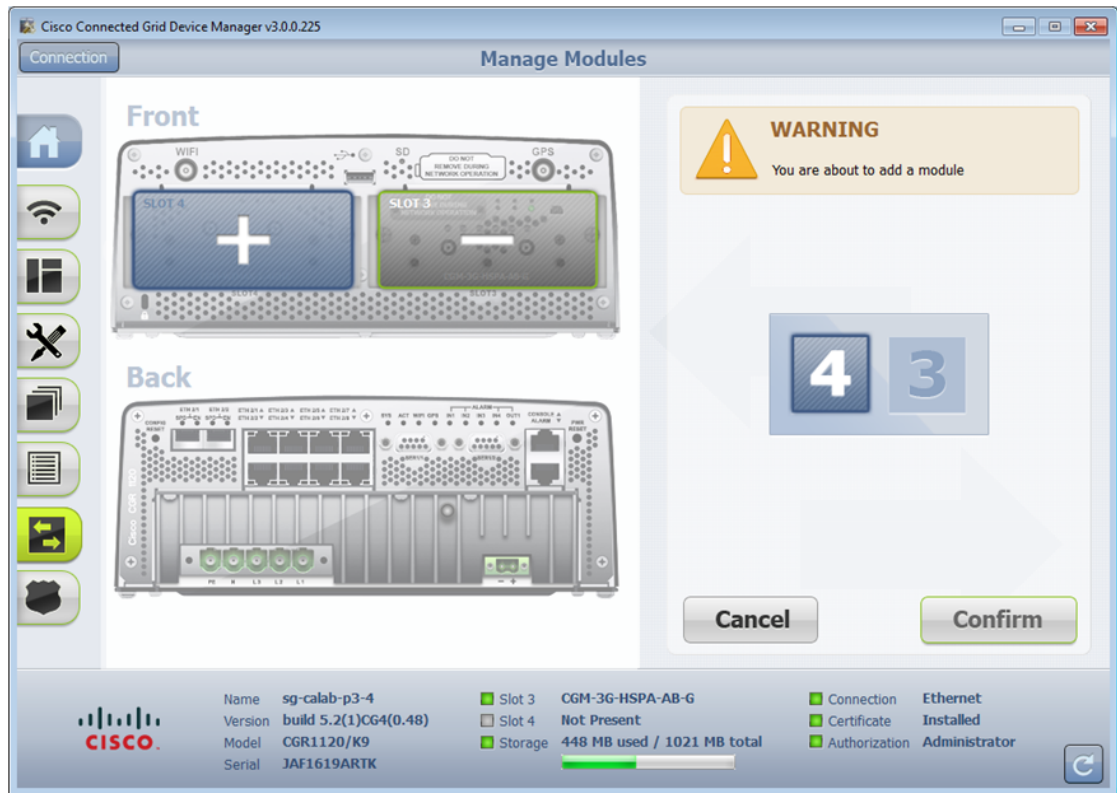


Note

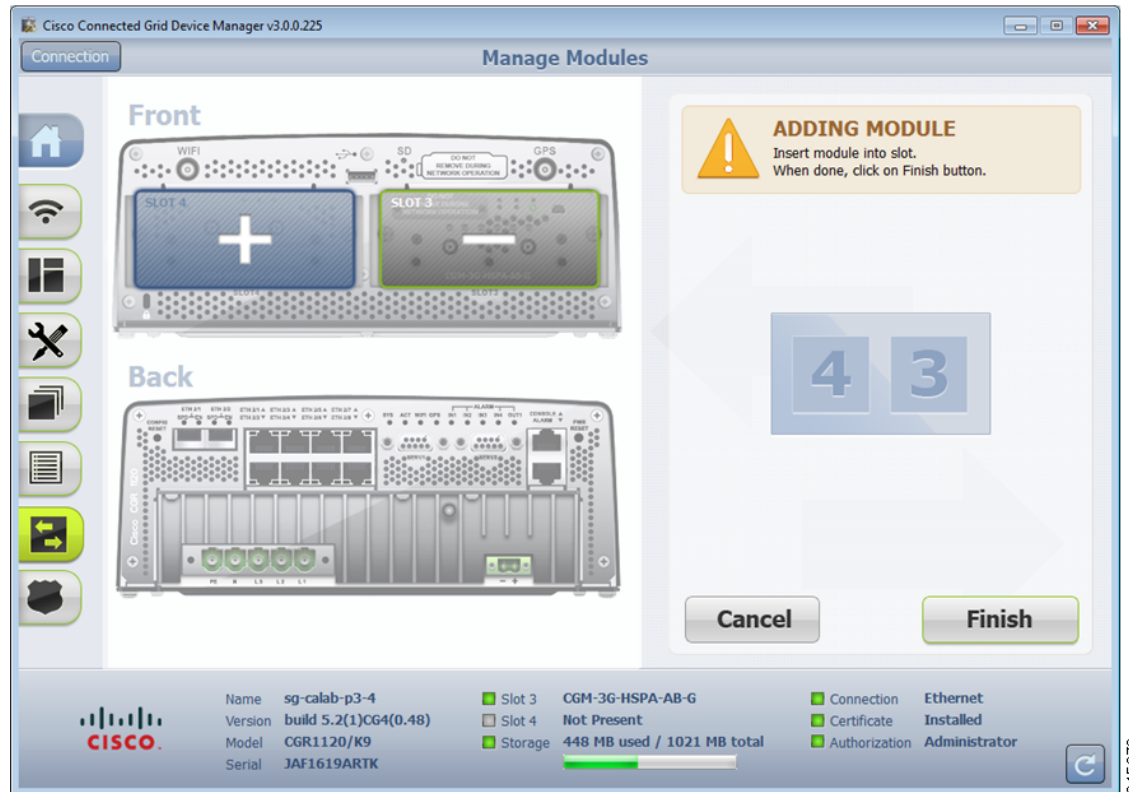
You cannot run any other operations when adding the module.

To add a module, do the following:

- Step 1** On the Manage Modules page, click on a plus (+) sign in the router diagram (left pane) to get started. A blue outline appears around the slot in the router diagram to confirm selection, and a *Please wait...* message appears on the page. Do not install the module until this message disappears from the page.



- Step 2** After the *Please wait...* message disappears, insert the module into the physical slot of the router.

**Step 3** Click **Finish**.

The following message appears on the page to indicate an update to the configuration file is in process: *Inserting module into slot. This process will take several minutes. Please wait.*

A green line appears around the slot within the router diagram when the module is active.

**Step 4** After you successfully insert the module, click Refresh icon (lower-right corner).

A minus (-) sign appears in the slot where you added the module.

## Remove 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, do the following:

**Step 1** On the Manage Modules page, click on a module slot within the Info area (right pane) that corresponds to the location of the module that you want to remove. Populated slots display a minus sign (-).

A blue outline appears around the slot in the router diagram to confirm selection, and a Warning message appears stating that you are about to remove a module.

