Cisco Connected Grid Device Manager Installation and User Guide, Release 3.0

First Published: October 2012
Last Updated: June 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28196-02

No combinations are authorized or intended under this document.

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.

Cisco Connected Grid Device Manager Installation and User Guide

CONTENTS

CHAPTER 1

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 1-4

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.

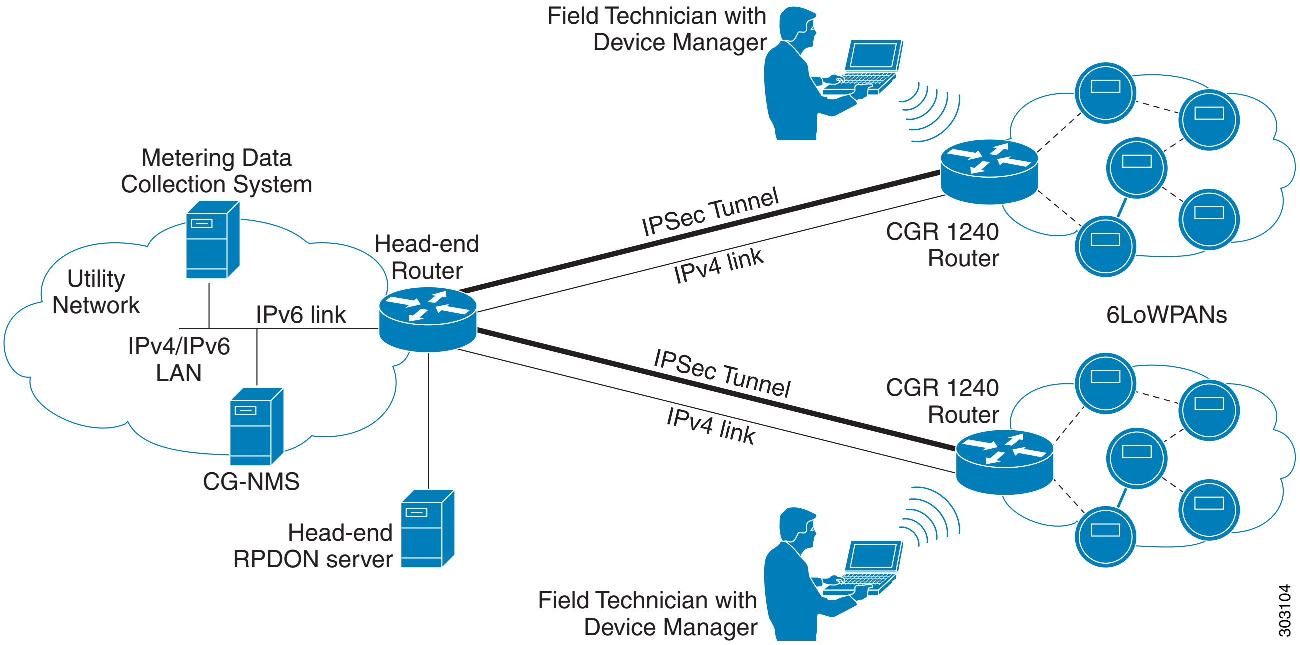
The Device Manager can operate in Connected Grid field deployments operating with or without CG-NMS.

- 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 user's 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



Tasks

The Device Manager enables you to:

- Troubleshoot connectivity between a CGR 1000 and the devices connected to the router. *See* Test Connectivity, page 3-16
- Bring up or shut down an CGR 1000 interface.

  See Manage Interfaces, page 3-21
- Check and update the current CGR 1000 configuration.

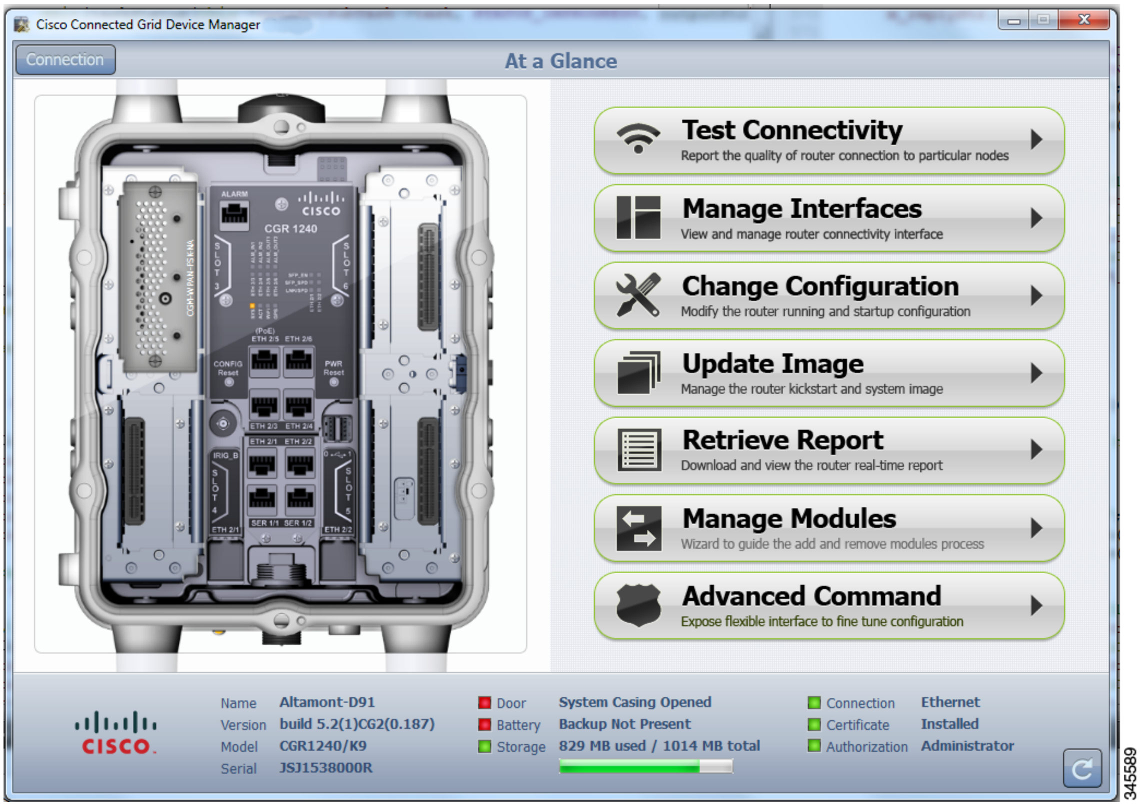
  See Change Configuration, page 3-25 and Advanced Command, page 3-37
- Update the CGR 1000 image on the router.

  See Update Image, page 3-28
- View real-time CGR 1000 configuration log for troubleshooting. *See* Retrieve Report, page 3-31
- Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. *See* Manage Modules, page 3-32
- Use advanced commands to troubleshoot the CGR 1000.

  See Advanced Command, page 3-37

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


Cisco Connected Grid Device Manager
Connection
At a Glance
CISCO
CGR 1240
ALARM
Test Connectivity
Report the quality of router connection to particular nodes
Manage Interfaces
View and manage router connectivity interface
Change Configuration
Modify the router running and startup configuration
Update Image
Manage the router kickstart and system image
Retrieve Report
Download and view the router real-time report
Manage Modules
Wizard to guide the add and remove modules process
Advanced Command
Expose flexible interface to fine tune configuration
cisco
345589

Name Altamont-D91
Version build 5.2(1)CG2(0.187)
Model CGR1240/K9
Serial JSJ1538000R

🟥 Door System Casing Opened
🟥 Battery Backup Not Present
🟩 Storage 829 MB used / 1014 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

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 can be assigned up to four different types of roles that manage your access to operational and management functions of the Device Manager summarized on the At a Glance page. Roles, users, and permissions are defined and assigned by an CG-NMS admin.

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

- When the Device Manager is operating in non-NMS mode, user access is managed by the assigned certificate extension OID.
- When the Device Manager is operating in NMS mode, user access is managed by the role assigned to a Work Authorization. The supported roles are admin, technician, and viewer.
  - 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, view status of interfaces, and retrieve reports.

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

CHAPTER 2

Installation

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

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 interfaces
- 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 now import certificates through the Device Manager by employing the Setup wizard or by command line. *See* Import Certificates, page 3-38

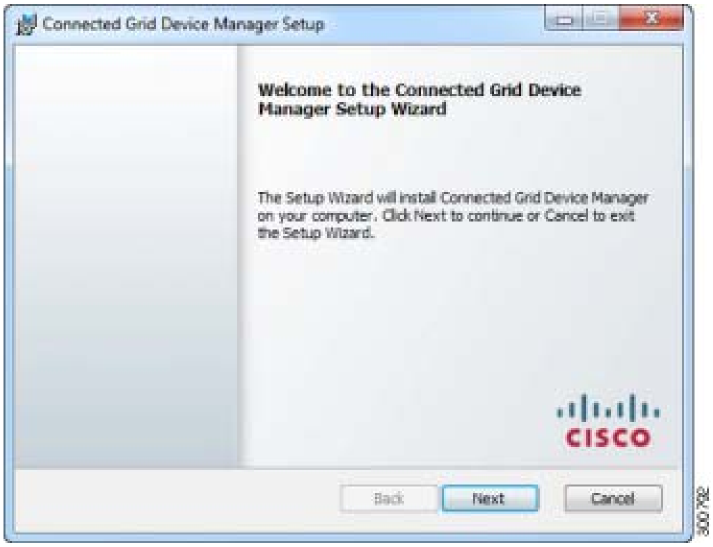
When the Device Manager cannot locate a valid Certificate Common Name in the registry, the Device Manager launches the Settings page to import a certificate.

Device Manager Installation

Follow these steps to install the Device Manager:

Step 1 Double-click CGDManager executable to start installation.

Step 2 Click **Next**.

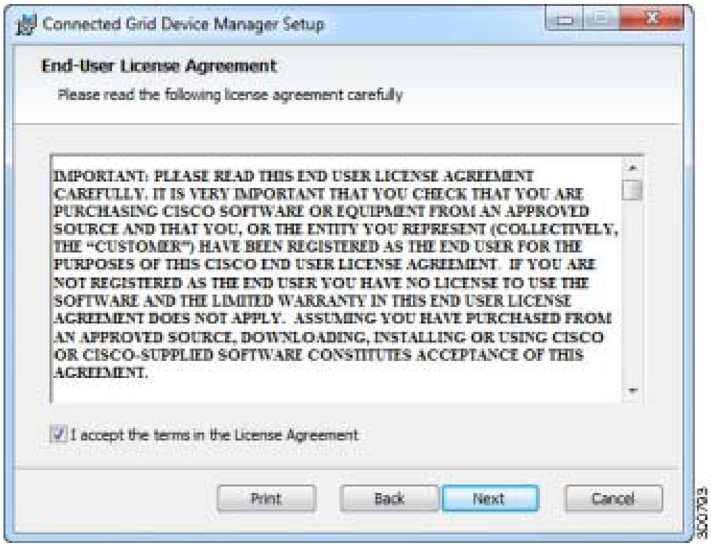


Connected Grid Device Manager Setup

Welcome to the Connected Grid Device Manager Setup Wizard

The Setup Wizard will install Connected Grid Device Manager on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



End-User License Agreement

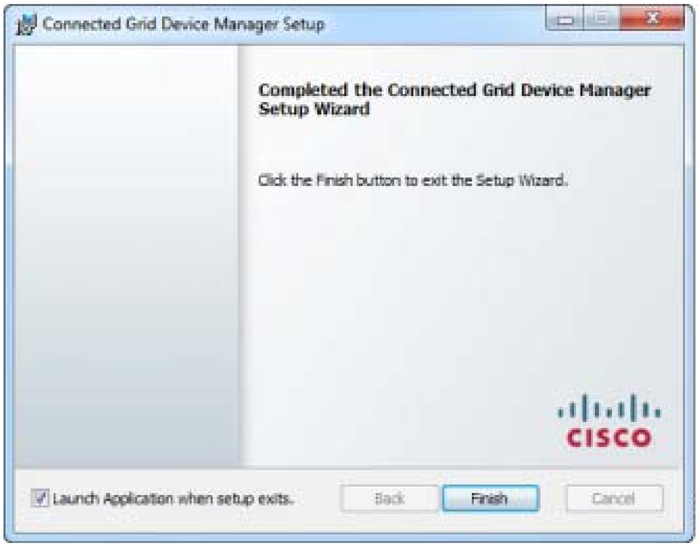
Please read the following license agreement carefully

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

☑ I accept the terms in the License Agreement

300793

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



Completed the Connected Grid Device Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch Application when setup exits.

300794

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.

