Cisco Connected Grid Device Manager Installation and User Guide, Release 1.0.1

February 2012

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-26238-01

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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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

Cisco Connected Grid Device Manager Installation and User Guide

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

Introduction

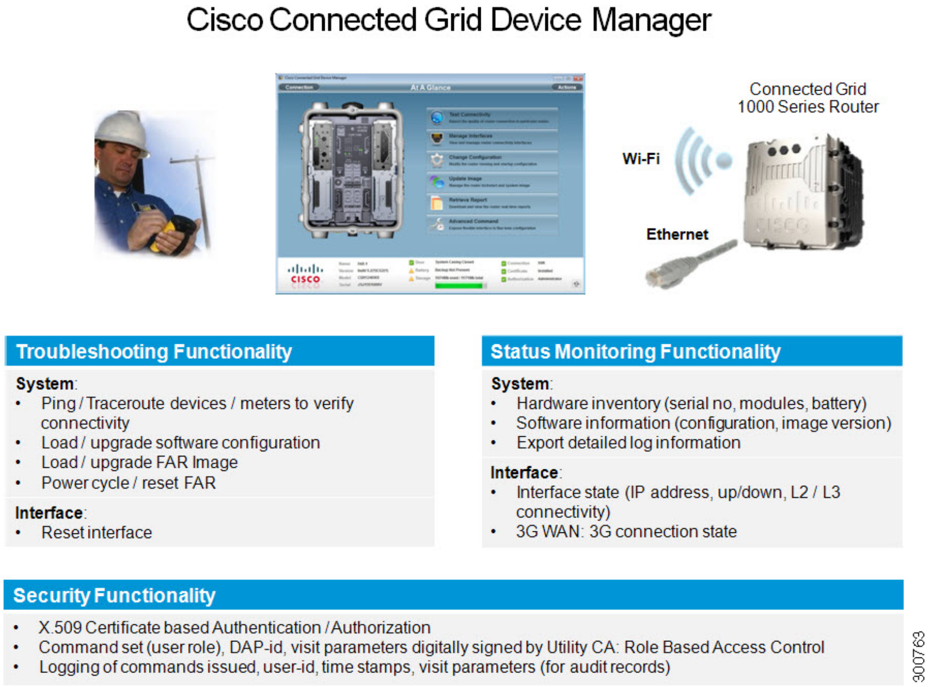
The Cisco Connected Grid Device Manager is a tool used to troubleshoot a Cisco Connected Grid Field Area Router (FAR or router). This chapter contains the following topics:

- Overview, page 1-1
- The Connected Grid Network, page 1-3
- Additional Information, page 1-4

Overview

The Device Manager is an application used to troubleshoot a FAR (or Connected Grid router), as well as test devices connected to the FAR. The Device Manager reads FAR configuration information, displays data, and manages individual FARs. You can connected to the Device Manager using a secured Ethernet or WiFi link for first-time deployment or troubleshooting.

The following illustration lists the functionality of the Device Manager.



Troubleshooting Functionality

System:
- Ping / Traceroute devices / meters to verify connectivity
- Load / upgrade software configuration
- Load / upgrade FAR Image
- Power cycle / reset FAR

Interface:
- Reset interface

Status Monitoring Functionality

System:
- Hardware inventory (serial no, modules, battery)
- Software information (configuration, image version)
- Export detailed log information

Interface:
- Interface state (IP address, up/down, L2 / L3 connectivity)
- 3G WAN: 3G connection state

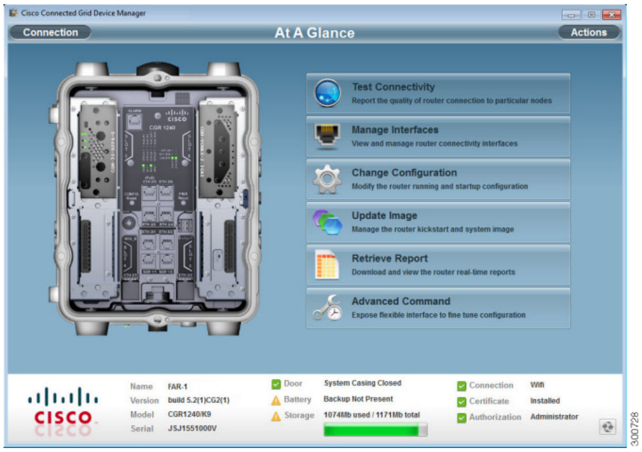
Security Functionality

- X.509 Certificate based Authentication / Authorization
- Command set (user role), DAP-id, visit parameters digitally signed by Utility CA: Role Based Access Control
- Logging of commands issued, user-id, time stamps, visit parameters (for audit records)

The Device Manager enables you to:

- Troubleshoot connectivity between a FAR and the devices connected to the router (see Test Connectivity, page 3-5)
- Check and update the current FAR configuration (see Advanced Command, page 3-19 and Change Configuration, page 3-12)
- Update the FAR image and reset the router (see Update Image, page 3-15)
- View real-time FAR configuration information for troubleshooting (see Retrieve Report, page 3-18)
- Use advanced commands to troubleshoot the FAR (see Advanced Command, page 3-19)

Once the Device Manager connects to a Field Area Router (FAR), the system information displays at the bottom of each screen. The example screen below shows that the FAR has two Connected Grid Modules installed (WiMAX in slot 3 and Cellular in slot 6), and the LEDs flash indicating the modules are operating.



Test Connectivity
Report the quality of router connection to particular nodes

Manage Interfaces
View and manage router connectivity interfaces

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 reports

Advanced Command
Expose flexible interface to fine tune configuration

Name	FAR-1	✓ Door	System Casing Closed	✓ Connection	Wifi
Version	build 5.2(1)CG2(1)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	CGR1240/K9	⚠ Storage	1074Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ1551000V				

Other information that displays at the bottom of each screen includes:

- Name of the router
- Software build version
- Model number of the FAR
- Serial number of the FAR
- Door (system casing) status
- Battery status (if a backup battery is installed)
- Storage status including amount of storage available
- Connection method (WiFi or Ethernet)
- Certificate status
- Authorized user (Administrator)

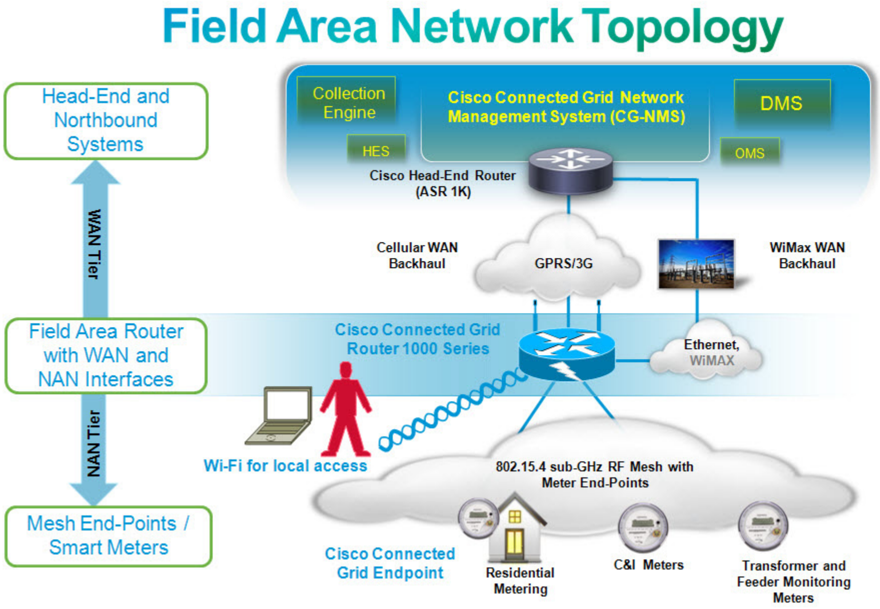
Information can be refreshed at any time by using the Refresh icon, located in the lower right-hand of the screen.

The Connected Grid Network

Cisco's Connected Grid Field Area Network (FAN) solution is a two-tier architecture containing both the Neighborhood Area Network (NAN) and the Wide Area Network (WAN). The NAN provides network connectivity to end-points such as smart meters and devices. The WAN tier provides network connectivity from the FAR to the utility's control center over either public 2G/3G network, or over a utility-owned (private) WiMAX or Ethernet network.

The Connected Grid FAN solution is comprised of the Cisco 1000 Series Connected Grid Router, the Connected Grid Network Management System, and the Connected Grid Device Manager. The FAR (or Connected Grid Router) connects the NAN to the WAN. The Connected Grid Network Management System is management tool which manages a number of FARs, while the Connected Grid Device Manager provides access to a single FAR (at a time), for the tasks described in this guide.

The following illustrates the FAN topology.


Field Area Network Topology
Head-End and Northbound Systems
WAN Tier
Field Area Router with WAN and NAN Interfaces
NAN Tier
Mesh End-Points / Smart Meters
Collection Engine
HES
Cisco Connected Grid Network Management System (CG-NMS)
DMS
OMS
Cisco Head-End Router (ASR 1K)
Cellular WAN Backhaul
GPRS/3G
WiMax WAN Backhaul
Cisco Connected Grid Router 1000 Series
Ethernet, WiMAX
Wi-Fi for local access
802.15.4 sub-GHz RF Mesh with Meter End-Points
Cisco Connected Grid Endpoint
Residential Metering
C&I Meters
Transformer and Feeder Monitoring Meters

Field Area Routers

Unlike traditional routers and switches that reside in locations such as utility data centers or an enterprise Network Operations Center (NOC), a FAR (router) connects equipment in the field such as meters, sensors, and control equipment to the utility’s control center.

The Cisco 1000 Series Connected Grid Router is a multi-service communication platform designed for use in FARs. The Connected Grid Router is designed to operate reliably in various types of harsh environments, including outdoor pole-top deployments. The Connected Grid Router is modular and supports a variety of communication interfaces including WiMAX, Cellular, 900 MHz RF Mesh, Ethernet, and WiFi.