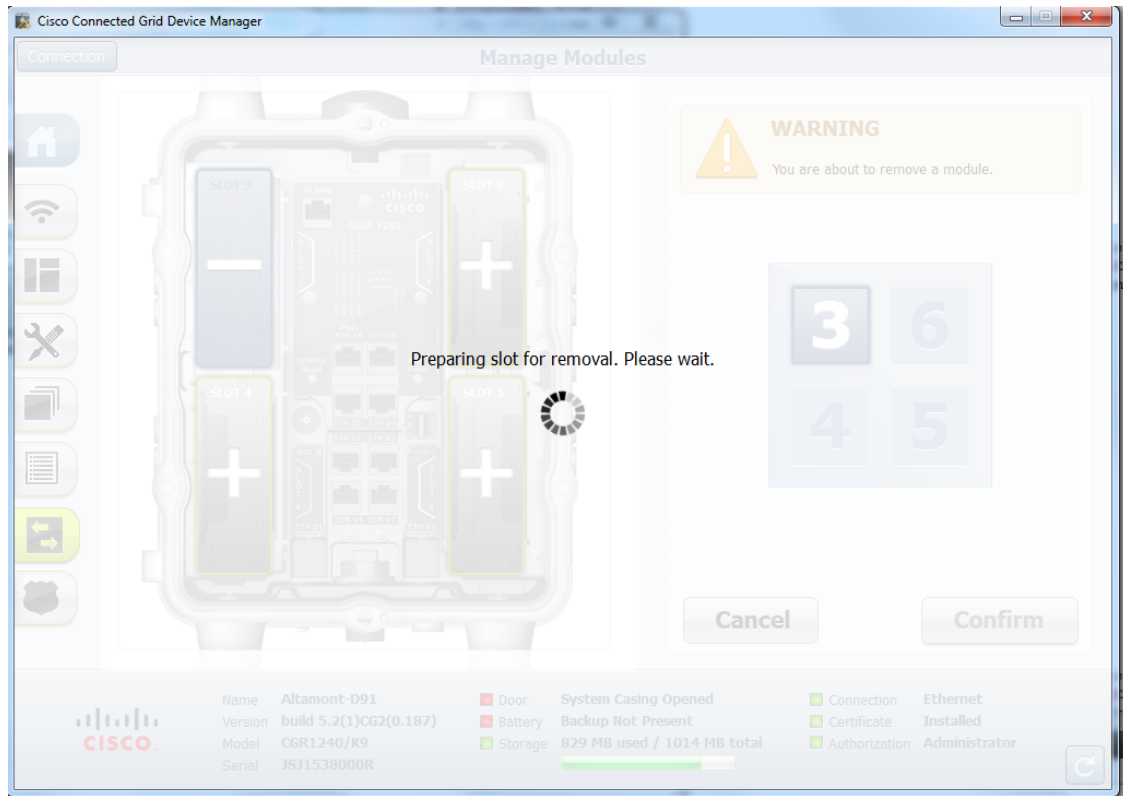
**Step 2** To continue the removal, click **Confirm**.

The following message appears on the page:  
*Preparing slot for removal. Please wait.*



**Caution**

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



345591



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

**Step 4** Click **Finish**.

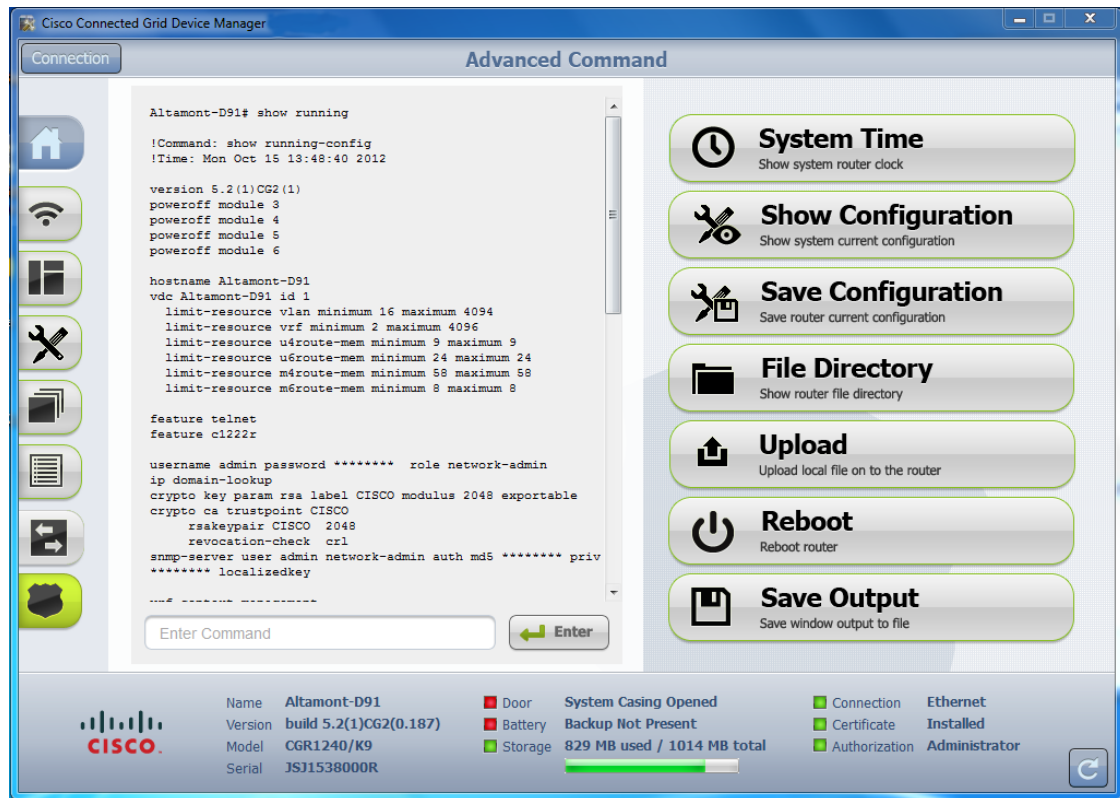
The following message appears on the page to indicate an update to the configuration file is in process:  
*Removing module from slot. This process will take several minutes. Please wait.*