CHAPTER 3

Using the Device Manager

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

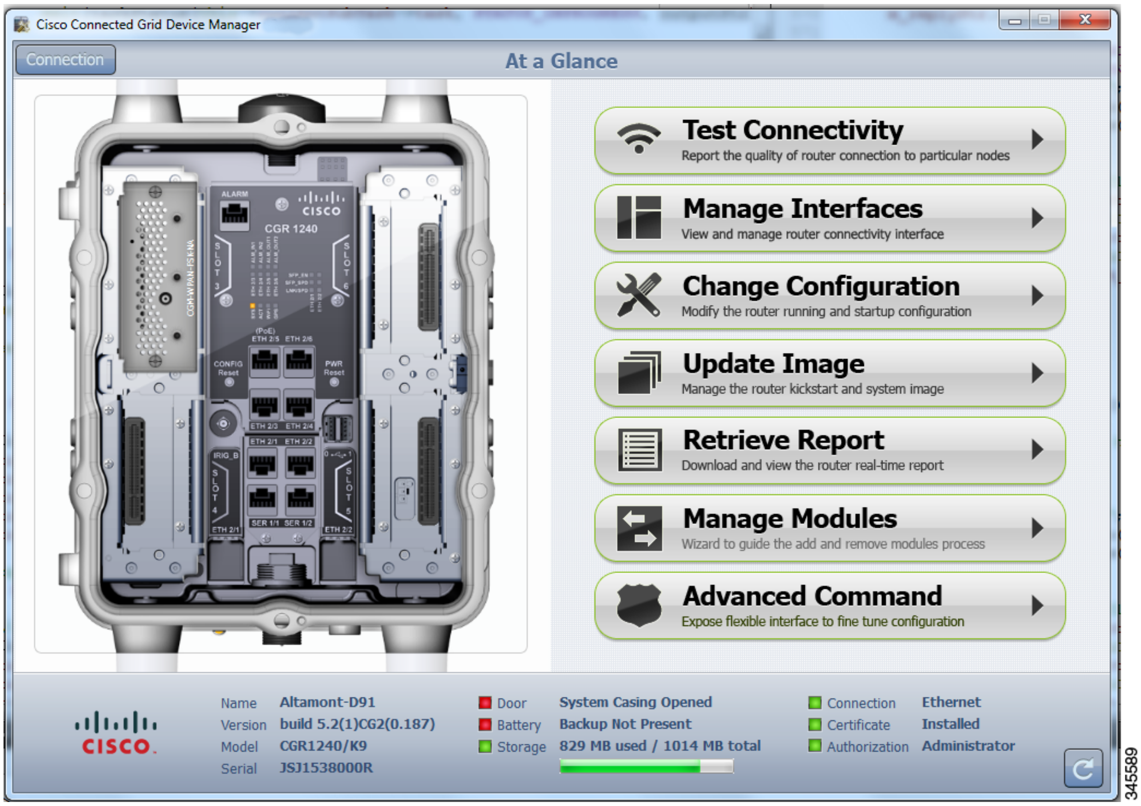
Overview

The At a Glance page displays 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 3-16
- **Manage Interfaces**: Bring up or shut down an CGR 1000 interface. *See* Manage Interfaces, page 3-21
- **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 3-25
- **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 3-28
- **Retrieve Report:** Download and view the CGR 1000 system logs. *See* Retrieve Report, page 3-31
- **Manage Modules:** Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. *See* Manage Modules, page 3-32

- **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 3-37

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


Cisco Connected Grid Device Manager
Connection
At a Glance
Test Connectivity
Report the quality of router connection to particular nodes
Manage Interfaces
View and manage router connectivity interface
Change Configuration
Modify the router running and startup configuration
Update Image
Manage the router kickstart and system image
Retrieve Report
Download and view the router real-time report
Manage Modules
Wizard to guide the add and remove modules process
Advanced Command
Expose flexible interface to fine tune configuration
CGR 1240
345589

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				

The CGR 1000 image that displays with the At a Glance page, provides a view of the CGR 1000 router to which the Device Manager connects (left-side). The CGR 1000 image also displays the Connected Grid Modules installed, as well as LEDs which 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 at 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 3-16
  - When you reconnect to the devices, review the CGR 1000 configuration information. *See* Advanced Command, page 3-37
  - When the configuration information is incorrect, you can update the configuration at Update Configuration File, page 3-26 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 3-37) 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 3-28
- 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
- (CGR 1240 Only) The door of the CGR 1240 is open. Start the Device Manager and check the status of the door (bottom panel 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-hand) 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 3-32

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.

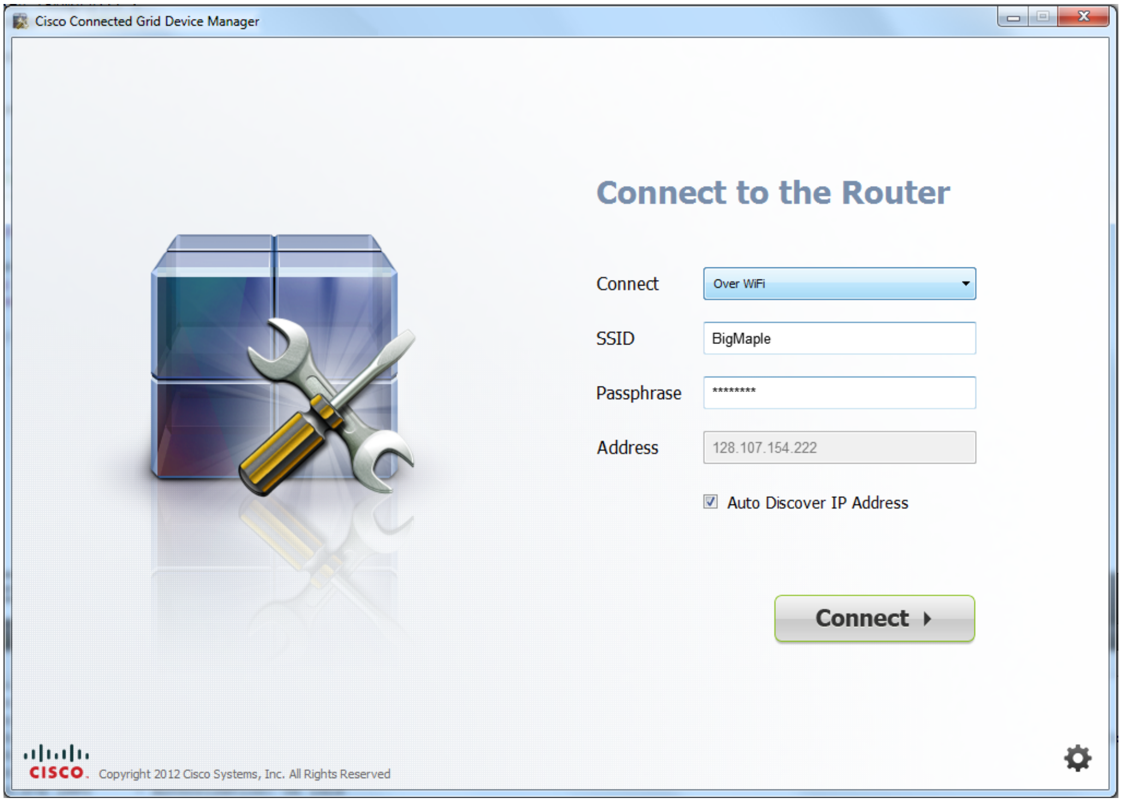
Connect to the Device Manager by employing one of the following methods:

- 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 Router page.



Connect to the Router

Connect: Over WiFi

SSID: BigMaple

Passphrase: ********

Address: 128.107.154.222

☑ Auto Discover IP Address

Copyright 2012 Cisco Systems, Inc. All Rights Reserved

Step 2 At 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 At 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 at the bottom-right of the Router page. Non-NMS is the default setting.

  The Setup Wizard panel 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 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:

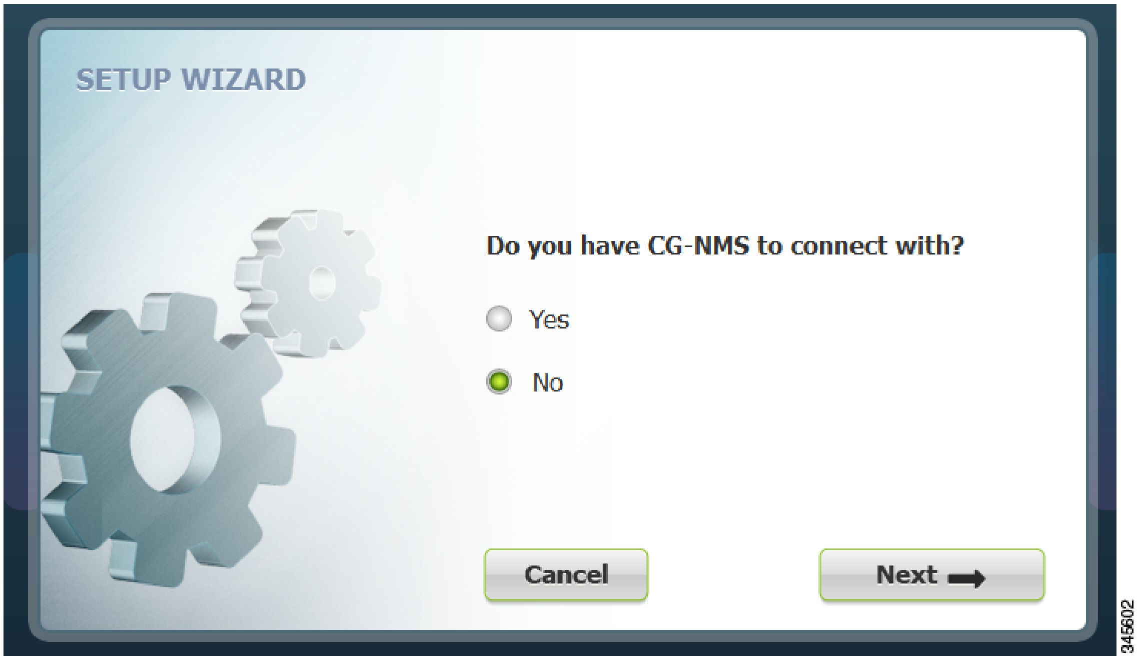
NMS Mode–When you have a CG-NMS operating in the network, you can connect to that system with the Device Manager to download and update work authorizations. Work authorizations allow the Device Manager to view status and perform tasks on the CGR 1000. To operate in conjunction with a CG-NMS system, configure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

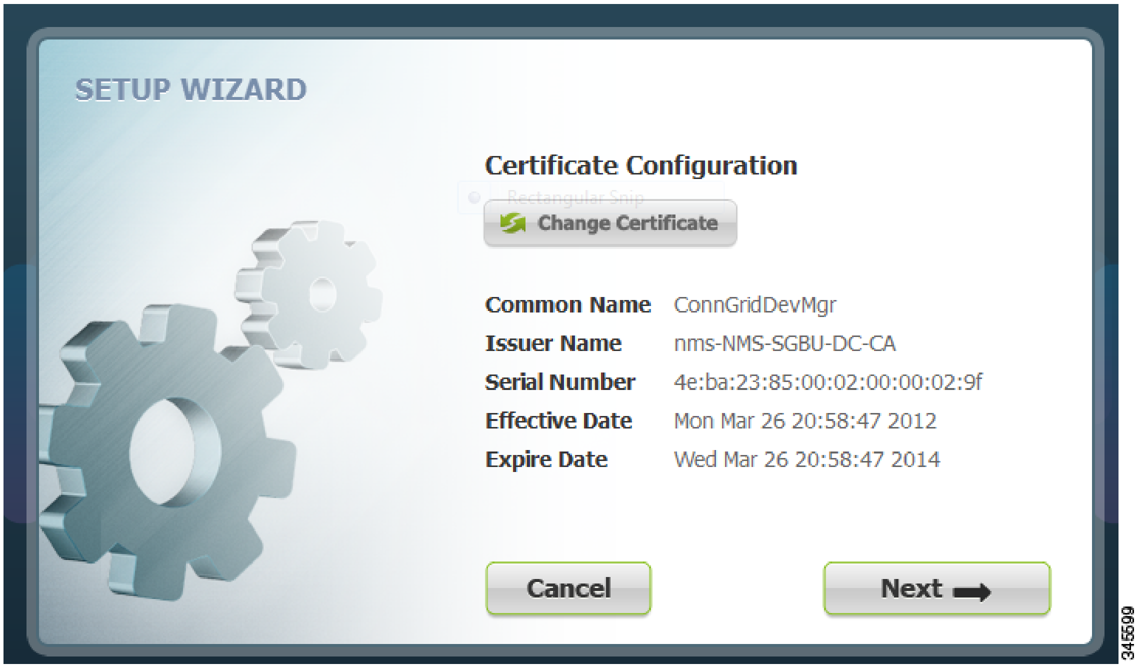

SETUP WIZARD

Do you have CG-NMS to connect with?

○ Yes

● No

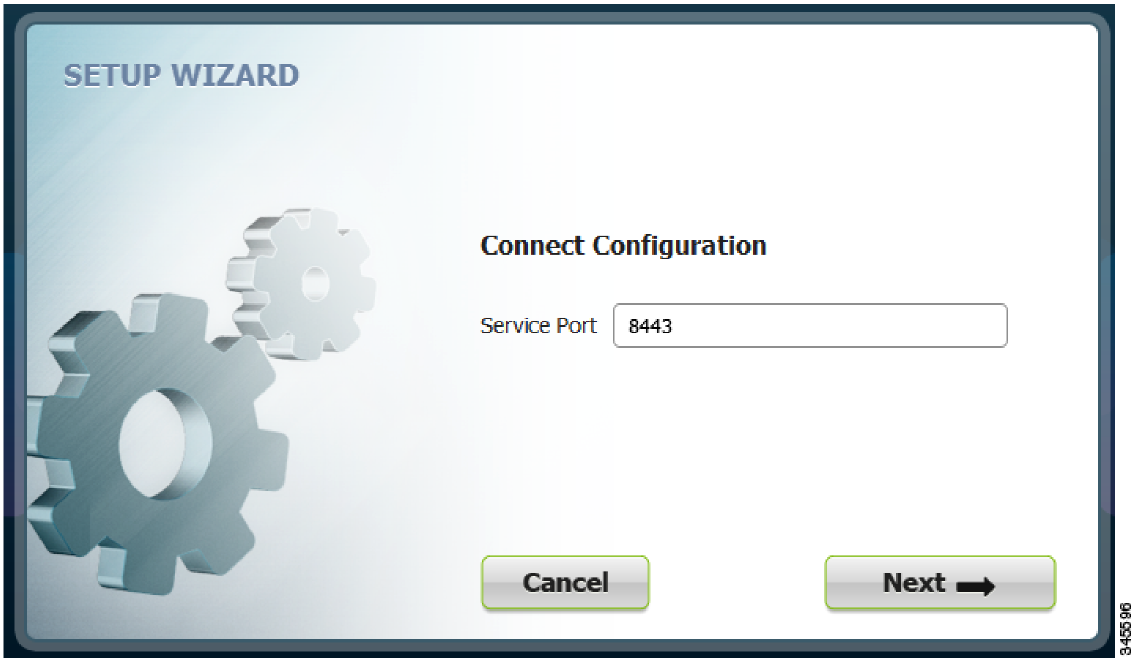
Step 2 (Non-NMS mode) At the Certificate Configuration panel that appears, review the Common Name and its details for accuracy and do the following:



Certificate Configuration

Common Name	ConnGridDevMgr
Issuer Name	nms-NMS-SGBU-DC-CA
Serial Number	4e:ba:23:85:00:02:00:00:02:9f
Effective Date	Mon Mar 26 20:58:47 2012
Expire Date	Wed Mar 26 20:58:47 2014

- 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**.