Additional Information

Please use the following links for additional information on Cisco Connected Grid products:

- For Cisco Solutions for Utilities/Smart Grid, see *http://www.cisco.com/web/strategy/energy/external_utilities.html*
- For Cisco 1000 Series Connected Grid Routers, see *http://www.cisco.com/en/US/products/ps12256/index.html*

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 experience with a Cisco Field Area Router (FAR).

System Requirements

The Device Manager has the following system requirements:

- Microsoft Windows 7 Enterprise / Professional or Windows XP (with Service Pack 3)
- 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 FAR authentication (obtained from your IT department)

Certificate Installation

Before you can install the Device Manager, you must install the client identity and CA certificates in the computer.

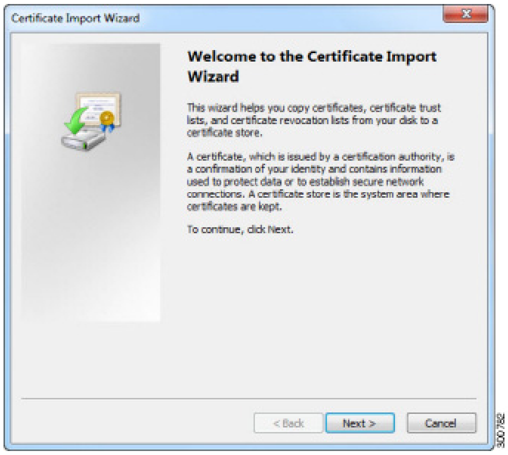
Follow these steps to install the certificate on the computer running the Device Manager:

Step 1 Contact your IT Department for the PKCS #12 formatted certificate, which should contain the client identity and CA certificates (along with the private key and its password to import the certificates onto the laptop).

Step 2 Copy the certificate (provided by your IT Department) to your computer, for example, on the Desktop.

Step 3 Double-click the certificate to open the Installation Wizard.

Step 4 Click **Next** to start the installation.



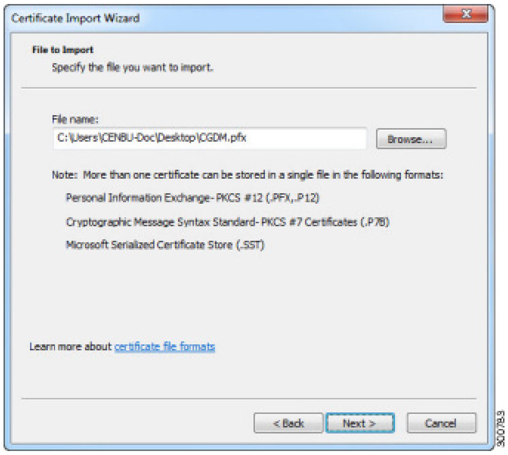
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 5 Browse to the location of the certificate file, and then click **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\CENBU-Doc\Desktop\CGDM.pfx

Note: More than one certificate can be stored in a single file in the following formats:

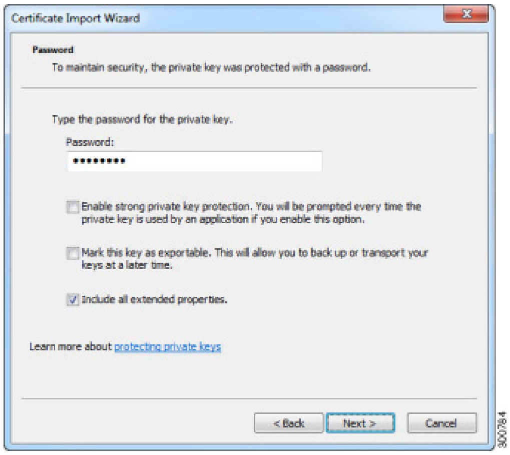
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Step 6 Enter the password, unmark the ‘Enable strong private key protection’, mark ‘Include all extended properties’, and then click **Next**.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••

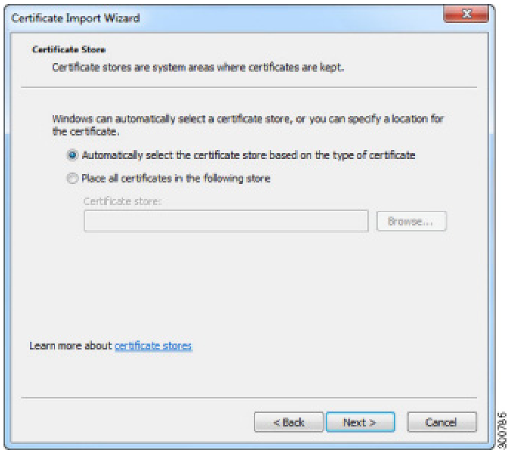
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

Step 7 Keep the default setting ‘Automatically select the certificate store based on the type of certificate,’ and then click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

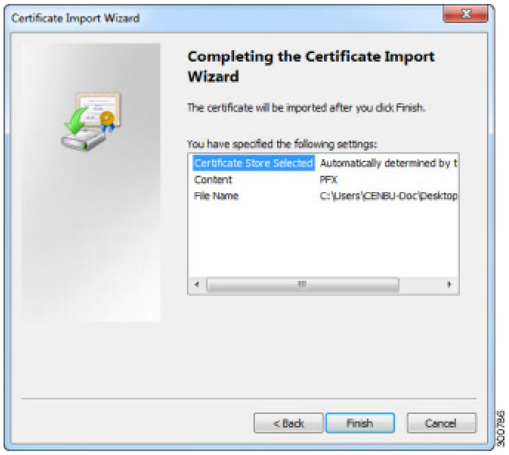
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

Step 8 Click **Finish**.



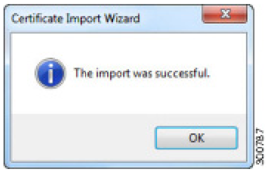
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\CENBU-Doc\Desktop

Step 9 Click **OK** to complete installation of the certificate.



The import was successful.

Step 10 Open the Windows Registry using regedit and search for the following registry entry:

```
Computer\HKEY_CURRENT_USER\Software\Cisco\CGDManager\Cgdm
```

Step 11 Edit the `CERT_COMMON_NAME` to match the common name of the certificate from step 1 (above).

Note Specify the `CA_COMMON_NAME` field or leave it as `--AutoDetect--`.

Follow these steps to verify the client certificate (optional):

Step 1 (Optional) Verify the client certificate in the Internet Explorer browser:

```
IE browser\Tools\Internet Options\Content\Certificates\Personal
```

Step 2 (Optional) Verify the CA certificate in the Internet Explorer browser:

```
IE browser\Tools\Internet Options\Content\Certificates\Trusted Root Certification
Authorities
```

Step 3 (Optional) Delete the *C:\ProgramData\Cisco\CGDManager* folder. Run the Device Manager to automatically generate this folder, and then quit the Device Manager without any actions (to clean up any previous settings).

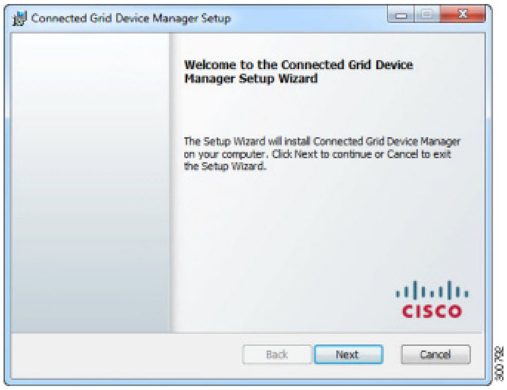
Note The program data directory for the Device Manager is hidden, by default. To view this directory, open an Explorer window, select Folder Options from the Tools menu, and then select the View tab. Select ‘Show hidden files and folders’, and then click **OK**.

Device Manager Installation

Follow these steps to install the Device Manager:

Step 1 Double-click CGDManager executable to start installation.

Step 2 Click **Next**.

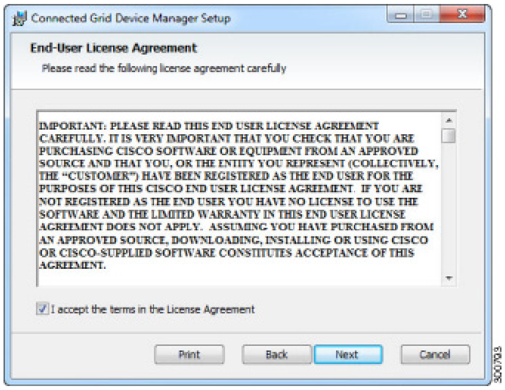


Connected Grid Device Manager Setup

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 checkbox to accept the terms of the License Agreement, and then click **Next**.



Connected Grid Device Manager Setup

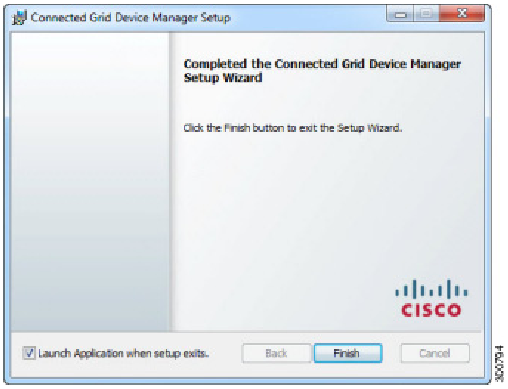
End-User License Agreement

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

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



Connected Grid Device Manager Setup

Completed the Connected Grid Device Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch Application when setup exits.