**Step 5** When the configuration update completes, a success message appears.

A plus (+) sign now appears in the slot where you physically removed the module indicating an empty slot.

## Advanced Command

The Advanced Command task provides access to the CGR 1000 to fine-tune or troubleshoot the router. You must be familiar with Cisco CG-OS commands. For details on supported commands, refer to the CGR 1000 software configuration guides at: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)

**Note**

Not all interactive commands are supported. Configuration commands must be concatenated together, as follows: `configuration terminal ; interface ethernet2/1 ; shutdown ; end`

**Step 1**

From the At a Glance page, click **Advanced Command**. In addition to the advance console, you have the following choices:

- Click **System Time** to display the current setting of the system clock for the router.
- Click **Show Configuration** to display the current configuration of the router.
- Click **Save Configuration** to save the current router configuration to startup-config file.
- Click **File Directory** to display the router file directory.
- Click **Upload** to upload a new image file to the router.
- Click **Reboot** to reboot the router.
- Click **Save Output** to save the output displayed on the page to a file, *windowslog.txt*. By default, the application saves the *windowslog.txt* file to the Documents folder. (See [WINDOWSLOG.TXT SAMPLE](#), page 3-36.)



## Import Certificates

As admin, you can import certificates through the Device Manager by employing the Setup wizard or by command line. You will 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 onto the Device Manager laptop.

The Setup wizard launches when either the user clicks the Settings icon on the opening page of the Device Manager or when the application does not detect a certificate.

To open the Import Certificate page, do the following:

- 
- Step 1** Step through the Setup wizard until you reach the Certificate Configuration page by clicking **Next** on each page. (See [Setting Operating Mode](#).)
- You do not need to change any values on the pages as you move through the pages.
- Step 2** On the Certificate Configuration page, click **Change Certificate**.
- The Import Certificate page appears.



- Step 3** On the Certificate Configuration page, browse to the location of the certificate file (.pfx) on your laptop.
- Step 4** Enter the certificate password and then click **Import**.
- 

## Disconnect from the CGR 1000

After finishing your work on the CGR 1000, click **Connection** (upper-left) to disconnect the Device Manager from the router. The application opens the Connect to the Router page.

## Connection Override

You only use the Connection Override option when you need to use different login information than that provided in the work order.

For example, 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 admin for that information and use Connection Override to enter that new information to log in to the router.

Optionally, the field technician can directly connect to the router by using the Over Ethernet option with the Auto Discover IP address option.

To change the login information, do the following:

- 
- Step 1** On the Work Authorization page, click **Connection Override**.

- Step 2** In the Connection Override dialog box, select the connection type (Over Ethernet, Over WiFi, or Auto Detect) from the Connect drop-down menu.

- Step 3** Click **Connect**.
- 

## Example Log File Output

This section contains output examples for files generated from the Retrieve Report and Advanced Command pages of the Device Manager.