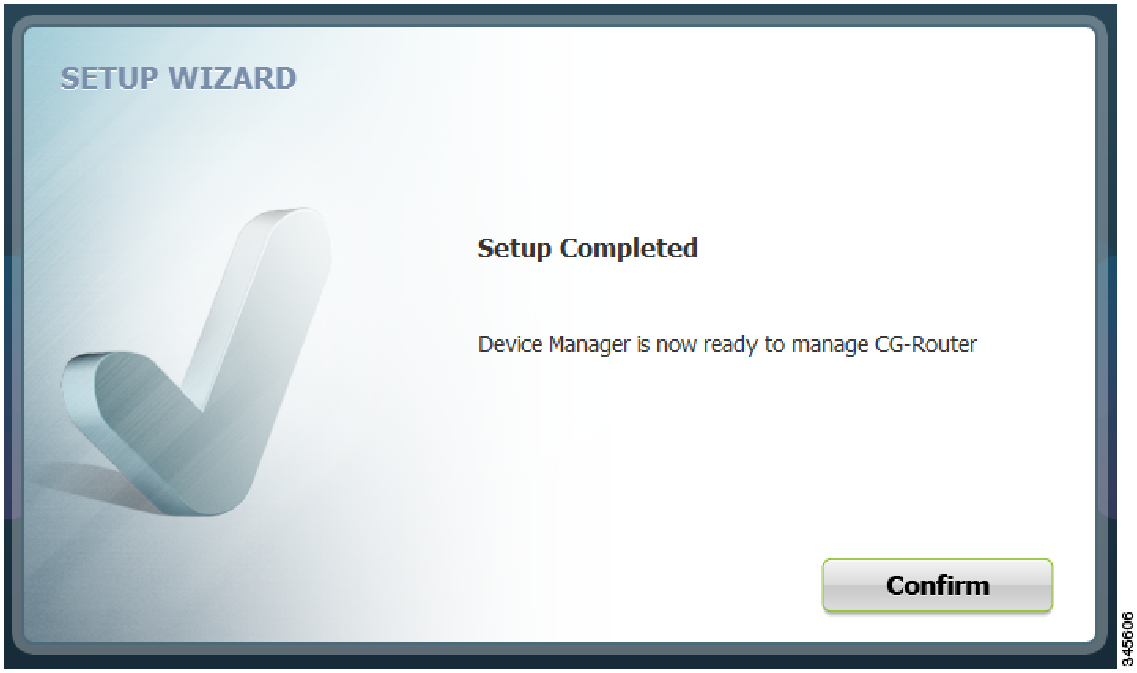


Connect Configuration

Service Port 8443

a. At the Connect Configuration panel that appears, confirm the Service Port and click **Next**.

b. At the Setup Completed panel, click **Confirm**.



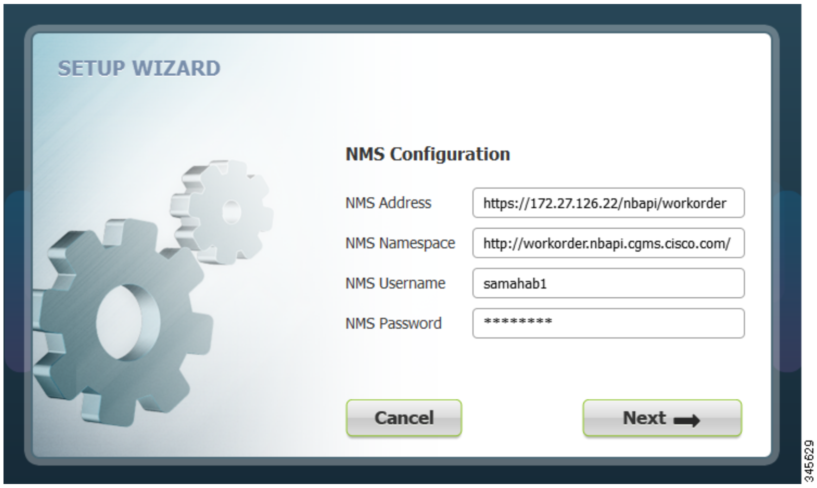
Setup Completed

Device Manager is now ready to manage CG-Router

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

The At a Glance page appears. Proceed to Performing Tasks on the Router.

Step 3 (CG-NMS mode) At the NMS Configuration panel, do the following:



NMS Configuration

NMS Address: https://172.27.126.22/nbapi/workorder

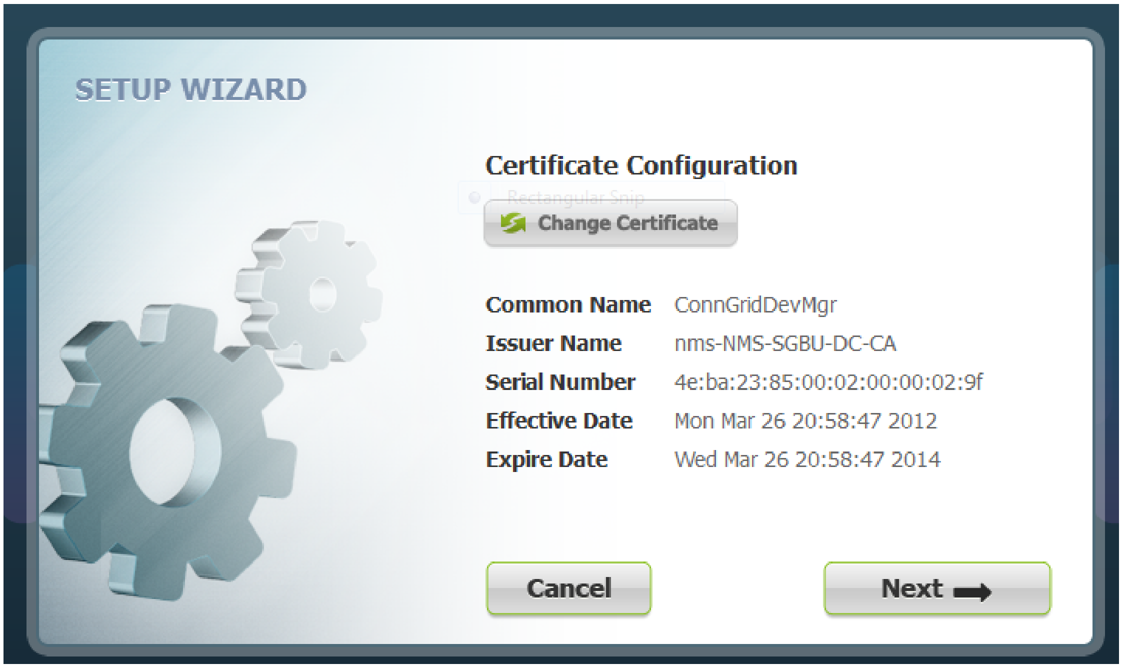
NMS Namespace: http://workorder.nbapi.cgms.cisco.com/

NMS Username: samahab1

NMS Password: ********

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. At the Certificate Configuration panel, review the certificate details, and do one of the following:

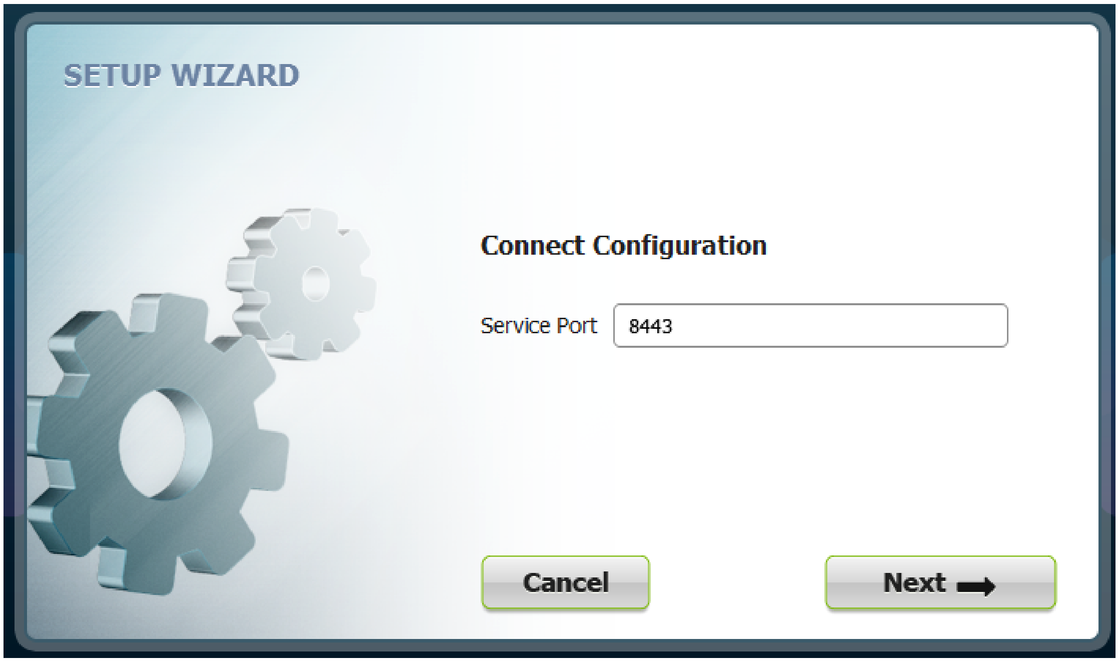


Certificate Configuration

Common Name	ConnGridDevMgr
Issuer Name	nms-NMS-SGBU-DC-CA
Serial Number	4e:ba:23:85:00:02:00:00:02:9f
Effective Date	Mon Mar 26 20:58:47 2012
Expire Date	Wed Mar 26 20:58:47 2014

- 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**.

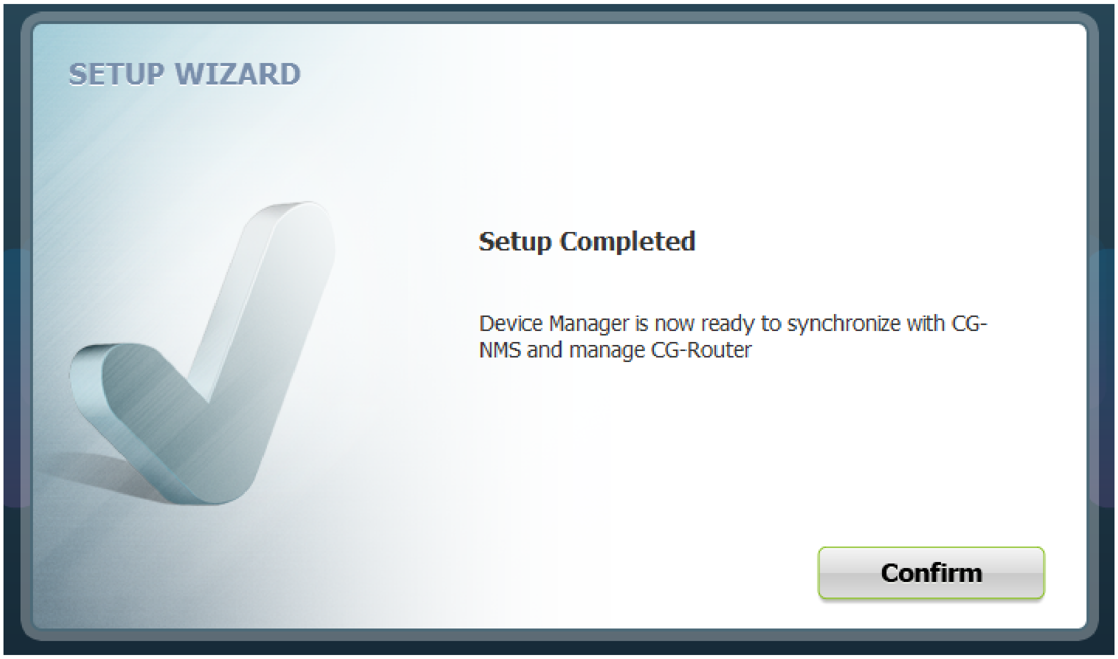
c. At the Connect Configuration panel, confirm the Service Port and click **Next**.



Connect Configuration

Service Port 8443

d. At the Setup Completed panel, click **Confirm**.



Setup Completed

Device Manager is now ready to synchronize with CG-NMS and manage CG-Router

e. At the Work Authorization page that appears, click **Confirm**. Proceed to Accessing Work Authorizations.

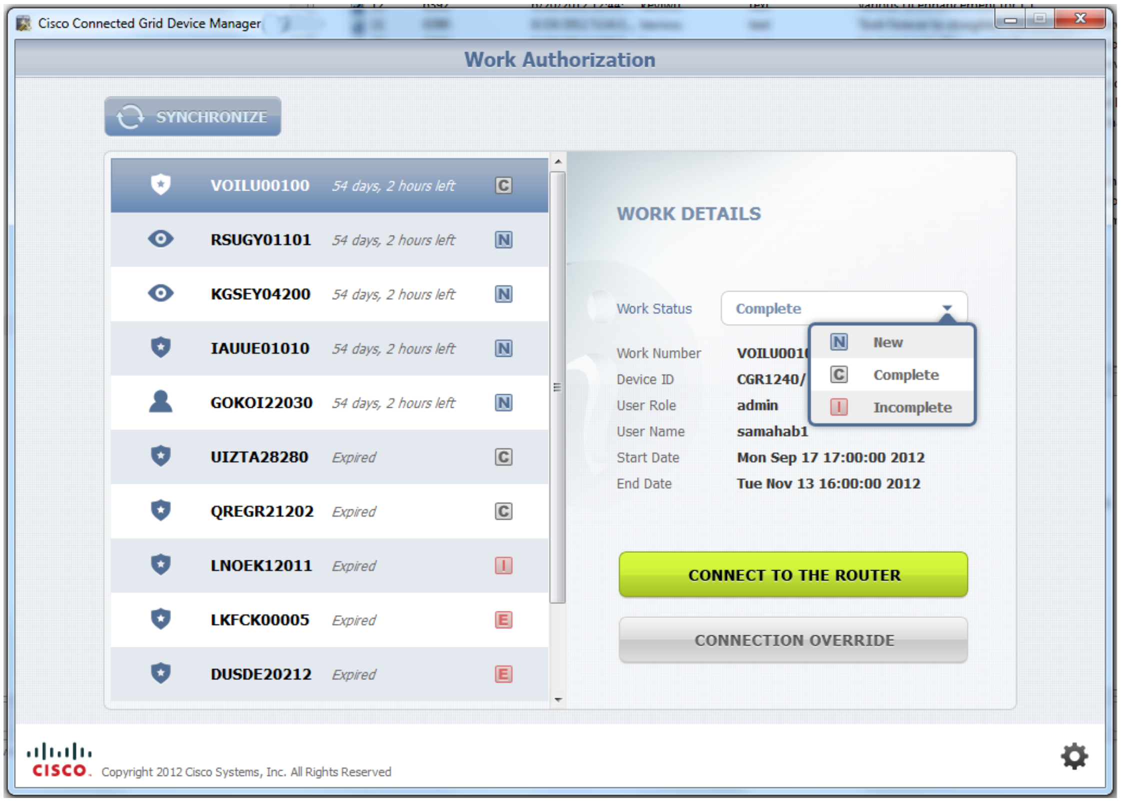
Accessing Work Authorizations

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).



VOILU00100	54 days, 2 hours left	C
RSUGY01101	54 days, 2 hours left	N
KGSEY04200	54 days, 2 hours left	N
IAUUE01010	54 days, 2 hours left	N
GOKOI22030	54 days, 2 hours left	N
UIZTA28280	Expired	C
QREGR21202	Expired	C
LNOEK12011	Expired	I
LKFCK00005	Expired	E
DUSDE20212	Expired	E

Work Status	Complete
Work Number	VOILU0010
Device ID	CGR1240/
User Role	admin
User Name	samahab1
Start Date	Mon Sep 17 17:00:00 2012
End Date	Tue Nov 13 16:00:00 2012

Copyright 2012 Cisco Systems, Inc. All Rights Reserved

345628

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 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 day-end when back at the office to update CG-NMS with the changes.