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

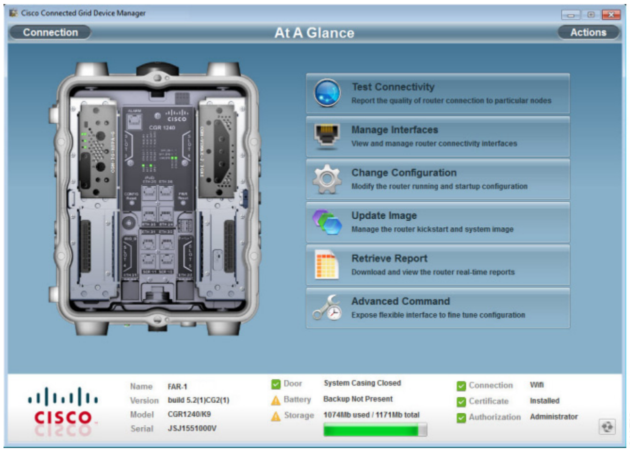
The chapter explains how to use the Device Manager, and contains the following topics:

Device Manager Overview

The Device Manager main screen displays after securely connecting. From here you have several options:

- **Test Connectivity** is used to see if you can reach a device's IP address from the FAR, check link connectivity and quality, or traceroute the address if it is not reachable. This feature helps you confirm and re-check the connectivity through troubleshooting (see Test Connectivity, page 3-5).
- **Manage Interfaces** is used to bring up or shut down an interface (see Manage Interfaces, page 3-10).
- **Change Configuration** is used to update the FAR configuration with a provided configuration file, and then reboot the FAR with the new configuration (see Change Configuration, page 3-12).
- **Update Image** is used to update the FAR with an image file. The upgrade allows a complete refresh of the FAR with the designated softwasre image (see Update Image, page 3-15).
- **Retrieve Report** is used to view and/or download the FAR system logs (see Retrieve Report, page 3-18).

- **Advanced Command** is used to verify the router system time is correct, view the current router configuration, save the current configuration, view the current file directory, reboot the router, or save the window output to a file (seeAdvanced Command, page 3-19).


Cisco Connected Grid Device Manager
Connection
At A Glance
Actions
Test Connectivity
Report the quality of router connection to particular nodes
Manage Interfaces
View and manage router connectivity interfaces
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 reports
Advanced Command
Expose flexible interface to fine tune configuration
300728

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

☑ Door System Casing Closed
⚠ Battery Backup Not Present
⚠ Storage 1074Mb used / 1171Mb total

☑ Connection Wifi
☑ Certificate Installed
☑ Authorization Administrator

The router image that displays in the Device Manager is an exact replicate of the FAR you are connected to. The router image shows 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 every screen.

How to Use the Device Manager

Using a work order, you can log into the Device Manager, and then connect to a FAR to troubleshoot devices connected to the router.

Note Work order retrieval is not supported in this release of Device Manager. You must obtain works orders from the utility's back-end system.

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

- Your work order states that there are devices connected to a FAR that cannot be reached. You need to start Device Manager, connect to the FAR, and then check connectivity to the devices (see Test Connectivity, page 3-5). If you can connect to the devices, you should now review the FAR configuration information (see Advanced Command, page 3-19). If the configuration information is not correct, you should now update the configuration (see Change/Update Configuration, page 3-14) by adding a configuration file to the Device Manager, and then updating the FAR configuration. Once the configuration is updated (see Advanced Command, page 3-19) the FAR automatically resets and restarts with the new configuration. You are now ready to disconnect from the Device Manager.
- Your work order states that the FAR needs to have a software image update. You need to start the Device Manager, add the new image file, and then update the FAR with the new image (see Update Image, page 3-15). The FAR automatically restarts once the software image has updated. You are now ready to disconnect from the Device Manager.

- Your work order states that there are new FARs that have been deployed and they are not showing in the back-end system. You need to start the Device Manager, and then review the FAR graphic on the main screen. Check the modules installed and the LEDs indicating if the modules are operating. If the LEDs are not flashing, you need to check installation of the modules (see the *Connected Grid Module Installation and Configuration Guide* for the module model).
- Your work order states that the door to the FAR is open. You need to start the Device Manager and check the status of the door. If the door status is *System Casing Open*, you need to access the FAR and ensure the door is closed. Once the door is closed, press the Refresh icon located at the bottom right-hand corner of the Device Manager and verify the door status is now *System Casing Closed*. You are now ready to disconnect from the Device Manager.

How to Start

Now that you understand the basic functionality of the Device Manager and how to use it, you are now ready to troubleshoot devices connected to a FAR. Refer to the following sections for specific steps to troubleshoot devices.

Connect to the FAR

You can connect to a FAR (or Connected Grid Router) either by Ethernet or WiFi. The WiFi connectivity control ensures data traffic between the Device Manager and the FAR are protected by WPA Layer 2 security, once the association and key handshake are complete. The Ethernet connection is secured by https only.

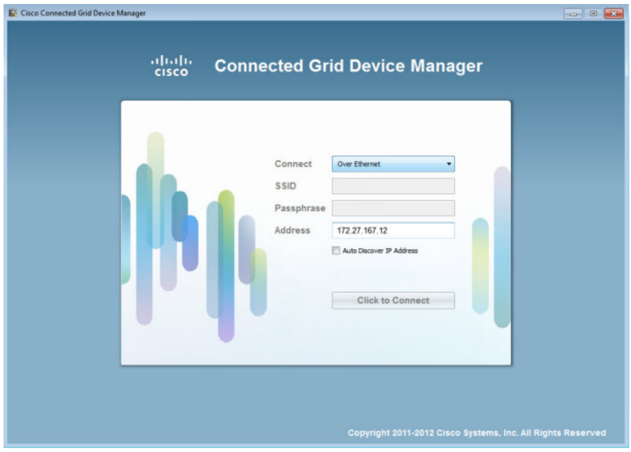
Connection to the Device Manager can be done using one of the following:

- 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 Double-click the **Cisco GCD Manager** from the Desktop, or select **Start** > **All Programs** > **Cisco CGD Manager**.

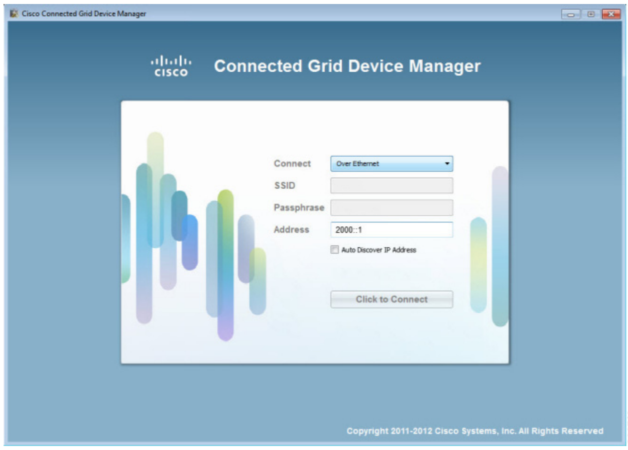
The following example screen shows connecting over Ethernet using an IPv4 IP address.


Cisco Connected Grid Device Manager
cisco
Connected Grid Device Manager
Click to Connect
Copyright 2011-2012 Cisco Systems, Inc. All Rights Reserved
300721

Connect: Over Ethernet
SSID:
Passphrase:
Address: 172.27.167.12
□ Auto Discover IP Address

Step 2 Select the connection method (Over WiFi, Over Ethernet, or Auto Detect).

The following example screen shows connecting over Ethernet with an IPv6 address.


Cisco Connected Grid Device Manager
cisco
Connected Grid Device Manager
Click to Connect
Copyright 2011-2012 Cisco Systems, Inc. All Rights Reserved
300722

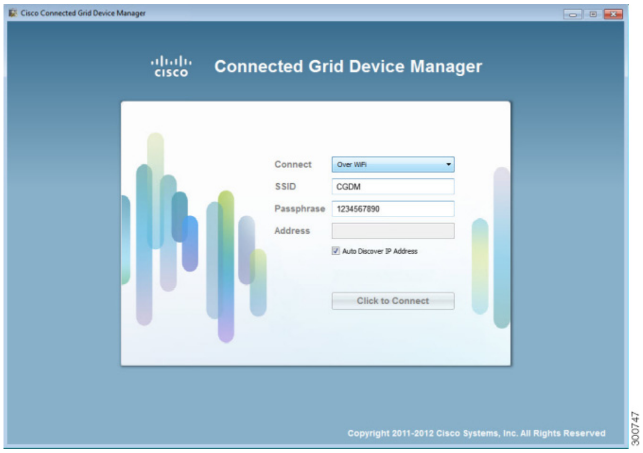
Connect: Over Ethernet
SSID:
Passphrase:
Address: 2000::1
□ Auto Discover IP Address

Step 3 Enter the SSID and Passphrase if connecting over WiFi.

Step 4 *Optional*. Enter the address, or select the checkbox to auto-detect the address.

Note When Auto Detect is selected, the computer running Device Manager must be connected directly to the FAR via Ethernet or WiFi to automatically discover IPv6 addresses.

The following example screen shows connecting over WiFi using Auto Discover IP address.



Cisco Connected Grid Device Manager
Connected Grid Device Manager

Connect: Over WiFi
SSID: CGDM
Passphrase: 1234567890
Address:
☑ Auto Discover IP Address

Click to Connect
Copyright 2011-2012 Cisco Systems, Inc. All Rights Reserved
300747

Step 5 Select **Click to Connect**.

See Frequently Asked Questions, page 3-25 if you cannot connect to the Device Manager for possible connection problems.