### WINDOWSLOG.TXT SAMPLE

The following example represents typical content that might be found in the *windowslog.txt* file generated from the Advanced Command page.

```
CGR-1# show clock
15:13:37.311 PST Tue Oct 16 2012
```

```
CGR-1# show running

!Command: show running-config
!Time: Tue Oct 16 15:13:38 2012

version 5.2(1)CG3(1)
logging level feature-mgr 0
hostname CGR-1
vdc CGR-1 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource u4route-mem minimum 9 maximum 9
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature telnet
feature crypto ike
crypto ike domain ipsec
  policy 10
  group 1
  identity hostname
feature ospf
feature tunnel
feature crypto ipsec virtual-tunnel
feature c1222r

username admin password *** <fingerprint value> role network-admin
no password strength-check
ip domain-lookup
ip host nms.cisco.com 192.168.193.11
crypto key param rsa label Blue modulus 2048
crypto ca trustpoint Blue
  enrollment profile Blue
  rsakeypair Blue 2048
  revocation-check none
  enrollment retry count 3
  enrollment retry period 5
  serial-number
  fingerprint <fingerprint value>
crypto ca profile enrollment Blue
  enrollment url http://10.0.2.2:80
ip access-list ce-traffic
  statistics per-entry
  10 permit tcp any any eq 1153
class-map type qos match-all ce-traffic
  match access-group name ce-traffic
policy-map type qos ce-traffic
  class ce-traffic
    set dscp 46
snmp-server user admin network-admin auth md5 <value> priv <value> localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
callhome
  email-contact root@localhost
  phone-contact +1-000-000-0000
  streetaddress a-street-address
  destination-profile nms
  destination-profile nms format netconf
  destination-profile nms transport-method http
```

```
destination-profile nms http https://nms.cisco.com:9121 trustpoint Blue
destination-profile nms alert-group all
enable

vrf context management
crypto ipsec transform-set trans1 esp-aes 128 esp-sha1-hmac
crypto ipsec profile MyIPSecProfile
  set transform-set trans1
vlan 1

route-map CONN permit 10
  match interface loopback0

chat-script gsm PROFILE1
wimax scan-list airspan2344
  channel index 1 frequency 2344000 bandwidth 10000
  nap id C1:5C:00 priority 1 channel-index 1
  nsp id C1:5C:00 home
wifi ssid CGDM
  authentication key-management wpa2
  wpa2-psk ascii encrypted 7 1234567890

interface Tunnel1
  ip address 20.5.20.3/31
  tunnel source loopback0
  tunnel destination 20.2.10.1
  description GRE tunnel
  no keepalive
  no shutdown

interface Tunnel19
  ip address 20.4.20.2/24
  ip ospf cost 100
  ip ospf mtu-ignore
  ip router ospf 1 area 0.0.0.1
  tunnel mode ipsec ipv4
  tunnel source Wimax6/1
  tunnel destination 10.0.4.8
  description ipsec tunnel through wimax
  no keepalive
  tunnel protection ipsec profile MyIPSecProfile
  no shutdown

interface Tunnel20
  ip address 20.3.20.2/24
  ip ospf cost 200
  ip ospf mtu-ignore
  ip router ospf 1 area 0.0.0.1
  tunnel mode ipsec ipv4
  tunnel source Cellular3/1
  tunnel destination 173.36.248.197
  description ipsec tunnel through ATT 3G
  no keepalive
  tunnel protection ipsec profile MyIPSecProfile
  no shutdown

interface Tunnel21
  service-policy type qos output ce-traffic
  ip address 20.1.20.2/24
  ip ospf cost 300
  ip ospf mtu-ignore
  ip router ospf 1 area 0.0.0.1
  tunnel mode ipsec ipv4
```

```
tunnel source Ethernet2/1
tunnel destination 10.0.4.8
description ipsec tunnel through E2/1
no keepalive
tunnel protection ipsec profile MyIPSecProfile
no shutdown

interface Dialer1
dialer persistent
dialer pool 1
dialer string gsm
no shutdown

interface Ethernet2/1
description ==sol-3750-1
ip address 10.0.5.1/24
no shutdown

interface Ethernet2/2
description ==2.3.094 blue
ip address 172.27.89.56/25
no shutdown

interface Ethernet2/3
no shutdown

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface loopback0
ip address 20.2.10.2/32
ip router ospf 1 area 0.0.0.1

interface Cellular3/1
dialer pool-member 1
no shutdown

interface Wimax6/1
no shutdown
scan-list airspan2344
ip address 10.0.7.3/24

interface Wpan4/1

interface Wifi2/1
ssid CGDM
no shutdown
ipv6 address use-link-local-only
clock timezone PST -8 0
line console
exec-timeout 0
line vty
exec-timeout 0
router ospf 1
redistribute direct route-map CONN
ip route 10.0.2.0/24 10.0.5.2
ip route 10.0.2.1/32 10.0.5.2
ip route 10.0.2.2/32 10.0.5.2
ip route 10.0.2.3/32 10.0.5.2
ip route 10.0.2.53/32 20.2.10.1
ip route 10.0.2.102/32 20.2.10.1
```

```

ip route 10.0.4.0/24 10.0.5.2 2
ip route 10.0.4.0/24 10.0.7.2
ip route 128.0.0.0/24 Cellular3/1
ip route 171.0.0.0/8 172.27.89.1
ip route 172.0.0.0/8 172.27.89.1
ip route 173.36.248.0/24 Cellular3/1

cgdm
  registration start trustpoint Blue
ip http secure-server
ip http secure-port 8443
ip http secure-server trustpoint Blue