To view work order details, do the following:

Step 1 At the Work Authorization page, click a work order (left-pane).

Step 2 Using the Work Number that displays (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 At the Work Authorization page, select the Work Status drop-down menu (right-pane).

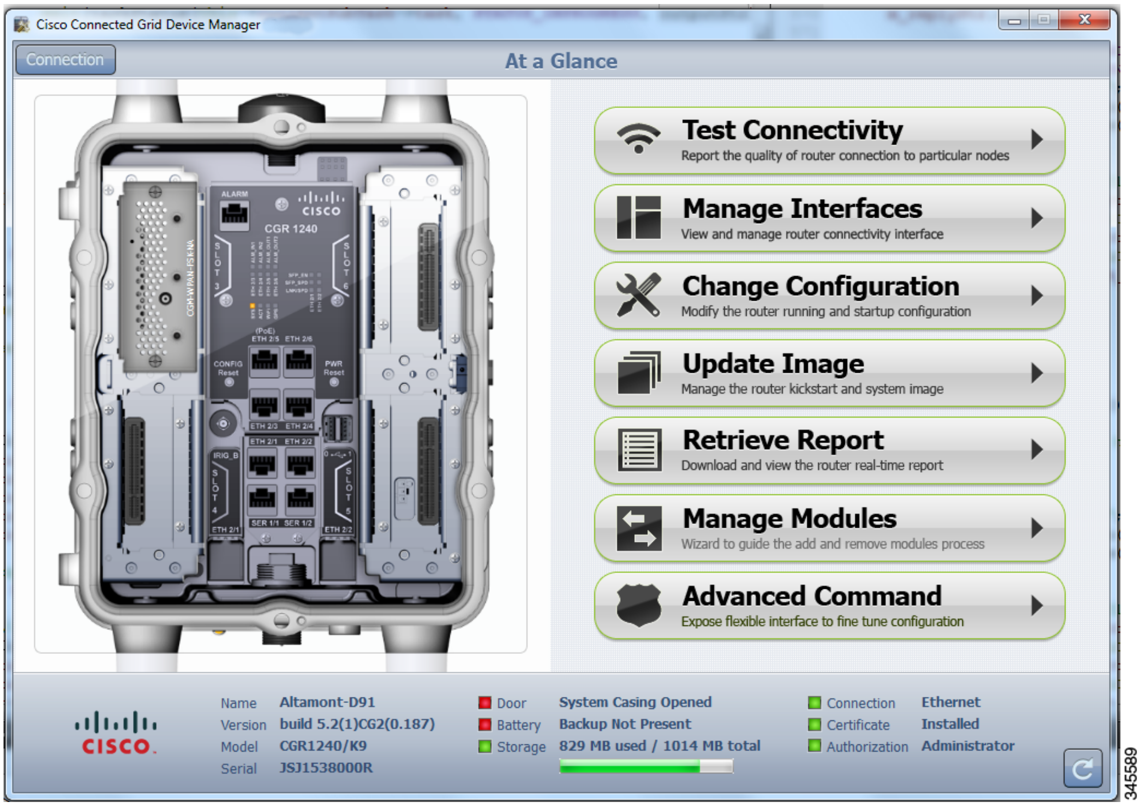
Step 2 Select the current state of the work order.

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 displays after you click **Connect** from the Connect to Router page (Non-NMS mode) or click **Connect to the Router** from the Work Authorization page (NMS mode).



At a Glance

Test Connectivity — Report the quality of router connection to particular nodes

Manage Interfaces — View and manage router connectivity interface

Change Configuration — Modify the router running and startup configuration

Update Image — Manage the router kickstart and system image

Retrieve Report — Download and view the router real-time report

Manage Modules — Wizard to guide the add and remove modules process

Advanced Command — Expose flexible interface to fine tune configuration

Name Altamont-D91
Version build 5.2(1)CG2(0.187)
Model CGR1240/K9
Serial JSJ1538000R

🟥 Door System Casing Opened
🟥 Battery Backup Not Present
🟩 Storage 829 MB used / 1014 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

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

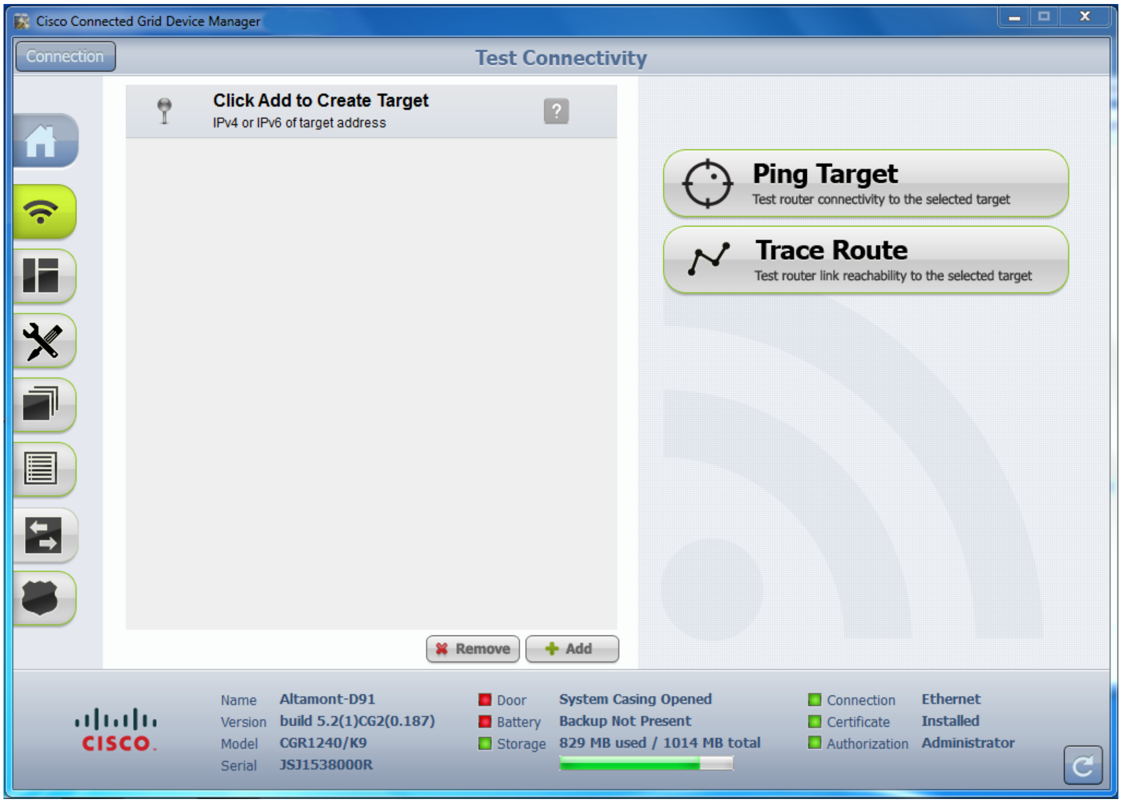
- Troubleshoot connectivity between a CGR 1000 and the devices connected to the router. *See* Test Connectivity, page 3-16
- Bring up or shut down an CGR 1000 interface. *See* Manage Interfaces, page 3-21
- Check and update the current CGR 1000 configuration.

  See Change Configuration, page 3-25 and Advanced Command, page 3-37
- Upload and/or update the CGR 1000 image and reset the router. *See* Update Image, page 3-28
- View real-time CGR 1000 configuration log for troubleshooting. *See* Retrieve Report, page 3-31
- Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. *See* Manage Modules, page 3-32
- Use advanced commands to troubleshoot the CGR 1000. *See* Advanced Command, page 3-37

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.


Cisco Connected Grid Device Manager
Connection
Test Connectivity
Click Add to Create Target
IPv4 or IPv6 of target address
?
Ping Target
Test router connectivity to the selected target
Trace Route
Test router link reachability to the selected target
Remove
Add
CISCO

Name Altamont-D91
Version build 5.2(1)CG2(0.187)
Model CGR1240/K9
Serial JSJ1538000R

🟥 Door System Casing Opened
🟥 Battery Backup Not Present
🟩 Storage 829 MB used / 1014 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

345607

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

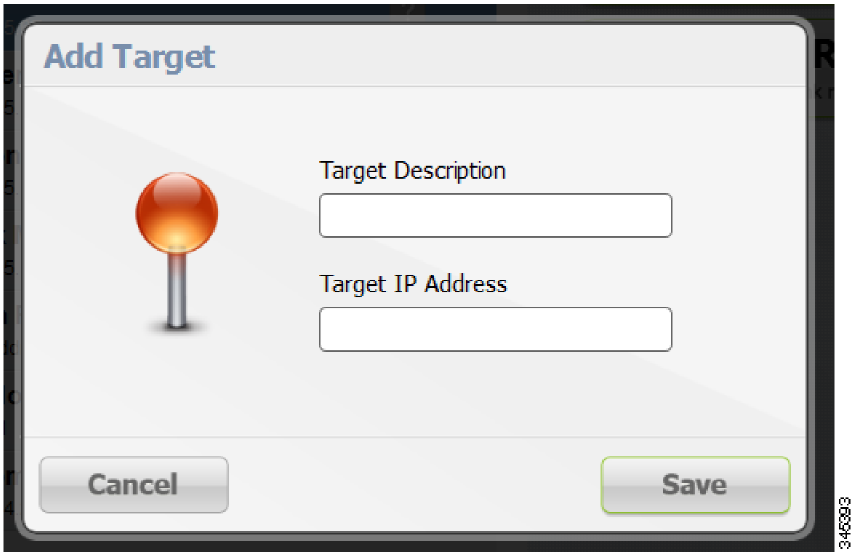
Follow these steps to add a device IP address:

Step 1 From the At a Glance page, click **Test Connectivity**.

The opening page displays the defined sample devices and/or target addresses.

Step 2 Click **Add** to create a target IP address.

An entry panel appears to enter the target description and address for the device.



Step 3 In the Target Description field, enter a description of 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

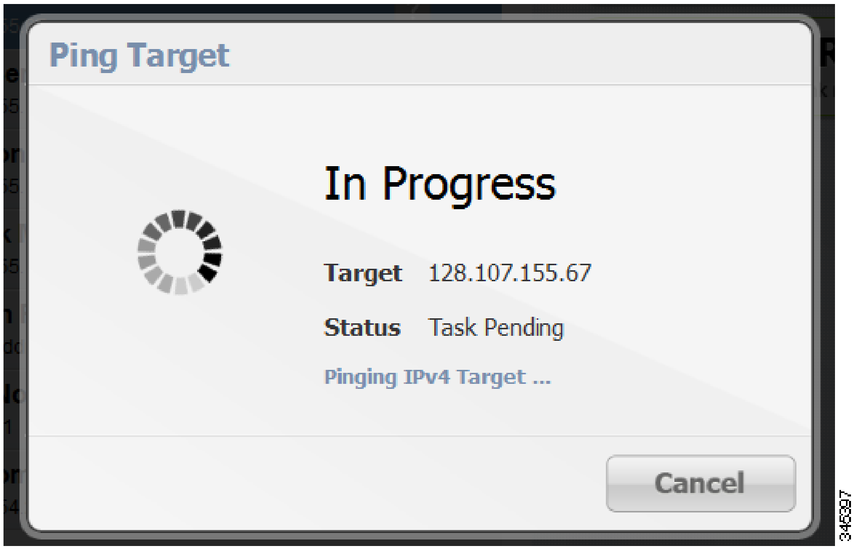
The Ping feature allows you to verify connectivity to a device by querying the target IP address.

Follow these steps to test connectivity between the CGR 1000 and the device:

Step 1 At the Test Connectivity page, click on a target IP address from the listing on the page (left-pane).

Step 2 Click **Ping Target**.

An In Progress panel displays.



Ping Target

In Progress

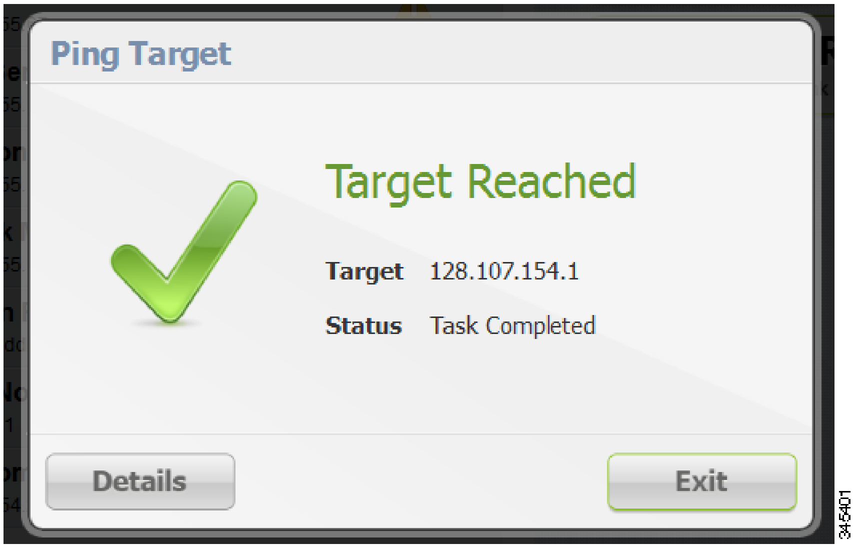
Target 128.107.155.67

Status Task Pending

Pinging IPv4 Target ...

When the system successfully pings the device the Target Reached panel appears.

When the system does not successfully ping a device, refer to Failed Ping, page 3-19.



Ping Target

Target Reached

Target 128.107.154.1

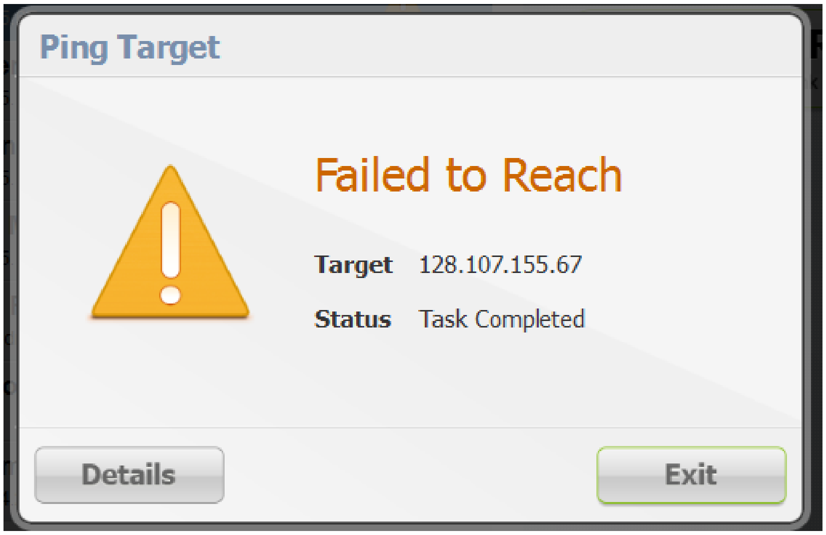
Status Task Completed

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 At the Failed to Reach panel, click **Details** to view the reason the system could not reach the IP address.