Test Connectivity

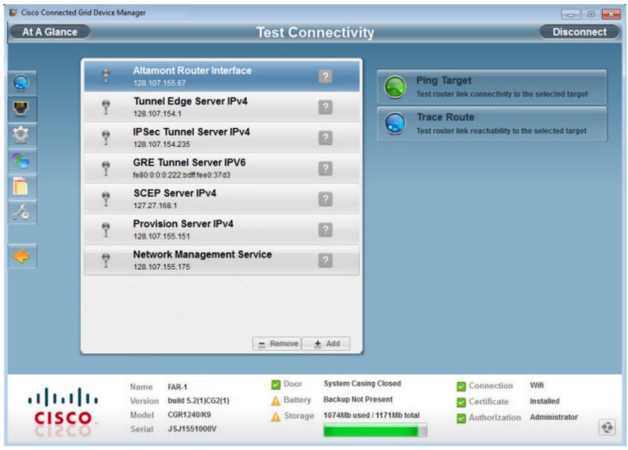
This feature is used to confirm and re-check the connectivity to a device from the FAR. Before you can check the device connection or route to a FAR, you must add a device's IP address to the Device Manager. IP addresses can be either IPv4 or IPv6.

Add a Device IP Address

Follow these steps to add a device's IP address (the destination device the FAR is trying to reach):

Step 1 Click **Test Connectivity** 🌐.

The following example shows sample devices and/or target addresses.



Cisco Connected Grid Device Manager

Test Connectivity

Altamont Router Interface
128.107.155.67

Tunnel Edge Server IPv4
128.107.154.1

IPSec Tunnel Server IPv4
128.107.154.235

GRE Tunnel Server IPV6
fe80:0:0:0:222:bdff:fee0:37d3

SCEP Server IPv4
127.27.168.1

Provision Server IPv4
128.107.155.151

Network Management Service
128.107.155.175

Ping Target
Test router link connectivity to the selected target

Trace Route
Test router link reachability to the selected target

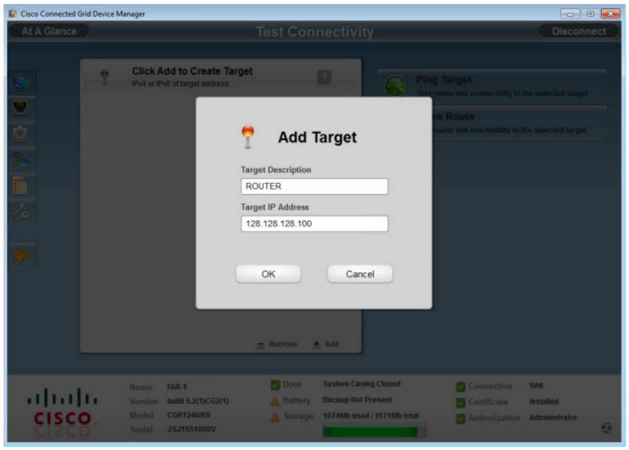
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total

Connection Wifi
Certificate Installed
Authorization Administrator

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

In the following example, we're adding a router with a target address of 128.128.128.100.



Cisco Connected Grid Device Manager

Test Connectivity

Click Add to Create Target
IPv4 or IPv6 of target address

Add Target

Target Description
ROUTER

Target IP Address
128.128.128.100

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total

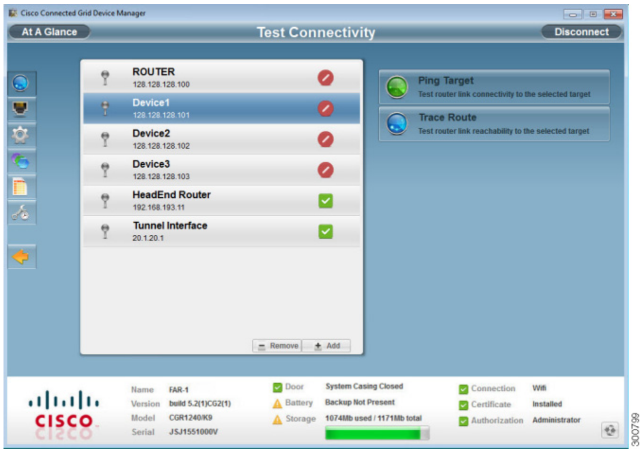
Connection Wifi
Certificate Installed
Authorization Administrator

Step 3 Enter a Target Description (or description of the device).

Step 4 Enter the Target IP Address (device's IP address). This can be either an IPv4 or IPv6 address.

Step 5 Click **OK**.

The following example shows a device’s IP address was added.



Cisco Connected Grid Device Manager

At A Glance | Test Connectivity | Disconnect

ROUTER 128.128.128.100	⊘
Device1 128.128.128.101	⊘
Device2 128.128.128.102	⊘
Device3 128.128.128.103	⊘
HeadEnd Router 192.168.193.11	☑
Tunnel Interface 20.1.20.1	☑

Remove | Add

Ping Target
Test router link connectivity to the selected target

Trace Route
Test router link reachability to the selected target

Name	FAR-1	☑	Door	System Casing Closed	☑	Connection	Wifi
Version	build 5.2(1)CG2(1)	⚠	Battery	Backup Not Present	☑	Certificate	Installed
Model	CGR1240/K9	⚠	Storage	1074Mb used / 1171Mb total	☑	Authorization	Administrator
Serial	JSJ1551000V						

You are now ready to test the connectivity to the device you just added into Device Manager.

Ping a Device IP Address

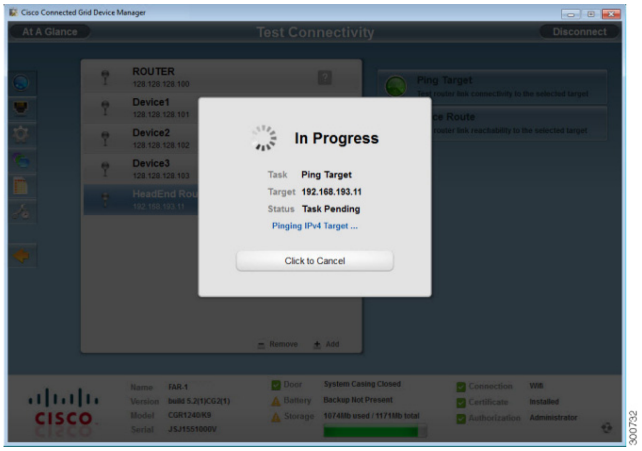
This feature allows you to test if you can reach a specified device’s IP address.

Follow these steps to test connectivity between the FAR and the device:

Step 1 Select a target IP address from the list.

Step 2 Click **Ping Target** to test the connectivity to the selected IP address.

The following example shows the Device Manager is attempting to ping the IPv4 address.



Cisco Connected Grid Device Manager

At A Glance | Test Connectivity | Disconnect

ROUTER 128.128.128.100
Device1 128.128.128.101
Device2 128.128.128.102
Device3 128.128.128.103
HeadEnd Rou 192.168.193.11

Remove | Add

In Progress

Task Ping Target
Target 192.168.193.11
Status Task Pending
Pinging IPv4 Target ...

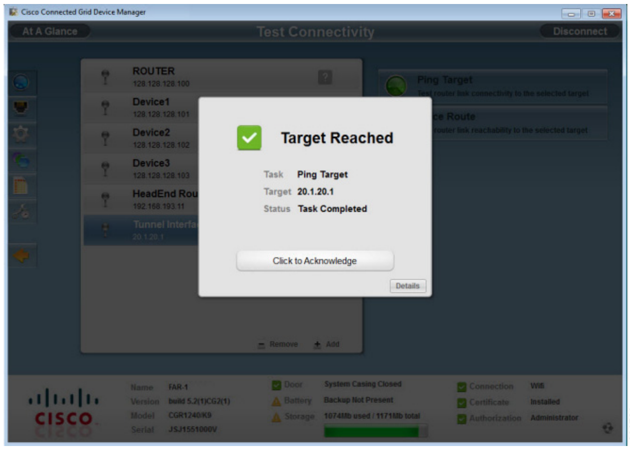
Click to Cancel

Ping Target
Test router link connectivity to the selected target

ce Route
router link reachability to the selected target

Name	FAR-1	☑	Door	System Casing Closed	☑	Connection	Wifi
Version	build 5.2(1)CG2(1)	⚠	Battery	Backup Not Present	☑	Certificate	Installed
Model	CGR1240/K9	⚠	Storage	1074Mb used / 1171Mb total	☑	Authorization	Administrator
Serial	JSJ1551000V						

The following example shows the ping was successful. Note that the icon to the left of the successful ping is green, representing that the target was reached.

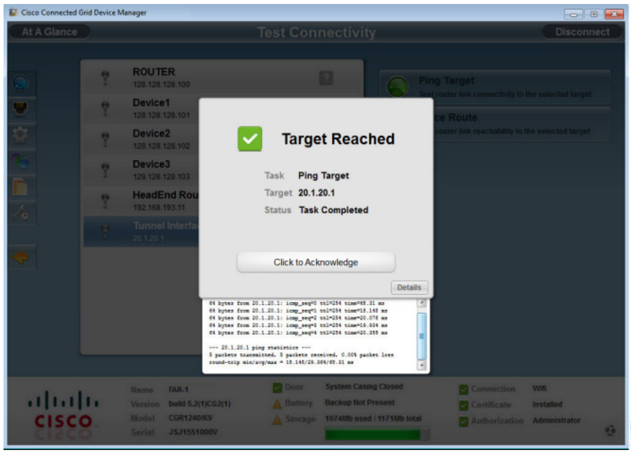


Target Reached

Task Ping Target
Target 20.1.20.1
Status Task Completed

300730

Step 3 Select **Click to Acknowledge** to close the window, or you can also click **Details** to view the ping details (shown below).