```

## SYSTEMLOG.TXT SAMPLE

The following example represents typical content that might be found in a *systemlog.txt* file generated from the Retrieve Reports page.

```

2012 Oct 16 14:44:12 CGR-1 Oct 16 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456678] - kernel
2012 Oct 16 14:44:12 CGR-1 Oct 16 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456830]
/1_0_cdma_qos/third-party/src/linux/kernel/wr13/linux-2.6.27_wrl30/drivers/i2c/busses/ih/
ih_i2c_hal.c:ih_i2c_wait_for_xfer_complete returns 0 - kernel
2012 Oct 16 14:44:12 CGR-1 Oct 16 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456847] - kernel
2012 Oct 16 14:44:13 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:47:02 CGR-1 last message repeated 1 time
2012 Oct 16 14:47:31 CGR-1 last message repeated 2 times
2012 Oct 16 14:47:31 CGR-1 %PLATFORM-2-DISK_ALERT: Disk Status Alert : disk partition
'/bootflash' is at high usage level (91%).
2012 Oct 16 14:47:31 CGR-1 %CALLHOME-2-EVENT: LOW_FLASH_SPACE
2012 Oct 16 14:47:31 CGR-1 %PLATFORM-2-DISK_ALERT: Disk Status Alert : disk partition
'/isan' is at high usage level (91%).
2012 Oct 16 14:47:32 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:47:57 CGR-1 last message repeated 1 time
2012 Oct 16 14:47:57 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:47:57 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:48:01 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - dcos-ping
2012 Oct 16 14:49:39 CGR-1 last message repeated 2 times
2012 Oct 16 14:50:20 CGR-1 last message repeated 1 time
2012 Oct 16 14:50:20 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:50:21 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - dcos-ping
2012 Oct 16 14:50:34 CGR-1 last message repeated 1 time
2012 Oct 16 14:50:34 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:50:37 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - dcos-ping
2012 Oct 16 14:50:38 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:51:15 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - rm
2012 Oct 16 14:51:16 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - java
2012 Oct 16 14:51:16 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - pidof
2012 Oct 16 14:51:20 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:51:30 CGR-1 last message repeated 1 time
2012 Oct 16 14:51:30 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:51:31 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:51:38 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - su
2012 Oct 16 14:51:38 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - xmlsa
2012 Oct 16 14:51:39 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called -
dcos-traceroute
2012 Oct 16 14:52:11 CGR-1 last message repeated 1 time
2012 Oct 16 14:52:25 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:52:32 CGR-1 last message repeated 1 time
2012 Oct 16 14:52:32 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:52:33 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:52:33 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:53:10 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - vsh