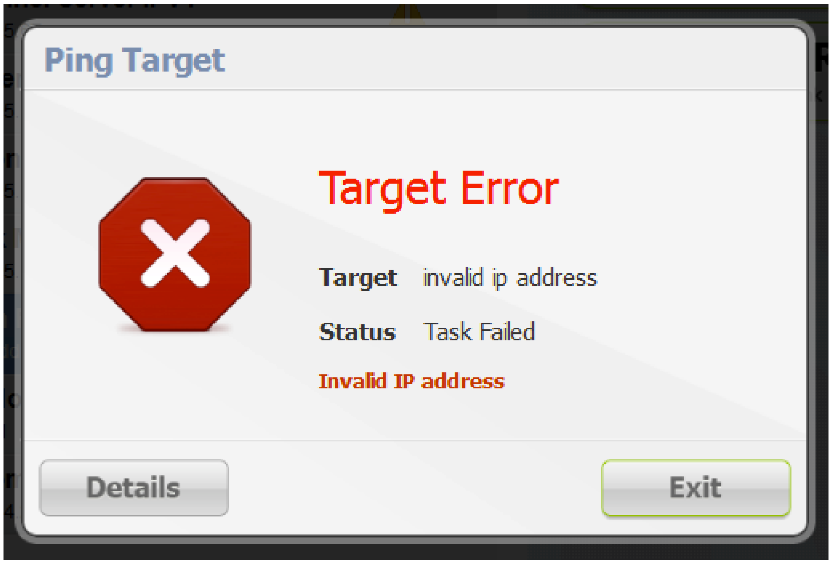


Ping Target

Failed to Reach

Target 128.107.155.67

Status Task Completed



Ping Target

Target Error

Target invalid ip address

Status Task Failed

Invalid IP address

Step 2 At the Target Error page, click **Exit** after reviewing the reason for the error.

Proceed to Trace Route a Device IP Address, page 3-20.

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 At 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** on the Trace Route panel.
- If the trace route is unsuccessful, proceed to Remove a Device IP Address, page 3-20.

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 At the Test Connectivity page, select the target IP address from the list.

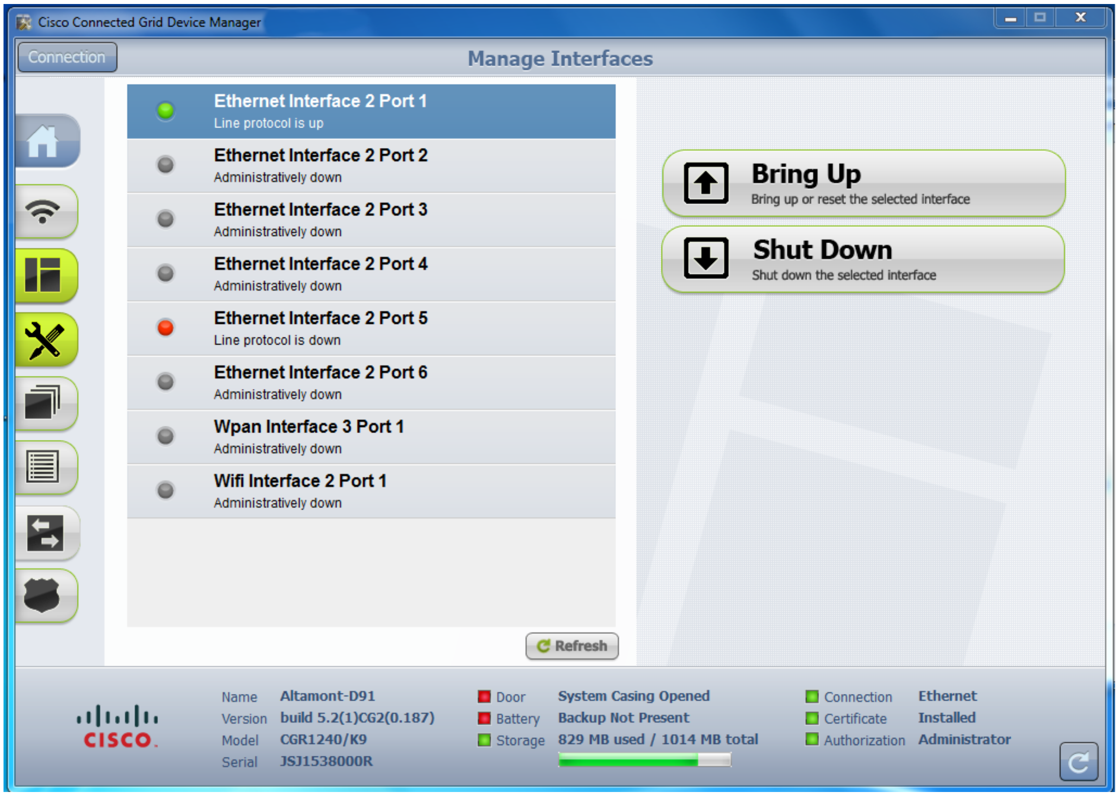
Step 2 Click **Remove**.

Manage Interfaces

You can bring up or shut down an interface on the Manage Interfaces page.

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

All interfaces installed within the CGR 1000, display automatically.



● Ethernet Interface 2 Port 1
Line protocol is up

● Ethernet Interface 2 Port 2
Administratively down

● Ethernet Interface 2 Port 3
Administratively down

● Ethernet Interface 2 Port 4
Administratively down

● Ethernet Interface 2 Port 5
Line protocol is down

● Ethernet Interface 2 Port 6
Administratively down

● Wpan Interface 3 Port 1
Administratively down

● Wifi Interface 2 Port 1
Administratively down

Bring Up
Bring up or reset the selected interface

Shut Down
Shut down the selected interface

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				

This section covers the following topics:

- Bring Up an Interface
- Shut Down an Interface

Follow these steps to view or manage selected router interfaces:

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

The opening page displays.

Step 2 Select an interface:

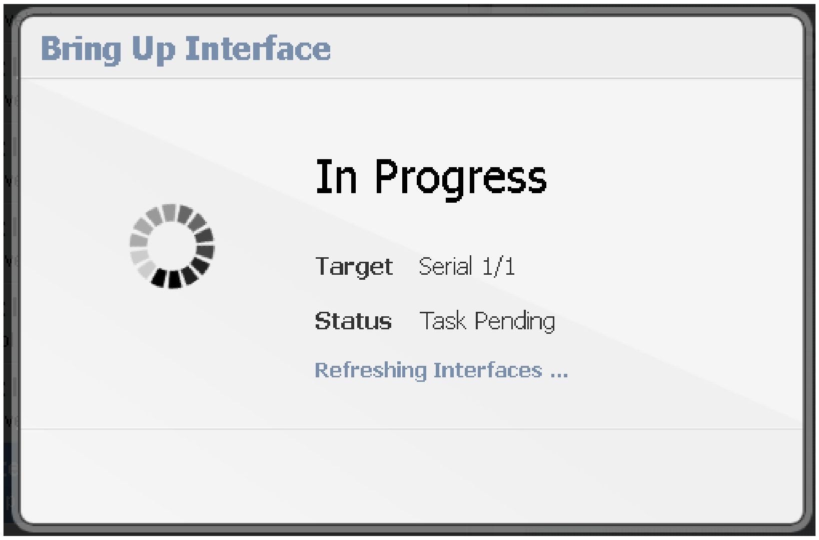
- To bring up an interface, proceed to Bring Up an Interface, page 3-22
- To shut down an interface, proceed to Shut Down an Interface, page 3-23.

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 At the Manage Interfaces page, select an interface and then click **Bring Up Interface**.

The In Progress panel appears. When the interface is up, the Interface Up panel appears.



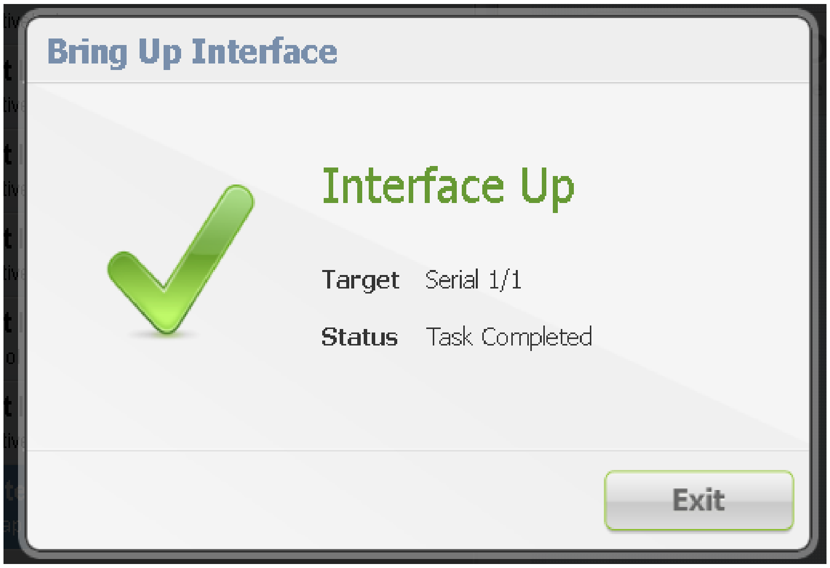
Bring Up Interface

In Progress

Target Serial 1/1

Status Task Pending

Refreshing Interfaces ...



Bring Up Interface

Interface Up

Target Serial 1/1

Status Task Completed

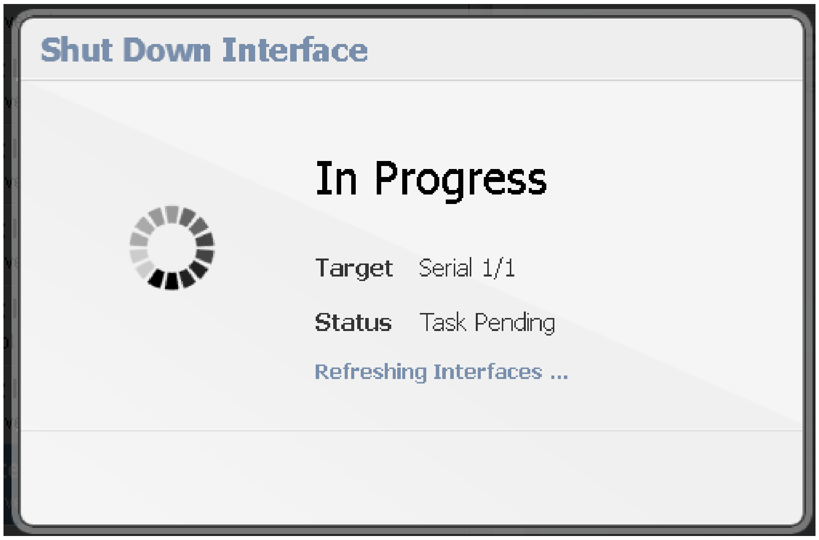
Shut Down an Interface

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 At the Manage Interfaces page, select an interface and then click **Shut Down**.

The In Progress panel appears. When the process completes, the Interface Down panel appears.



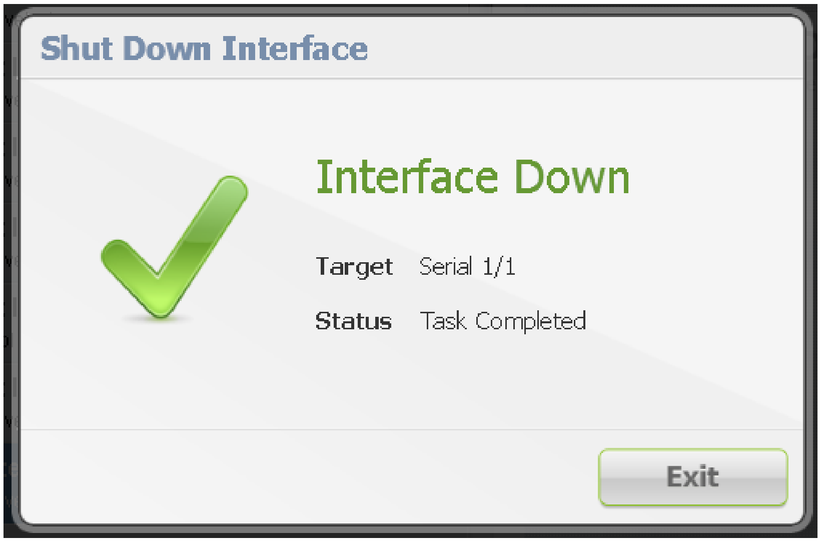
Shut Down Interface

In Progress

Target Serial 1/1

Status Task Pending

Refreshing Interfaces ...



Shut Down Interface

Interface Down

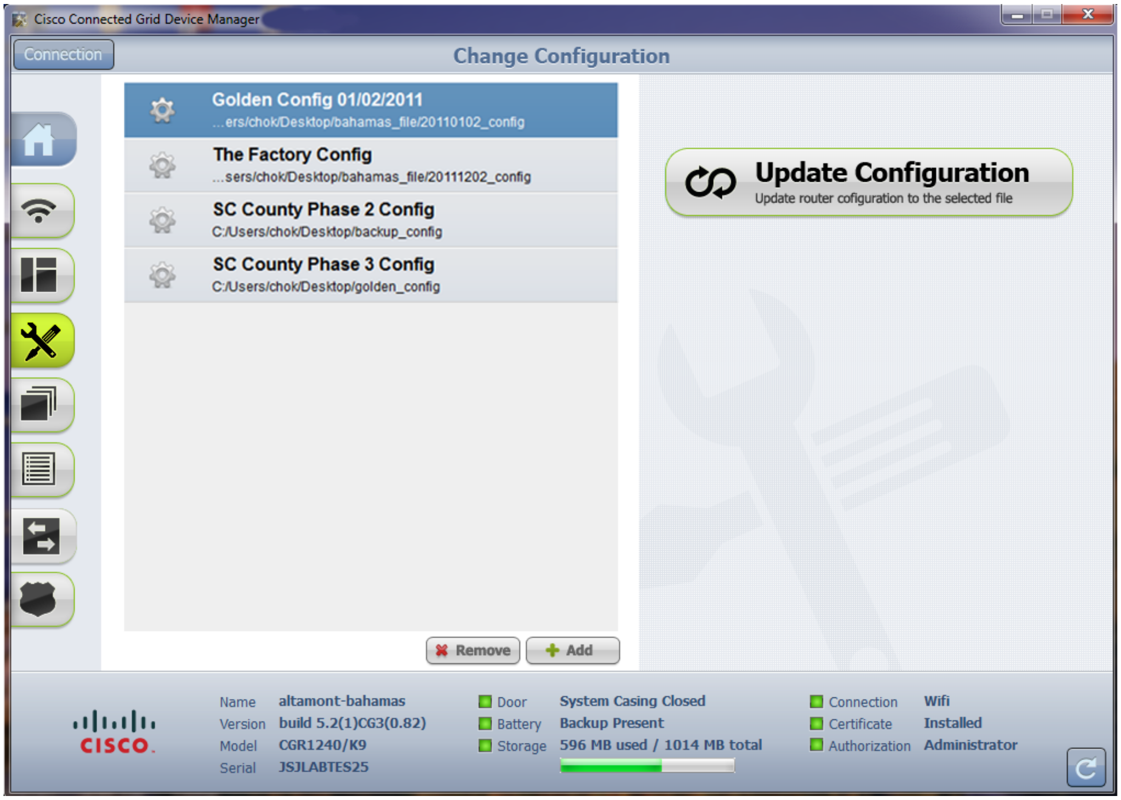
Target Serial 1/1

Status Task Completed

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.