Target Reached

Task Ping Target
Target 20.1.20.1
Status Task Completed

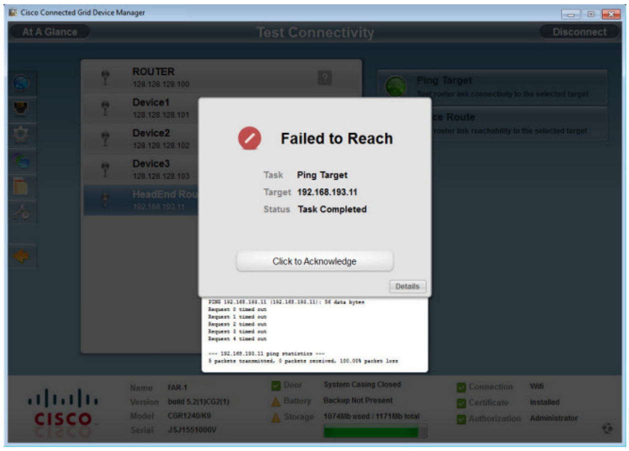
```
64 bytes from 20.1.20.1: icmp_seq=0 ttl=254 time=68.31 ms
64 bytes from 20.1.20.1: icmp_seq=1 ttl=254 time=18.148 ms
64 bytes from 20.1.20.1: icmp_seq=2 ttl=254 time=20.078 ms
64 bytes from 20.1.20.1: icmp_seq=3 ttl=254 time=19.924 ms
64 bytes from 20.1.20.1: icmp_seq=4 ttl=254 time=20.355 ms

--- 20.1.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 18.148/29.364/68.31 ms
```

300731

Follow these steps if the target IP address is not reachable:

Step 1 Click **Details** to view the reason the IP address was not reachable.

The following example shows the connection timed out, with five packets sent, and zero packets received Note that the icon to the left of the failed ping is red, representing that the target was not reached.



Failed to Reach

Task Ping Target
Target 192.168.193.11
Status Task Completed

```
PING 192.168.193.11 (192.168.193.11): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 192.168.193.11 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator

300727

Step 2 Select **Click to Acknowledge** to close the window.

Step 3 Go the next section and traceroute the IP address.

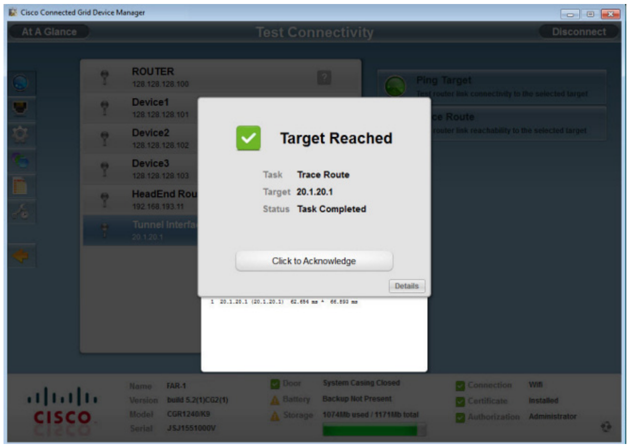
Traceroute a Device IP Address

If an IP address cannot be reached using Ping, you can use traceroute to check the route taken to reach the device's IP address.

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

Step 1 Select the device's IP address from the list.

Step 2 Click **Traceroute** to trace the route.



Target Reached

Task Trace Route
Target 20.1.20.1
Status Task Completed