```

```

2012 Oct 16 14:53:56 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:53:56 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:54:32 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:55:58 CGR-1 last message repeated 2 times
2012 Oct 16 14:55:58 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:55:59 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:57:13 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:57:53 CGR-1 last message repeated 2 times
2012 Oct 16 14:57:53 CGR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
console0
2012 Oct 16 14:57:53 CGR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
localhost@xml.7555
2012 Oct 16 14:57:54 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:57:55 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - vsh
2012 Oct 16 14:57:56 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 14:58:12 CGR-1 last message repeated 1 time
2012 Oct 16 14:58:12 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 14:58:13 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 14:58:53 CGR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
localhost@xml.7555
2012 Oct 16 14:58:54 CGR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed - xmlsa
2012 Oct 16 15:00:53 CGR-1 last message repeated 1 time
2012 Oct 16 15:00:53 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 15:00:53 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 15:03:08 CGR-1 %DIALER-5-DIALER_MODEM_UP: Modem active
2012 Oct 16 15:04:15 CGR-1 last message repeated 1 time
2012 Oct 16 15:04:15 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 15:04:15 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 15:07:56 CGR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Oct 16 15:07:56 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - curl
2012 Oct 16 15:10:51 CGR-1 %USER-3-SYSTEM_MSG: --- plcpm_init is called - vsh

```

## Feature History

Feature Name	Release	Feature Information
View details for WiMAX module and reload the module	Cisco CG-DM Release 3.1	Initial support of the feature on the Device Manager
Add and remove modules	Cisco CG-DM Release 3.0	
Certificate import enhancement		
Role-based Access Control (RBAC)		
Work Authorization access	Cisco CG-DM Release 1.1	
Support for Cisco 1120 Connected Grid Router (CGR 1120)		
Upload Image one-touch button		







## Troubleshooting

---

This chapter provides a listing of problems or common error messages that you might see when using the Device Manager and provides actions that you can take to resolve the issues.

This chapter addresses the following topics:

- [Certificate Errors, page 4-1](#)
- [Connection Errors, page 4-2](#)

### Certificate Errors

**“What should I do when I see the following errors?”**

**Causes:**

- Certificate Error
- Failed to create cert file
- Failed to parse cert file
- Failed to read client cert
- Failed to open client cert
- Invalid client cert
- Key Error
- Missing Certificate

**Resolution:** Verify that the Device Manager has a valid certificate. (See [Certificate Installation, page 2-1.](#))

**“How do I check to see if the certificate is installed?”**

See [Certificate Installation](#) page 2-5.

# Connection Errors

## “After I click Connect, I received a connection error message”

### Resolution:

- For an Ethernet connection: Verify that an IP address is defined for the interface, and verify that you can ping this IP address from the Device Manager laptop.
- For an Auto-Detect connection: Ensure that the Ethernet port on the Device Manager has a direct connection to the CGR 1000 router and that the router interface is configured with *ipv6 address use-link-local-only*.
- For a WiFi connection:
  - Verify that the WiFi parameters (SSID and passphrase) match the WiFi configuration on the router.
  - Ensure that there is no third-party wireless client tool controlling the WiFi interface. For example, if you are using a third-party client tool (such as Intel PROSet Wireless Client Tool), change the settings from that tool to enable Windows to manage the WiFi interface.