Cisco Connected Grid Device Manager
Connection
Change Configuration
Update Configuration
Update router cofiguration to the selected file
Remove
Add
CISCO
345595

Golden Config 01/02/2011
...ers/chok/Desktop/bahamas_file/20110102_config

The Factory Config
...sers/chok/Desktop/bahamas_file/20111202_config

SC County Phase 2 Config
C:/Users/chok/Desktop/backup_config

SC County Phase 3 Config
C:/Users/chok/Desktop/golden_config

Name altamont-bahamas
Version build 5.2(1)CG3(0.82)
Model CGR1240/K9
Serial JSJLABTES25

Door System Casing Closed
Battery Backup Present
Storage 596 MB used / 1014 MB total

Connection Wifi
Certificate Installed
Authorization Administrator

This section covers the following topics:

- Add a Configuration File
- Update Configuration File
- Correct a Configuration File
- Remove Configuration File

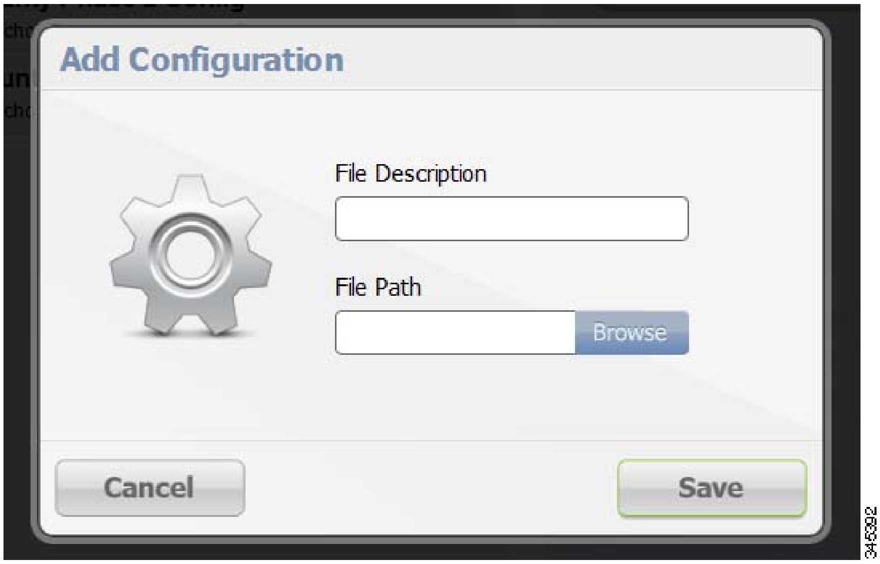
Add a Configuration File

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**.

An entry panel appears.



Step 3 At the Add Configuration panel:

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 File

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

Caution Updating 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.

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

Step 1 At the Change Configuration page, select the desired configuration file (left-pane).

Step 2 Click **Update Configuration**.

- If a confirmation panel appears, click **Confirm** to verify that you would like to change the router configuration.
- If an error panel 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 3-27

Step 3 Add the updated configuration file to Device Manager. *See* Add a Configuration File

Step 4 Update the configuration file. *See* Update Configuration File.

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.

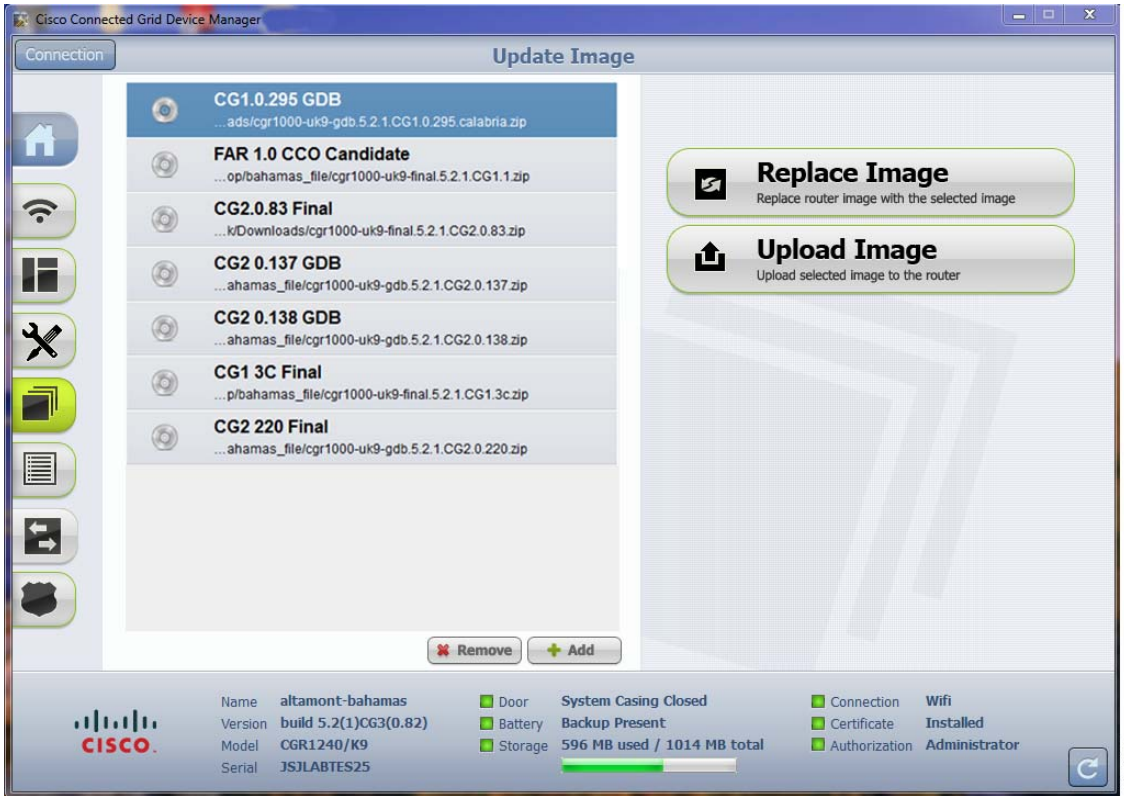
Follow these steps to remove a configuration file:

Step 1 At 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.


Cisco Connected Grid Device Manager
Connection
Update Image
Replace Image
Replace router image with the selected image
Upload Image
Upload selected image to the router
Remove
Add
CISCO
345608

CG1.0.295 GDB
...ads/cgr1000-uk9-gdb.5.2.1.CG1.0.295.calabria.zip

FAR 1.0 CCO Candidate
...op/bahamas_file/cgr1000-uk9-final.5.2.1.CG1.1.zip

CG2.0.83 Final
...k/Downloads/cgr1000-uk9-final.5.2.1.CG2.0.83.zip

CG2 0.137 GDB
...ahamas_file/cgr1000-uk9-gdb.5.2.1.CG2.0.137.zip

CG2 0.138 GDB
...ahamas_file/cgr1000-uk9-gdb.5.2.1.CG2.0.138.zip

CG1 3C Final
...p/bahamas_file/cgr1000-uk9-final.5.2.1.CG1.3c.zip

CG2 220 Final
...ahamas_file/cgr1000-uk9-gdb.5.2.1.CG2.0.220.zip

Name altamont-bahamas
Version build 5.2(1)CG3(0.82)
Model CGR1240/K9
Serial JSJLABTES25

🟩 Door System Casing Closed
🟩 Battery Backup Present
🟩 Storage 596 MB used / 1014 MB total

🟩 Connection Wifi
🟩 Certificate Installed
🟩 Authorization Administrator

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 At 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 tasks 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 At the Update Image page, select an CGR 1000 image.

Step 2 Click **Replace Image**.

A confirmation panel 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:

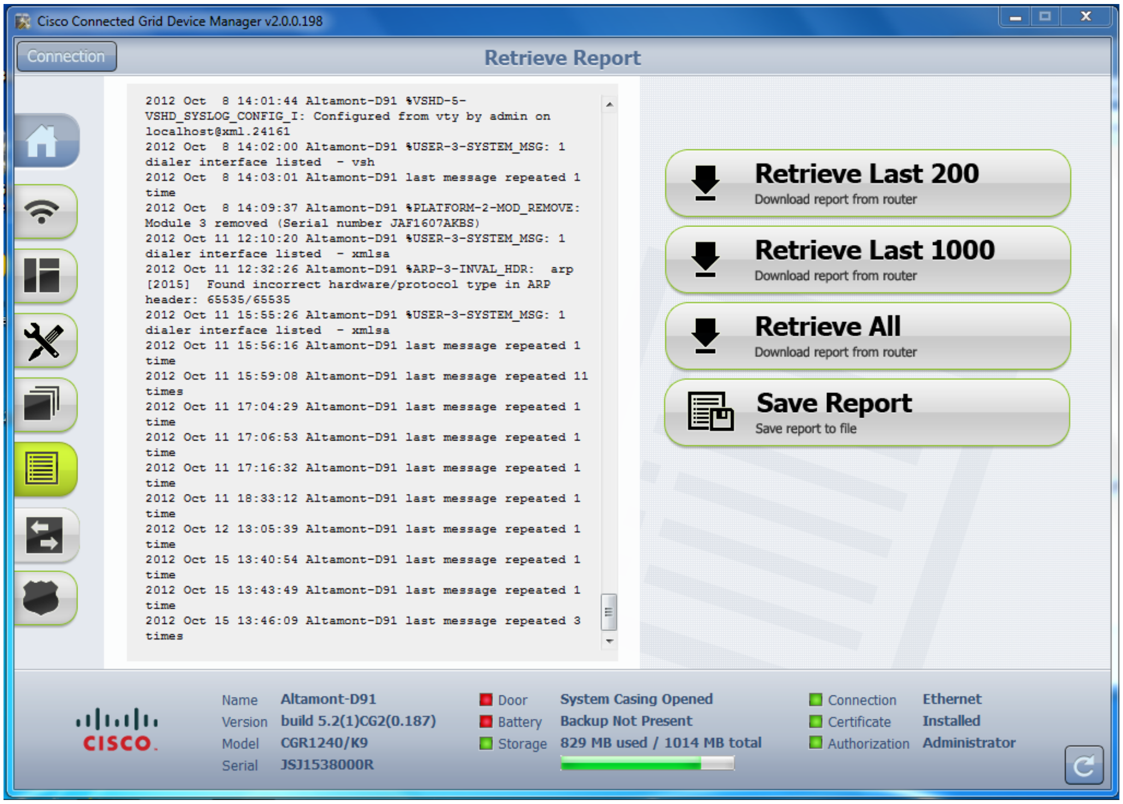
Step 1 At the Update Image page, select an CGR 1000 image.

Step 2 Click **Remove** button (bottom of page).

Retrieve Report

You can retrieve real-time reports log events from the CGR 1000 and view them at 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)


Cisco Connected Grid Device Manager v2.0.0.198
Connection
Retrieve Report
Retrieve Last 200
Download report from router
Retrieve Last 1000
Download report from router
Retrieve All
Download report from router
Save Report
Save report to file
345601

```
2012 Oct  8 14:01:44 Altamont-D91 %VSHD-5-
VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
localhost@xml.24161
2012 Oct  8 14:02:00 Altamont-D91 %USER-3-SYSTEM_MSG: 1
dialer interface listed  - vsh
2012 Oct  8 14:03:01 Altamont-D91 last message repeated 1
time
2012 Oct  8 14:09:37 Altamont-D91 %PLATFORM-2-MOD_REMOVE:
Module 3 removed (Serial number JAF1607AKBS)
2012 Oct 11 12:10:20 Altamont-D91 %USER-3-SYSTEM_MSG: 1
dialer interface listed  - xmlsa
2012 Oct 11 12:32:26 Altamont-D91 %ARP-3-INVAL_HDR:  arp
[2015]  Found incorrect hardware/protocol type in ARP
header: 65535/65535
2012 Oct 11 15:55:26 Altamont-D91 %USER-3-SYSTEM_MSG: 1
dialer interface listed  - xmlsa
2012 Oct 11 15:56:16 Altamont-D91 last message repeated 1
time
2012 Oct 11 15:59:08 Altamont-D91 last message repeated 11
times
2012 Oct 11 17:04:29 Altamont-D91 last message repeated 1
time
2012 Oct 11 17:06:53 Altamont-D91 last message repeated 1
time
2012 Oct 11 17:16:32 Altamont-D91 last message repeated 1
time
2012 Oct 11 18:33:12 Altamont-D91 last message repeated 1
time
2012 Oct 12 13:05:39 Altamont-D91 last message repeated 1
time
2012 Oct 15 13:40:54 Altamont-D91 last message repeated 1
time
2012 Oct 15 13:43:49 Altamont-D91 last message repeated 1
time
2012 Oct 15 13:46:09 Altamont-D91 last message repeated 3
times
```

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				

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 At 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 an example output.