```
1  20.1.20.1 (20.1.20.1)  62.654 ms *  66.893 ms
```

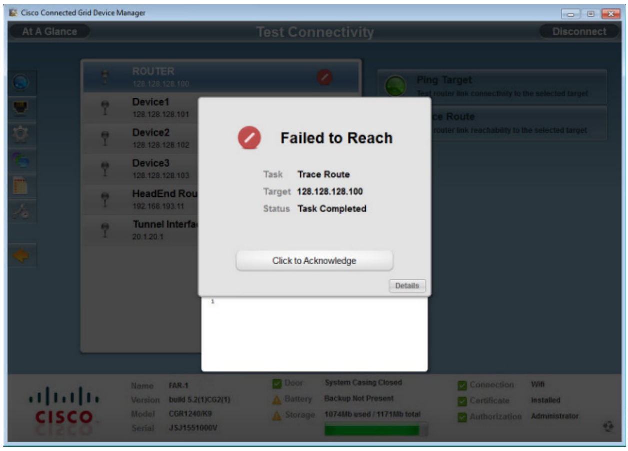
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator

300743

Step 3 Select **Click to Acknowledge**, or click **Details** to view the traceroute details.

Follow these steps if the traceroute fails:

Step 1 Select **Click to Acknowledge**.



Failed to Reach

Task Trace Route
Target 128.128.128.100
Status Task Completed

Step 2 The traceroute failed. Remove the device's IP address.

Remove a Device IP Address

Once you have tested a target IP address and verified connectivity, you can then remove the device from Device Manager. Another example would be entering an incorrect device address, which you now need to remove.

Follow these steps to remove a target IP address:

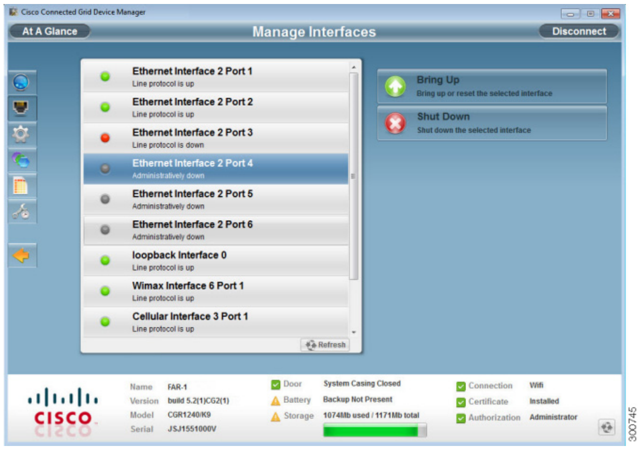
Step 1 Select the target IP address from the list.

Step 2 Click **Remove**.

Manage Interfaces

The feature is used to bring up or shut down an interface. If an interface is *up* (displays in green), it means that the line protocol is currently active. If an interface is *down* (displays in red), it means the line protocol is not active. If an interface is administratively down (displays in grey), it means that the line interface has been taken down by the administrator.

When Manage Interface is used, all interfaces contained on the FAR you are connected to display automatically. For example, the following screen shows that two modules are installed (WiMAX and Cellular), the FAR has six Ethernet interfaces, as well as a loopback interface.


Cisco Connected Grid Device Manager
At A Glance
Manage Interfaces
Disconnect
Bring Up
Bring up or reset the selected interface
Shut Down
Shut down the selected interface
Refresh
CISCO
300745

Ethernet Interface 2 Port 1
Line protocol is up

Ethernet Interface 2 Port 2
Line protocol is up

Ethernet Interface 2 Port 3
Line protocol is down

Ethernet Interface 2 Port 4
Administratively down

Ethernet Interface 2 Port 5
Administratively down

Ethernet Interface 2 Port 6
Administratively down

loopback Interface 0
Line protocol is up

Wimax Interface 6 Port 1
Line protocol is up

Cellular Interface 3 Port 1
Line protocol is up

Name	FAR-1	Door	System Casing Closed	Connection	Wifi
Version	build 5.2(1)CG2(1)	Battery	Backup Not Present	Certificate	Installed
Model	CGR1240/K9	Storage	1074Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ1551000V				

Follow these steps to view or manage selected router interfaces:

Step 1 Click **Manage Interfaces** .

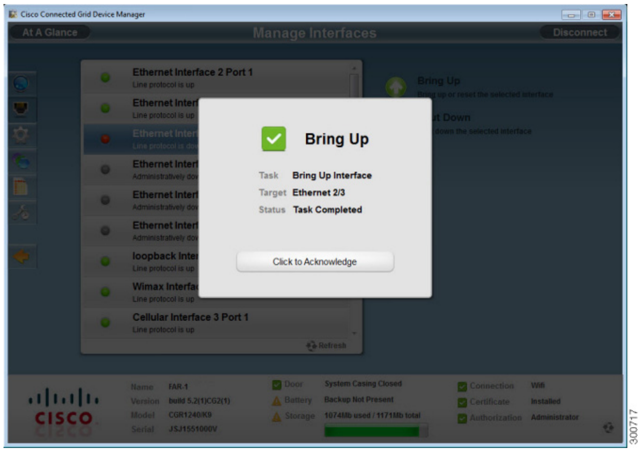
Step 2 Select an interface and then go to either Bring Up an Interface, page 3-11 or Shut Down an Interface, page 3-12.

Bring Up an Interface

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

Follow these steps to bring up an interface:

Step 1 Select an interface and then click **Bring Up**.



Bring Up

Task Bring Up Interface
Target Ethernet 2/3
Status Task Completed

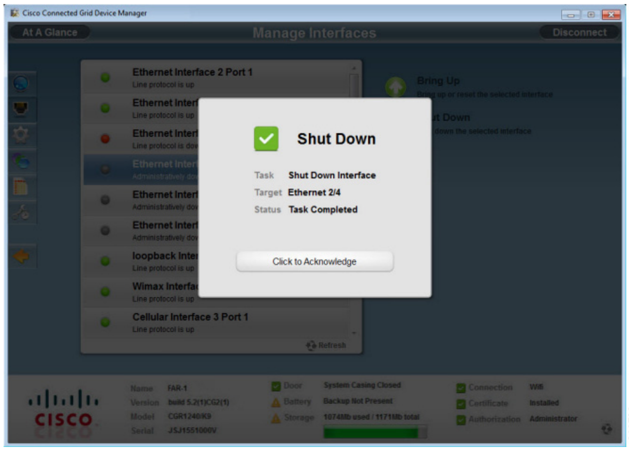
Step 2 Select **Click to Acknowledge**.

Shut Down an Interface

Caution Do not shut down the interface that the Device Manager is using or communication with the FAR will be lost.

Follow these steps to shut down an interface:

Step 1 Select an interface and then click **Shut Down**.



Shut Down

Task Shut Down Interface
Target Ethernet 2/4
Status Task Completed

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total

Connection Wifi
Certificate Installed
Authorization Administrator

Step 2 Select **Click to Acknowledge**.

Change Configuration

This feature is used to upload or add a configuration file to the Device Manager, and then use that file to update the configuration of the FAR. The configuration file information must include version, username and password, Ethernet and WiFi interfaces, and CGDM and IP https configurations.

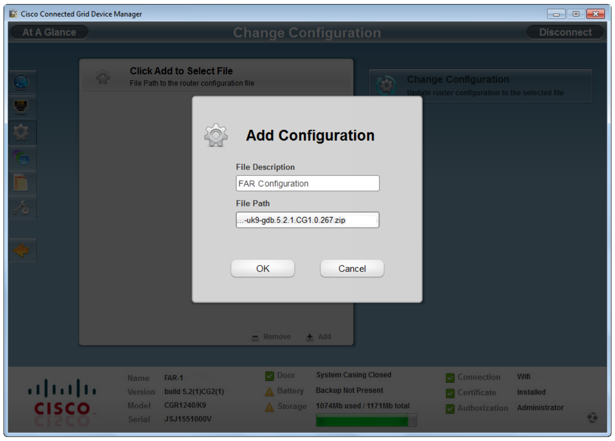
Note The configuration file needs to be a complete configuration file. If the configuration file contains missing fields, the Device Manager will not update the configuration properly. If you receive an error while updating the configuration file, check the configuration file for missing information.

Add a Configuration File

Follow these steps to add a configuration file:

Step 1 Click **Change Configuration** ⚙.

Step 2 Click **Add**.


Cisco Connected Grid Device Manager
At A Glance
Change Configuration
Disconnect
Click Add to Select File
File Path to the router configuration file
Change Configuration
Update router configuration to the selected file
Remove
Add
cisco

Add Configuration

File Description: FAR Configuration

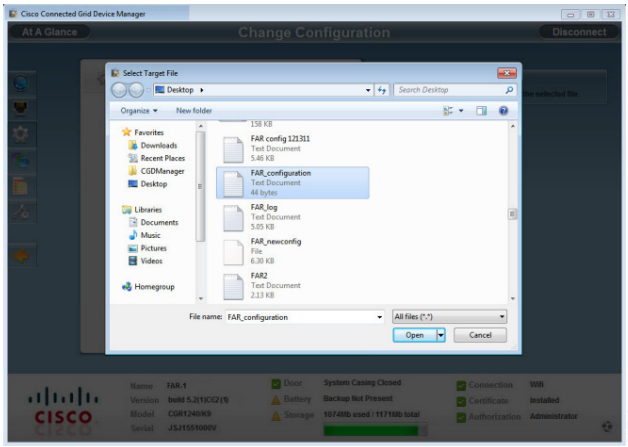
File Path: ...-uk9-gdb.5.2.1.CG1.0.267.zip

OK | Cancel

Name	FAR-1	Door	System Casing Closed	Connection	Wifi
Version	build 5.2(1)CG2(1)	Battery	Backup Not Present	Certificate	Installed
Model	CGR1240/K9	Storage	1074Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ1551000V				

Step 3 Enter a file description.

Step 4 Click to navigate to where the configuration file is located and select the file.



		158 KB
FAR config 121311	Text Document	5.46 KB
FAR_configuration	Text Document	44 bytes
FAR_log	Text Document	5.05 KB
FAR_newconfig	File	6.30 KB
FAR2	Text Document	2.13 KB

File name: FAR_configuration

All files (*.*)

Open | Cancel

Name	FAR-1	Door	System Casing Closed	Connection	Wifi
Version	build 5.2(1)CG2(1)	Battery	Backup Not Present	Certificate	Installed
Model	CGR1240/K9	Storage	1074Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ1551000V				

300719

Step 5 Click **OK**.

Change/Update Configuration

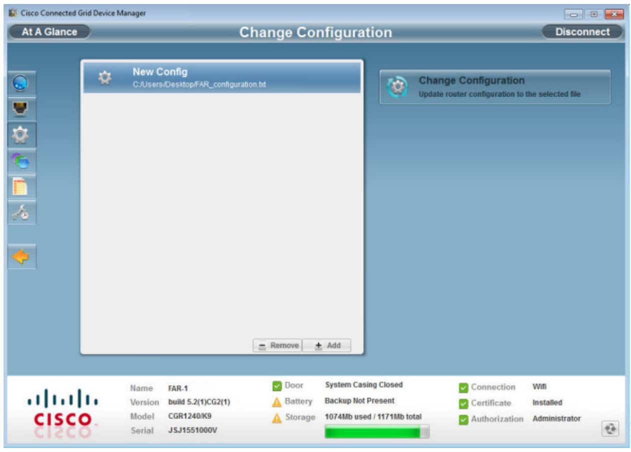
Once a configuration file has been added to Device Manager, you can then use the file to update the router configuration.

Caution Changing the router configuration will update the configuration file and reboot the FAR. All connections to the router will be lost while the configuration file is being updated.

Once this task starts, there is no way to cancel the event. Be careful when using this feature.

Follow these steps to update the FAR configuration file:

Step 1 Select the configuration file from the list.

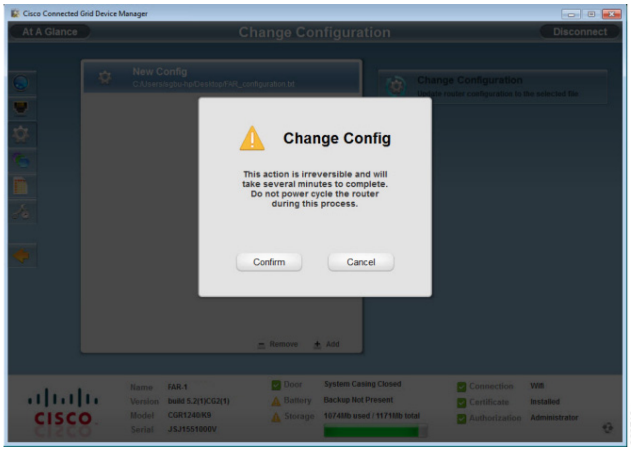


New Config
C:/Users/Desktop/FAR_configuration.txt

Change Configuration
Update router configuration to the selected file

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator

Step 2 Click **Change Configuration**.


Cisco Connected Grid Device Manager
At A Glance
Change Configuration
Disconnect
New Config
C:/Users/sgbu-hp/Desktop/FAR_configuration.txt
Change Configuration
Update router configuration to the selected file
Remove
Add
CISCO
300718

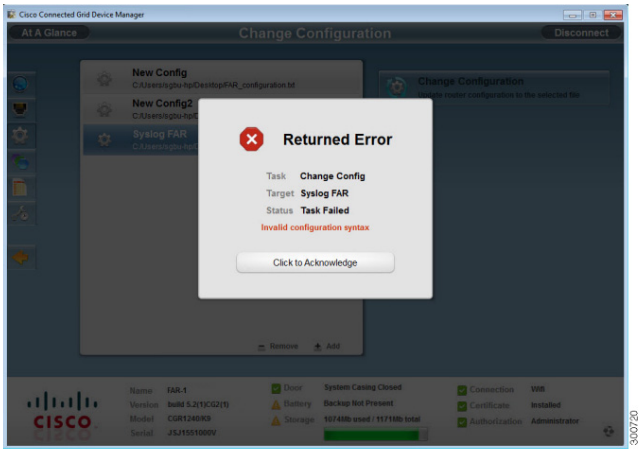
Change Config

This action is irreversible and will take several minutes to complete. Do not power cycle the router during this process.

Confirm Cancel

Step 3 Select **Confirm** to verify you would like to change the router configuration.

The following is an example error message received if the configuration file is not correct.



Returned Error

Task Change Config
Target Syslog FAR
Status Task Failed
Invalid configuration syntax

Click to Acknowledge

Cisco Connected Grid Device Manager
At A Glance
Change Configuration
Disconnect
New Config
C:/Users/sgbu-hp/Desktop/FAR_configuration.txt
New Config2
C:/Users/sgbu-hp/D
Syslog FAR
C:/Users/sgbu-hp/D
Change Configuration
Update router configuration to the selected file
Remove
Add
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator
300720

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 (see Remove Configuration, page 3-15), and then add the new (updated) configuration file to Device Manager (see Add a Configuration File, page 3-13).

Step 3 Follow the steps to update the configuration file again (see Change/Update Configuration, page 3-14).

Remove Configuration

Once a configuration file has been added and used to update a FAR, you can then remove the file from Device Manager. Use this function to remove unwanted or duplicate configuration files.

Follow these steps to remove a configuration file:

Step 1 Select the configuration file from the list.

Step 2 Click **Remove**.

Update Image

The FAR 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 image file is a zip file. The zip file contains a manifest file with information on versioning and files. Any missing files in the bundle will result in cancellation of the update process.

Add an Image

Before an image can be used to update a FAR, it must be added to Device Manager.

Follow these steps to add a router image:

Step 1 Click **Update Image** .

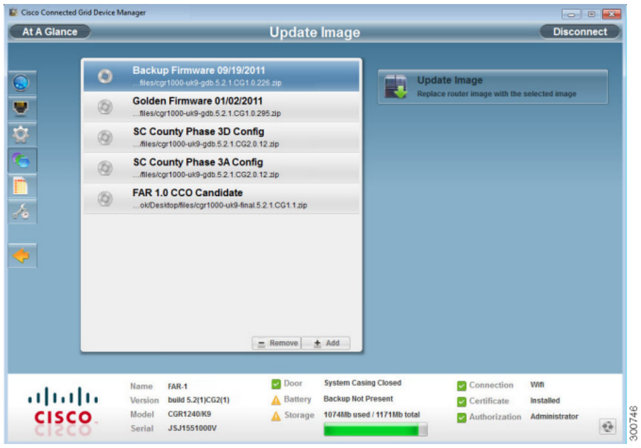
Step 2 Click **Add**.

Step 3 Enter a file description.

Step 4 Click **Browse** to navigate to where the image zip file is located.

Step 5 Click **OK**.

The image file is checked and the image is added to the Device Manager.



Backup Firmware 09/19/2011
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.226.zip

Golden Firmware 01/02/2011
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.295.zip

SC County Phase 3D Config
...files/cgr1000-uk9-gdb.5.2.1.CG2.0.12.zip

SC County Phase 3A Config
...files/cgr1000-uk9-gdb.5.2.1.CG2.0.12.zip

FAR 1.0 CCO Candidate
...ok/Desktop/files/cgr1000-uk9-final.5.2.1.CG1.1.zip

Update Image
Replace router image with the selected image

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total

Connection Wifi
Certificate Installed
Authorization Administrator

Update Image

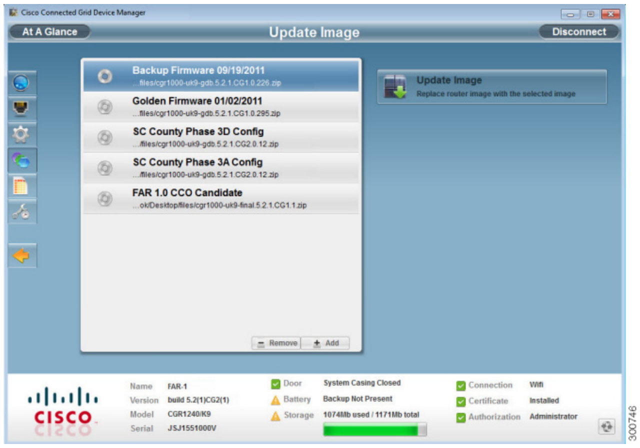
Caution Updating the router may take awhile to complete, and all connections to the router will be unavailable while the image is updating.

Once this tasks starts, there is no way to cancel the event. Be careful when using this feature.

Follow these steps to update an image:

Step 1 Select an image.

Step 2 Click **Update Image**.



Backup Firmware 09/19/2011
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.226.zip

Golden Firmware 01/02/2011
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.295.zip

SC County Phase 3D Config
.../files/cgr1000-uk9-gdb.5.2.1.CG2.0.12.zip

SC County Phase 3A Config
.../files/cgr1000-uk9-gdb.5.2.1.CG2.0.12.zip

FAR 1.0 CCO Candidate
...ok/Desktop/files/cgr1000-uk9-final.5.2.1.CG1.1.zip

Update Image
Replace router image with the selected image

Name	FAR-1	✓ Door	System Casing Closed	✓ Connection	Wifi
Version	build 5.2(1)CG2(1)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	CGR1240/K9	⚠ Storage	1074Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ1551000V				

Step 3 Click **Confirm**. The update may take awhile to update the FAR image and restart the router.

Remove Image

Once a file is used to update the image, it can be then be removed from the Device Manager. Another example may be that you added the wrong image file into Device Manager.

Follow these steps to remove an image:

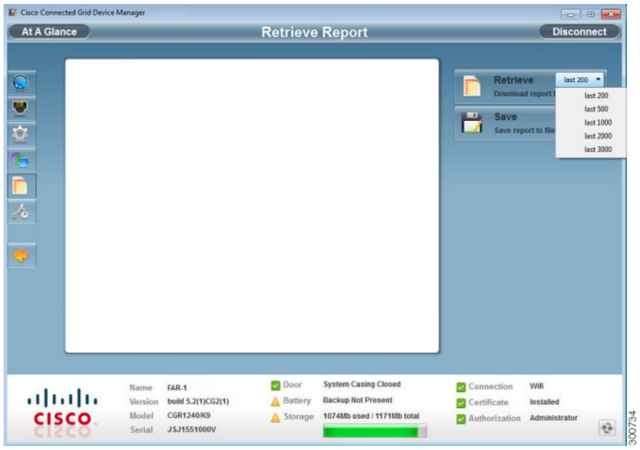
Step 1 Select an image.

Step 2 Click **Remove**.

Retrieve Report

Follow these steps to retrieve the router real-time reports:

Step 1 Click **Retrieve Report** .



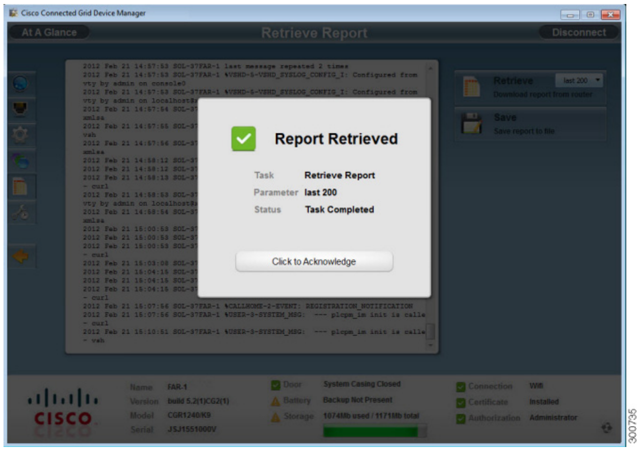
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

☑ Door System Casing Closed
⚠ Battery Backup Not Present
⚠ Storage 1074Mb used / 1171Mb total

☑ Connection Wifi
☑ Certificate Installed
☑ Authorization Administrator

Step 2 Select the number of lines in the log from the drop-down.

Step 3 Click **Retrieve** to display the report.