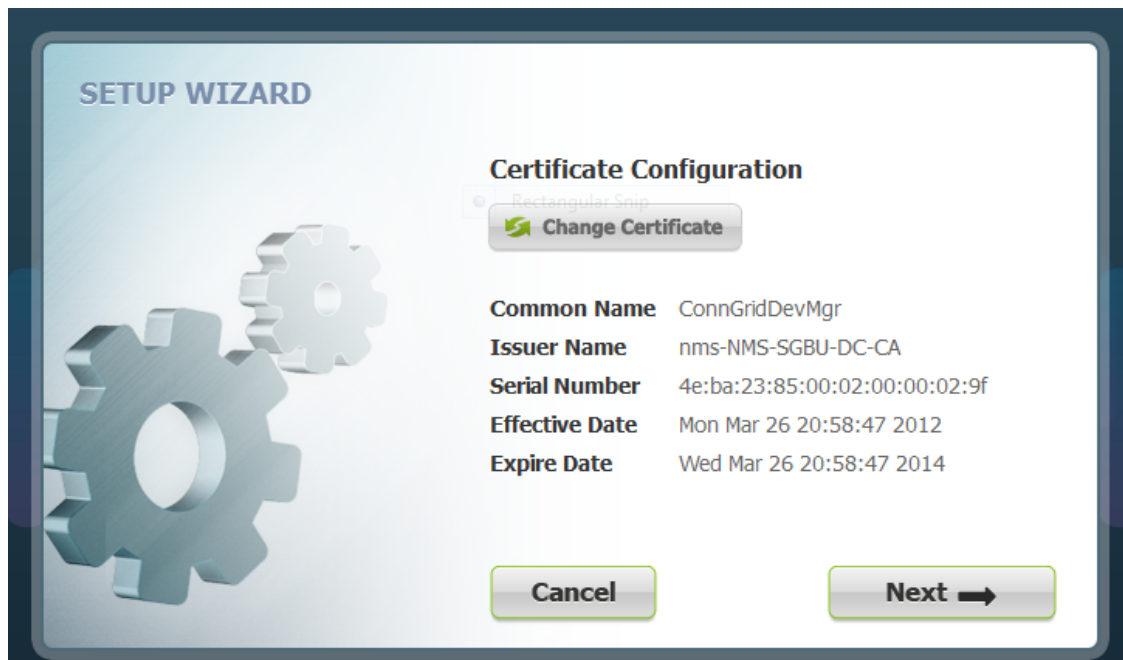
## “I cannot log in to Device Manager”

**Cause:** This message appears when the application cannot find a valid certificate. When this condition occurs, the Certificate Configuration page opens to display the currently installed certificate.

### Resolution:

Verify that the clock is set to the correct time, otherwise the certificate will not be honored.

See [Certificate Installation, page 2-1](#) for details on installing certificates.



**“Connectivity: Windows failed to join WLAN”**

**Cause:** The Device Manager cannot create a WiFi profile on the laptop on which it resides because third-party software has control of the laptop WiFi adapter. Additionally, the Device Manager cannot control WiFi through Windows API.

**Resolution:** Disable the third-party software and enable Windows to manage the WiFi interface.

**“Cannot detect peer’s IPv6 address”**

**Cause:** IPv6 peer was not found.

**Resolution:** Enable the IPv6 link local address on the CGR 1000 so that it will respond to an Auto-Discovery from the Device Manager.

See [Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide](#).

**“Connection Refused” and “Connection Timeout”****Causes:**

- IP HTTP server is not enabled on the CGR 1000
- IP HTTP server port is not set up on the CGR 1000
- Target port for the CGR 1000 and the Device Manager do not match
- IP HTTP server crashed

**Resolution:** Check the IP HTTP server settings noted above.

**“Valid work authorization is required to connect”**

**Cause:** The work authorization does not fall within the expected time, serial, and role requirements.

**Resolution:** Contact the CG-NMS admin to resubmit the work order.

**“SSL handshake failed”****Causes:**

- Certificates for the Device Manager and CGR 1000 do not match
- Inaccurate System time on the Device Manager or CGR 1000

**Resolution:** Verify that the certificates for the Device Manager and CGR 1000 match and check the System time setting on the Device Manager and CGR 1000.

**“Unable to connect to the CGR 1000 over WiFi”****Causes:**

- WiFi is not up
- Incorrect Passphrase entered in the Connect to the Router page of the Device Manager

**Resolution:**

- Attempt to connect to the CGR 1000 router over Ethernet.
- Recheck the WiFi Passphrase provided by your admin and reenter the value on the Connect to the Router page.
- Check the status of the WiFi connection.