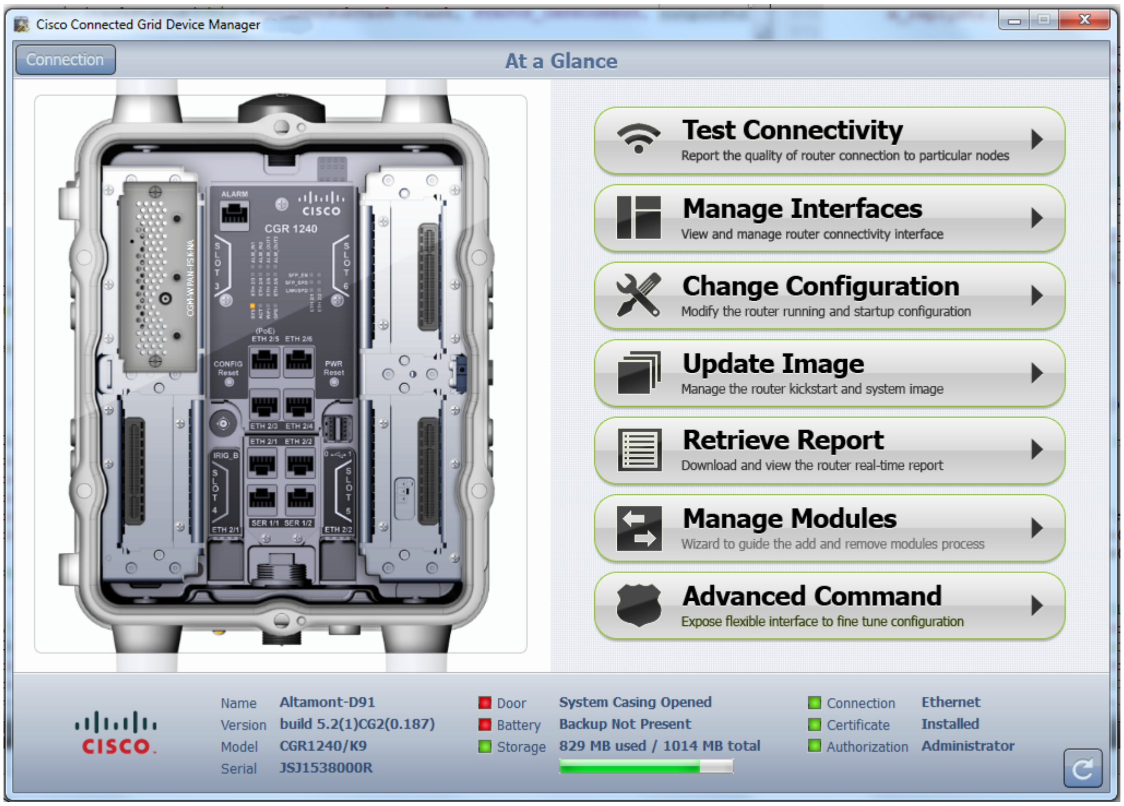
Manage Modules

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.


Cisco Connected Grid Device Manager
Connection
At a Glance
Test Connectivity
Report the quality of router connection to particular nodes
Manage Interfaces
View and manage router connectivity interface
Change Configuration
Modify the router running and startup configuration
Update Image
Manage the router kickstart and system image
Retrieve Report
Download and view the router real-time report
Manage Modules
Wizard to guide the add and remove modules process
Advanced Command
Expose flexible interface to fine tune configuration
CISCO
CGR 1240
345589

Name Altamont-D91
Version build 5.2(1)CG2(0.187)
Model CGR1240/K9
Serial JSJ1538000R

🟥 Door System Casing Opened
🟥 Battery Backup Not Present
🟩 Storage 829 MB used / 1014 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

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
- For details on installing a specific module, refer to the Installation and Configuration Guide for that module at: www.cisco.com/go/cgr1000-docs

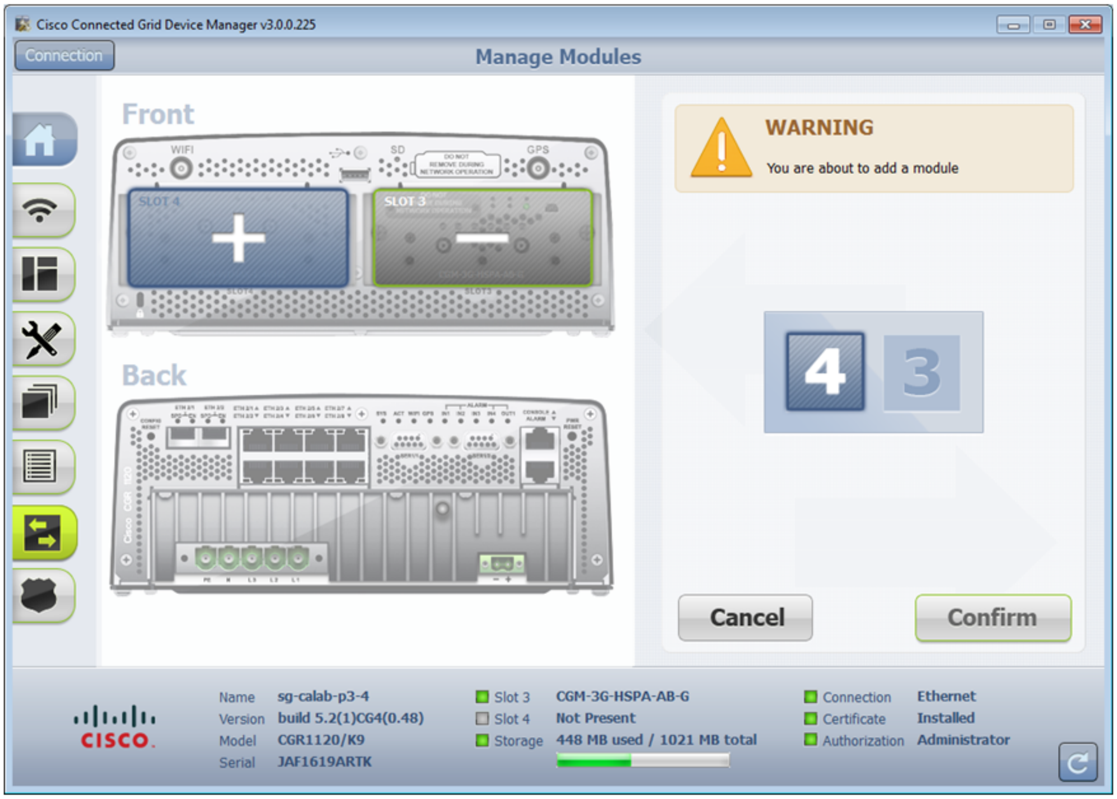
Add a Module

Note You cannot run any other operations when adding the module.

To add a module, do the following:

Step 1 At 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.



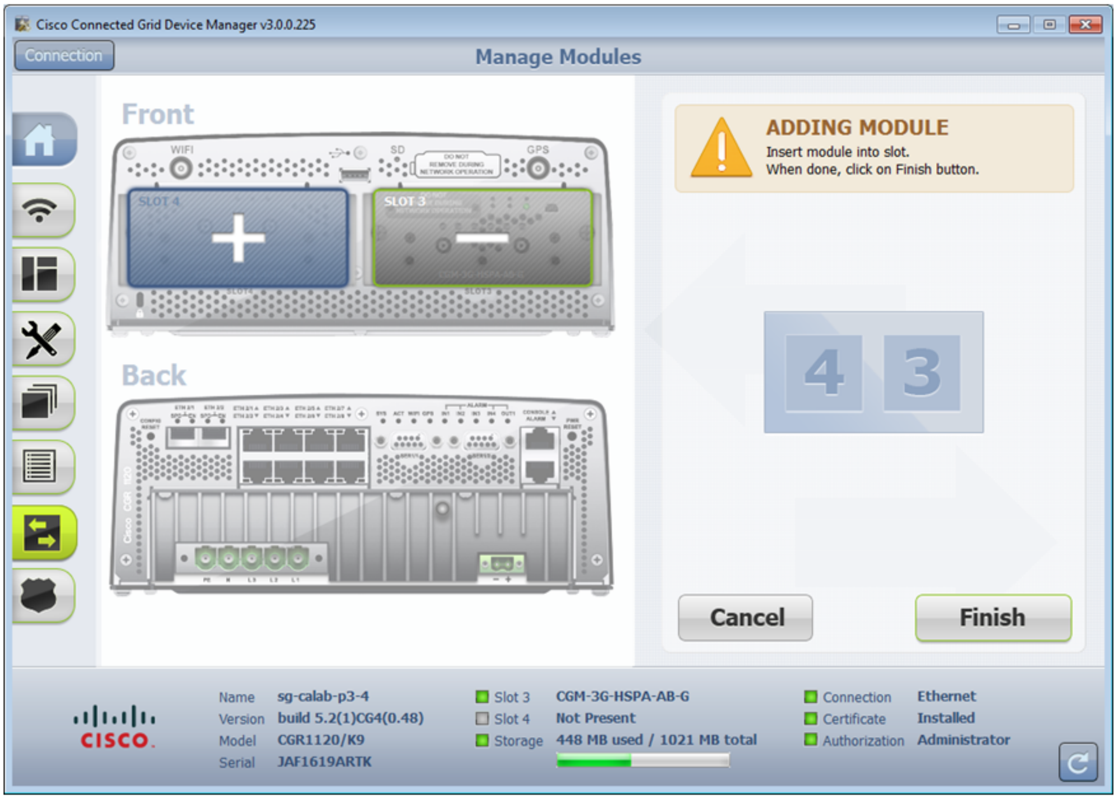
WARNING
You are about to add a module

Name sg-calab-p3-4
Version build 5.2(1)CG4(0.48)
Model CGR1120/K9
Serial JAF1619ARTK

🟩 Slot 3 CGM-3G-HSPA-AB-G
□ Slot 4 Not Present
🟩 Storage 448 MB used / 1021 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

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



ADDING MODULE
Insert module into slot.
When done, click on Finish button.

Name sg-calab-p3-4
Version build 5.2(1)CG4(0.48)
Model CGR1120/K9
Serial JAF1619ARTK

🟩 Slot 3 CGM-3G-HSPA-AB-G
□ Slot 4 Not Present
🟩 Storage 448 MB used / 1021 MB total

🟩 Connection Ethernet
🟩 Certificate Installed
🟩 Authorization Administrator

345673

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

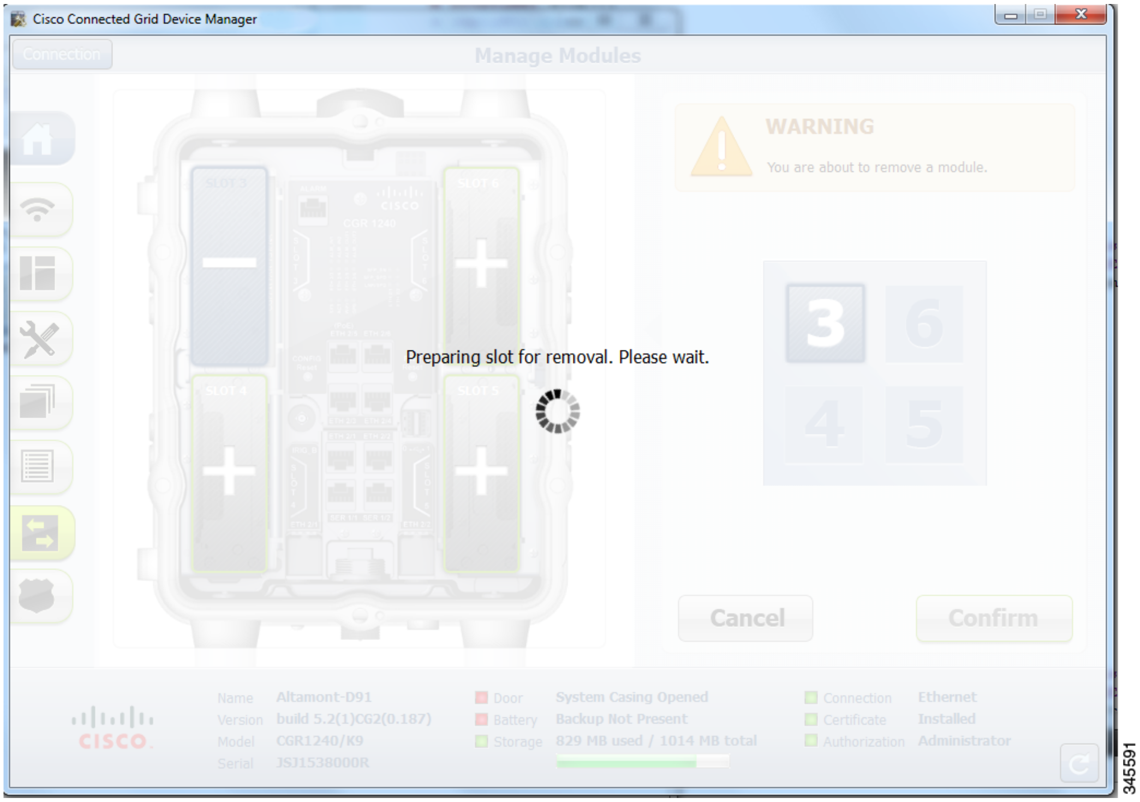
A blue outline appears around the slot in the router diagram to confirm selection, and a Warning message appears stating that you are about to remove a module.

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

The following message appears on the page:

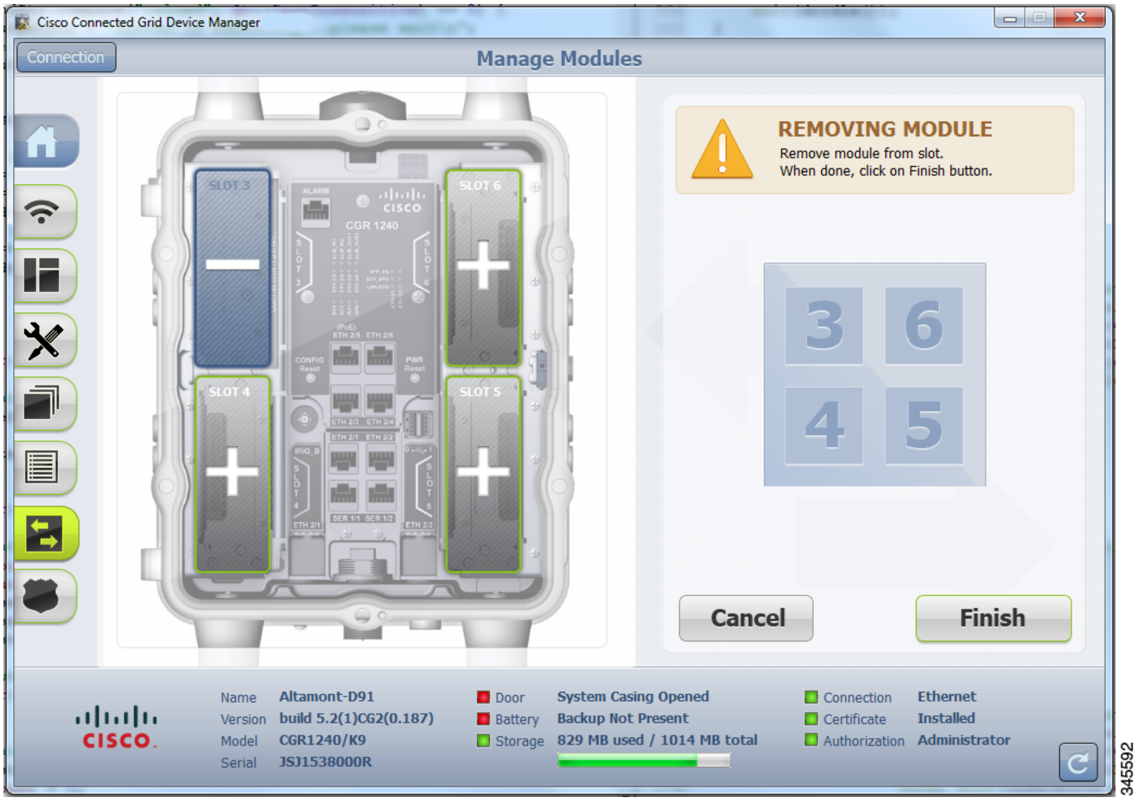
Preparing slot for removal. Please wait.