```
2012 Feb 21 14:57:53 SOL-37FAR-1 last message repeated 2 times
2012 Feb 21 14:57:53 SOL-37FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from
vty by admin on console0
2012 Feb 21 14:57:53 SOL-37FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from
vty by admin on localhost@
2012 Feb 21 14:57:54 SOL-37
xmlsa
2012 Feb 21 14:57:55 SOL-37
vsh
2012 Feb 21 14:57:56 SOL-37
xmlsa
2012 Feb 21 14:58:12 SOL-37
2012 Feb 21 14:58:12 SOL-37
2012 Feb 21 14:58:13 SOL-37
- curl
2012 Feb 21 14:58:53 SOL-37
vty by admin on localhost@
2012 Feb 21 14:58:54 SOL-37
xmlsa
2012 Feb 21 15:00:53 SOL-37
2012 Feb 21 15:00:53 SOL-37
2012 Feb 21 15:00:53 SOL-37
- curl
2012 Feb 21 15:03:08 SOL-37
2012 Feb 21 15:04:15 SOL-37
2012 Feb 21 15:04:15 SOL-37
2012 Feb 21 15:04:15 SOL-37
- curl
2012 Feb 21 15:07:56 SOL-37FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:07:56 SOL-37FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- curl
2012 Feb 21 15:10:51 SOL-37FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- vsh
```

✓ Report Retrieved

Task Retrieve Report
Parameter last 200
Status Task Completed

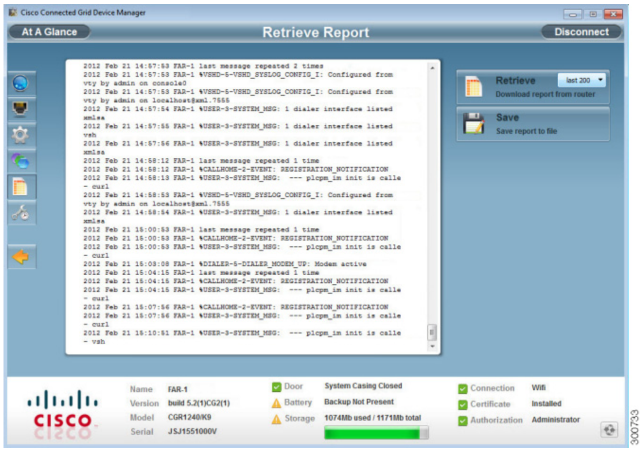
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V

☑ Door System Casing Closed
⚠ Battery Backup Not Present
⚠ Storage 1074Mb used / 1171Mb total

☑ Connection Wifi
☑ Certificate Installed
☑ Authorization Administrator

Step 4 Select **Click to Acknowledge** to view the selected report.

The following example shows 200 lines.



```
2012 Feb 21 14:57:53 FAR-1 last message repeated 2 times
2012 Feb 21 14:57:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from
vty by admin on console0
2012 Feb 21 14:57:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from
vty by admin on localhost@xml.7555
2012 Feb 21 14:57:54 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed
xmlsa
2012 Feb 21 14:57:55 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed
vsh
2012 Feb 21 14:57:56 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed
xmlsa
2012 Feb 21 14:58:12 FAR-1 last message repeated 1 time
2012 Feb 21 14:58:12 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:58:13 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- curl
2012 Feb 21 14:58:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from
vty by admin on localhost@xml.7555
2012 Feb 21 14:58:54 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed
xmlsa
2012 Feb 21 15:00:53 FAR-1 last message repeated 1 time
2012 Feb 21 15:00:53 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:00:53 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- curl
2012 Feb 21 15:03:08 FAR-1 %DIALER-5-DIALER_MODEM_UP: Modem active
2012 Feb 21 15:04:15 FAR-1 last message repeated 1 time
2012 Feb 21 15:04:15 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:04:15 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- curl
2012 Feb 21 15:07:56 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:07:56 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- curl
2012 Feb 21 15:10:51 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is calle
- vsh
```

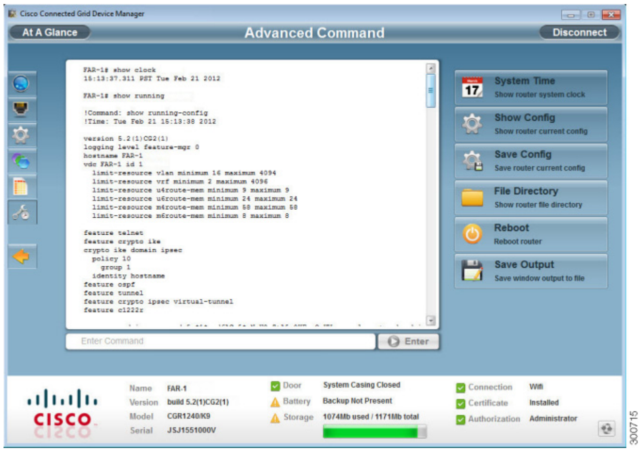
Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator

Step 5 Click **Save** to save the selected report to a file (see SYSTEMLOG.TXT SAMPLE, page 3-23) and save to your preferred directory (for example, on the Desktop).

Advanced Command

This feature is used to access the FAR to fine-tune or troubleshoot the FAR.

Note You must be familiar with Cisco NXOS commands. Issuing an incorrect command may cause the router to function incorrectly.