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



Preparing slot for removal. Please wait.

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				



REMOVING MODULE

Remove module from slot.
When done, click on Finish button.

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				

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:

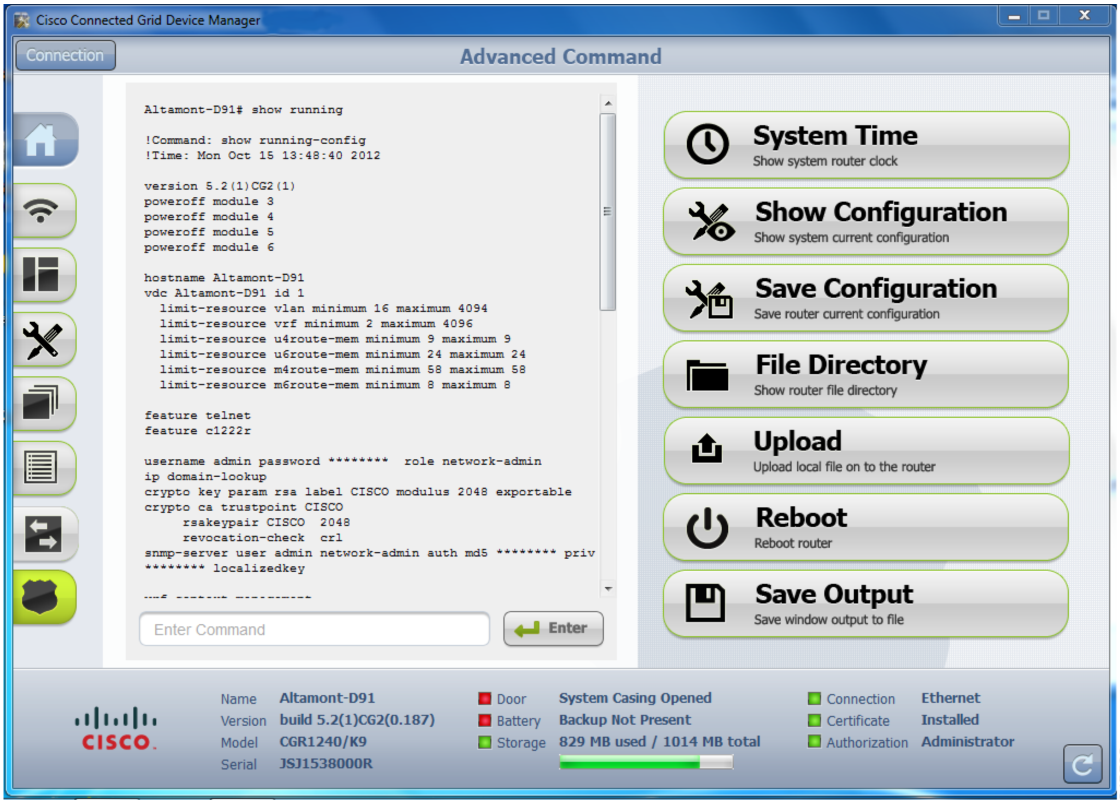
Removing module from slot. This process will take several minutes. Please wait.

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

A plus (+) sign now displays 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


Cisco Connected Grid Device Manager
Connection
Advanced Command
System Time
Show system router clock
Show Configuration
Show system current configuration
Save Configuration
Save router current configuration
File Directory
Show router file directory
Upload
Upload local file on to the router
Reboot
Reboot router
Save Output
Save window output to file
Enter Command
Enter
345593

```
Altamont-D91# show running

!Command: show running-config
!Time: Mon Oct 15 13:48:40 2012

version 5.2(1)CG2(1)
poweroff module 3
poweroff module 4
poweroff module 5
poweroff module 6

hostname Altamont-D91
vdc Altamont-D91 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 c1222r

username admin password ********  role network-admin
ip domain-lookup
crypto key param rsa label CISCO modulus 2048 exportable
crypto ca trustpoint CISCO
     rsakeypair CISCO  2048
     revocation-check  crl
snmp-server user admin network-admin auth md5 ******** priv
******** localizedkey
```

Name	Altamont-D91	🟥 Door	System Casing Opened	🟩 Connection	Ethernet
Version	build 5.2(1)CG2(0.187)	🟥 Battery	Backup Not Present	🟩 Certificate	Installed
Model	CGR1240/K9	🟩 Storage	829 MB used / 1014 MB total	🟩 Authorization	Administrator
Serial	JSJ1538000R				

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 displays 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 3-40

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.

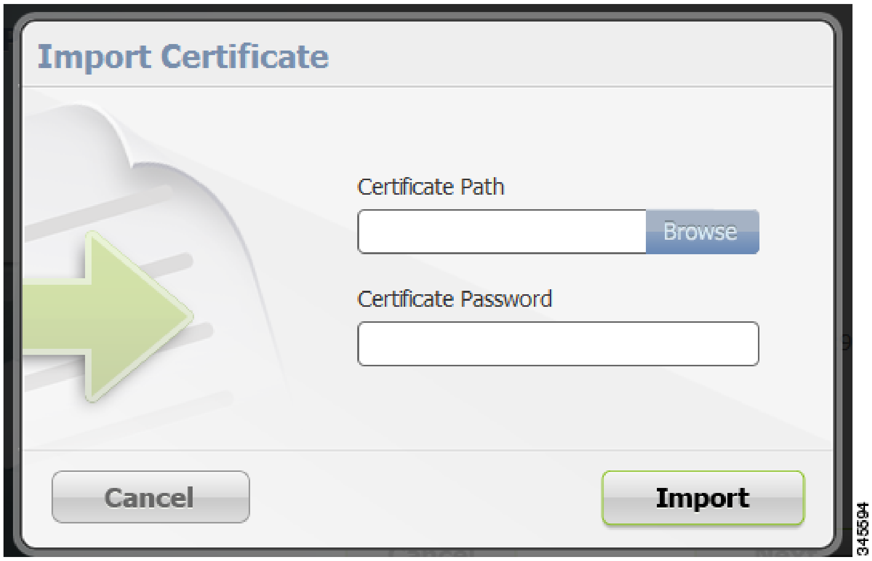
To open the Import Certificate panel, do the following:

Step 1 Step through the Setup wizard until you reach the Certificate Configuration panel by clicking **Next** at each panel. *See* Setting Operating Mode

You do not need to change any values on the pages as you move through the pages.

Step 2 At the Certificate Configuration panel, click **Change Certificate**.

The Import Certificate panel appears.



Step 3 At the Certificate Configuration panel, 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 Router page.

Connection Override

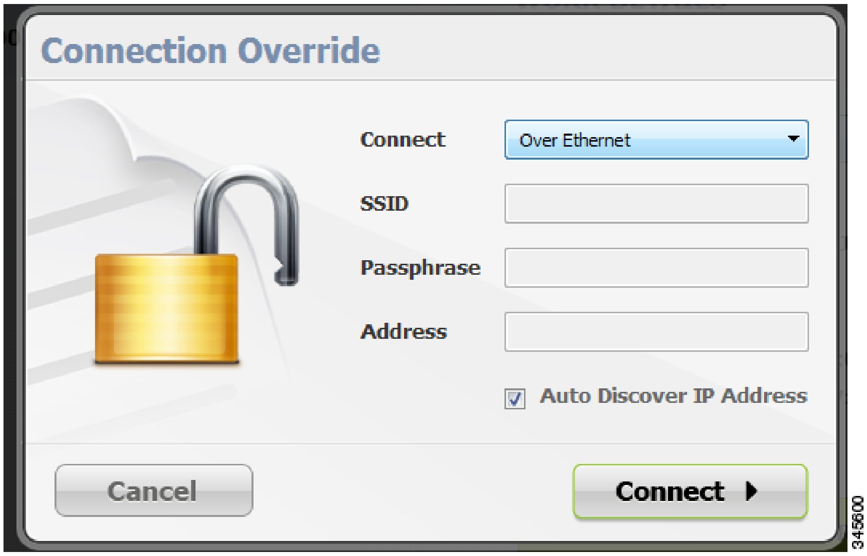
You only use the Connection Override option, when you need to use different login information than that provided in the work order.

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 the Connection Override panel 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 At the Work Authorization page, click **Connection Override**.



Connection Override

Connect: Over Ethernet

SSID:

Passphrase:

Address:

☑ Auto Discover IP Address

Step 2 At the Connection Override panel, select the connection type (Over Ethernet, Over WiFi, Auto Detect) from the Connect drop-down menu.

Step 3 Click **Connect**.

Example Log File Output

This section contains sample output examples for files generated at 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 at 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 at 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/wrl3/linux-2.6.27_wrl30/drivers/i2c/busses/ioh/
ioh_i2c_hal.c:ioh_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_im 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_im init is called - curl
2012 Oct 16 14:48:01 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im 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_im 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_im 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_im init is called - rm
2012 Oct 16 14:51:16 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - java
2012 Oct 16 14:51:16 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - pidof
2012 Oct 16 14:51:20 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im 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_im init is called - curl
2012 Oct 16 14:51:38 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - su
2012 Oct 16 14:51:38 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - xmlsa
2012 Oct 16 14:51:39 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im 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_im 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_im 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_im 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_im 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_im 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_im 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_im init is called - curl
2012 Oct 16 15:10:51 CGR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - vsh
```

Feature History

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

CHAPTER 4

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 2-2

"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"

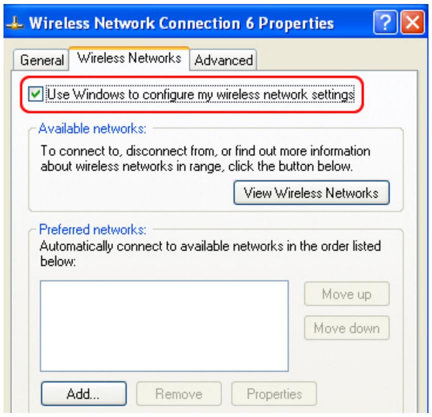
Resolution:

- 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.
  - Verify that the laptop has Windows Wireless Zero Configuration enabled.
  - Ensure that there is no third-party wireless client tool is 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 Wireless Zero Configuration.
- Enable Windows Wireless Zero Configuration by following these steps:

Step 1 Click **Start** > **Settings** > **Control Panel**.

Step 2 Double-click **Network Connections**.

Step 3 Right-click **Wireless Network Connection**.



Wireless Network Connection 6 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

Automatically connect to available networks in the order listed below:

Step 4 Click **Properties**.

Step 5 Click **Wireless Networks** tab.

Step 6 Check the *Use Windows to configure my wireless network settings* check box.

Step 7 Click **OK**. This confirms the third-party WiFi utility is not configured to mange your WiFi interface.

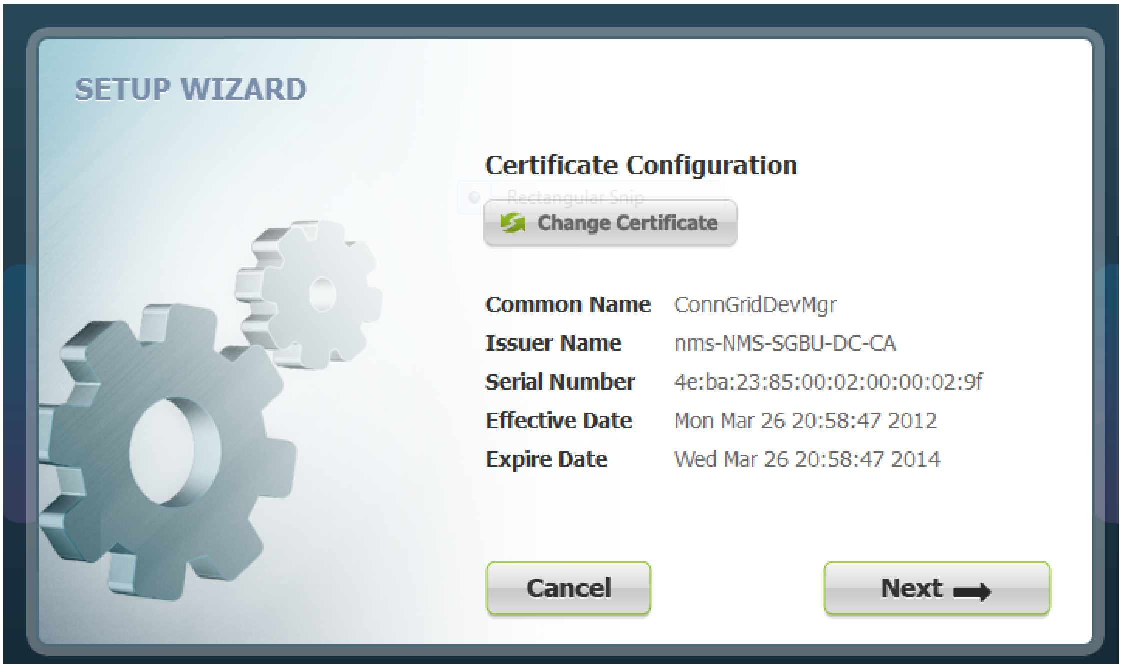
"I cannot log in to Device Manager"

Cause: This message displays 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 2-2 for details on installing certificates.



Certificate Configuration

Common Name	ConnGridDevMgr
Issuer Name	nms-NMS-SGBU-DC-CA
Serial Number	4e:ba:23:85:00:02:00:00:02:9f
Effective Date	Mon Mar 26 20:58:47 2012
Expire Date	Wed Mar 26 20:58:47 2014

345599

"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 adpater. Additionally, the Device Manager cannot control WiFi through Windows API.

Resolution: Disable the thrid-party software and enable Windows Wirelss Zero Configuration.

"Cannot detect peer's IPv6 address"

Cause: IPv6 peer was not found.

Resolution: Enable the IPv6 link local address on 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 setup 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 10000 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 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 at the Connect to Router page.
- Check the status of the WiFi connection.