```
FAR-1# show clock
15:13:37.311 PST Tue Feb 21 2012

FAR-1# show running

!Command: show running-config
!Time: Tue Feb 21 15:13:38 2012

version 5.2(1)CG2(1)
logging level feature-mgr 0
hostname FAR-1
vdc FAR-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
```

Name FAR-1
Version build 5.2(1)CG2(1)
Model CGR1240/K9
Serial JSJ1551000V
Door System Casing Closed
Battery Backup Not Present
Storage 1074Mb used / 1171Mb total
Connection Wifi
Certificate Installed
Authorization Administrator

Note All interactive commands are not supported. Configuration commands must be concatenated together, as shown in the following example: `configuration terminal ; interface ethernet2/1 ; shutdown ; end` (see the *Cisco NXOS Configuration Guide* for more information).

Follow these steps to use Advanced Command:

Step 1 Click **Advanced Command** .

Step 2 You have the following choices:

- Click **System Time** to display the router system clock
- Click **Show Config** to display the current router configuration
- Click **Save Config** to save the current router configuration to a file
- Click **File Directory** to display the router file directory
- Click **Reboot** to reboot the router
- Click **Save Output** to save the output displayed in the window to a file

Advanced Command Examples

This section contains sample output examples.

WINDOWSLOG.TXT SAMPLE

The following example output shows what the windowslog.txt file looks when saved from the Advance Commands page.

```
FAR-1# show clock
15:13:37.311 PST Tue Feb 21 2012

FAR-1# show running

!Command: show running-config
!Time: Tue Feb 21 15:13:38 2012

version 5.2(1)CG2(1)
logging level feature-mgr 0
hostname FAR-1
vdc FAR-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 5 $1$pxdfACg5$sNmH2rZtA5o9KFzeQwKVn.  role network-admin
```

```
no password strength-check
ip domain-lookup
ip host nms.cisco.com 192.168.193.11
crypto key param rsa label SolCA modulus 2048
crypto ca trustpoint SolCA
     enrollment profile SolCA
     rsakeypair SolCA  2048
     revocation-check  none
     enrollment retry count 3
     enrollment retry period 5
     serial-number
     fingerprint F2:33:14:78:7B:D9:8B:99:AF:1F:E0:B2:D3:38:96:1D:12:5E:AE:51
crypto ca profile enrollment SolCA
     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 0x4bcbbcd51d08af57a8fd93a26be558c1 priv
0x4bcbbcd51d08af57a8fd93a26be558c1 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 SolCA
  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 SolCA
ip http secure-server
ip http secure-port 8443
ip http secure-server trustpoint SolCA
```

SYSTEMLOG.TXT SAMPLE

The following example output shows what the systemlog.txt file looks when saved from the Advance Commands page.

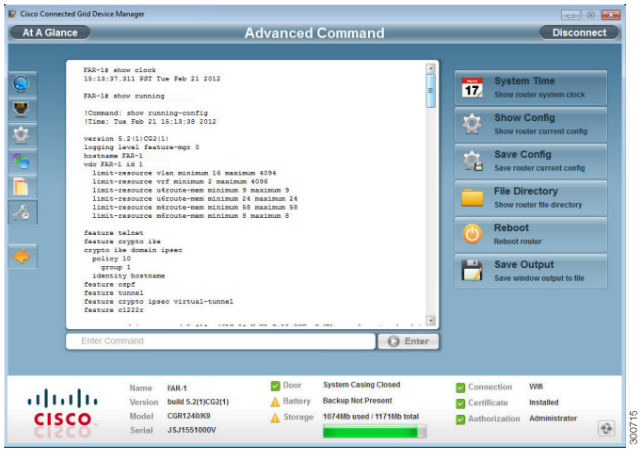
```
2012 Feb 21 14:44:12 FAR-1 Feb 21 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456678]  - kernel
2012 Feb 21 14:44:12 FAR-1 Feb 21 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456830]
/1_0_cdma_qos/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/drivers/i2c/busses/ioh/
ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2012 Feb 21 14:44:12 FAR-1 Feb 21 14:44:12 %KERN-3-SYSTEM_MSG: [ 1293.456847]  - kernel
2012 Feb 21 14:44:13 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:47:02 FAR-1 last message repeated 1 time
2012 Feb 21 14:47:31 FAR-1 last message repeated 2 times
```

```
2012 Feb 21 14:47:31 FAR-1 %PLATFORM-2-DISK_ALERT: Disk Status Alert : disk partition
'/bootflash' is at high usage level (91%).
2012 Feb 21 14:47:31 FAR-1 %CALLHOME-2-EVENT: LOW_FLASH_SPACE
2012 Feb 21 14:47:31 FAR-1 %PLATFORM-2-DISK_ALERT: Disk Status Alert : disk partition
'/isan' is at high usage level (91%).
2012 Feb 21 14:47:32 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:47:57 FAR-1 last message repeated 1 time
2012 Feb 21 14:47:57 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:47:57 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:48:01 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - dcos-ping
2012 Feb 21 14:49:39 FAR-1 last message repeated 2 times
2012 Feb 21 14:50:20 FAR-1 last message repeated 1 time
2012 Feb 21 14:50:20 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:50:21 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - dcos-ping
2012 Feb 21 14:50:34 FAR-1 last message repeated 1 time
2012 Feb 21 14:50:34 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:50:37 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - dcos-ping
2012 Feb 21 14:50:38 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:51:15 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - rm
2012 Feb 21 14:51:16 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - java
2012 Feb 21 14:51:16 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - pidof
2012 Feb 21 14:51:20 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:51:30 FAR-1 last message repeated 1 time
2012 Feb 21 14:51:30 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:51:31 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:51:38 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - su
2012 Feb 21 14:51:38 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - xmlsa
2012 Feb 21 14:51:39 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called -
dcos-traceroute
2012 Feb 21 14:52:11 FAR-1 last message repeated 1 time
2012 Feb 21 14:52:25 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:52:32 FAR-1 last message repeated 1 time
2012 Feb 21 14:52:32 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:52:33 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:52:33 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:53:10 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - vsh
2012 Feb 21 14:53:56 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:53:56 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:54:32 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:55:58 FAR-1 last message repeated 2 times
2012 Feb 21 14:55:58 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:55:59 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:57:13 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:57:53 FAR-1 last message repeated 2 times
2012 Feb 21 14:57:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
console0
2012 Feb 21 14:57:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
localhost@xml.7555
2012 Feb 21 14:57:54 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:57:55 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - vsh
2012 Feb 21 14:57:56 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 14:58:12 FAR-1 last message repeated 1 time
2012 Feb 21 14:58:12 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 14:58:13 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 14:58:53 FAR-1 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
localhost@xml.7555
2012 Feb 21 14:58:54 FAR-1 %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmlsa
2012 Feb 21 15:00:53 FAR-1 last message repeated 1 time
2012 Feb 21 15:00:53 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:00:53 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 15:03:08 FAR-1 %DIALER-5-DIALER_MODEM_UP: Modem active
2012 Feb 21 15:04:15 FAR-1 last message repeated 1 time
2012 Feb 21 15:04:15 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:04:15 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
```

```
2012 Feb 21 15:07:56 FAR-1 %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
2012 Feb 21 15:07:56 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - curl
2012 Feb 21 15:10:51 FAR-1 %USER-3-SYSTEM_MSG:  --- plcpm_im init is called - vsh
```

Disconnect from the FAR

Once you have finished all work required on an individual FAR, click **Disconnect** on the upper right-hand to disconnect from Device Manager. To connect to a different FAR, follow the steps on Device Manager Overview, page 3-1.



```
FAR-1# show clock
15:13:37.311 PST Tue Feb 21 2012

FAR-1# show running

!Command: show running-config
!Time: Tue Feb 21 15:13:38 2012

version 5.2(1)CG2(1)
logging level feature-mgr 0
hostname FAR-1
vdc FAR-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
```

Name	FAR-1	✓ Door	System Casing Closed	✓ Connection	Wifi
Version	build 5.2(1)CG2(1)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	CGR1240/K9	⚠ Storage	1074Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ1551000V				

Frequently Asked Questions

This section contains information on frequently asked questions of the Device Manager.

"How do I check if the certificate is installed?"

See Certificate Installation, page 2-2.

"After I clicked Connect, I received a connection error message"

If the Device Manager is connected to the FAR over Ethernet and the IP address is configured, ensure that you can 'ping' this IP address from the Device Manager computer. If the the IP address is auto-detected, ensure that the Device Manager computer Ethernet is connected to the FAR directly, and that FAR interface is configured with *ipv6 address use-link-local-only.*

If the Device Manager is connected to the FAR using WiFi, first ensure the WiFi parameters (ssid and paraphrase) match the configuration of the FAR. If you still cannot connect using WiFi, ensure the Windows Wireless Zero Configuration is enabled on the computer.

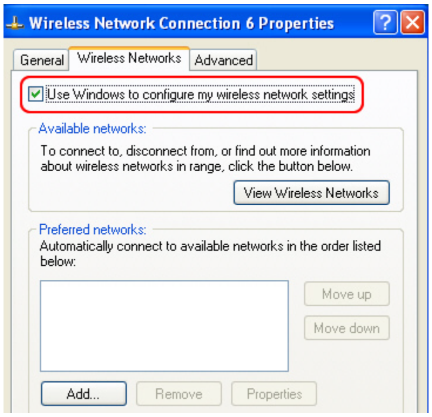
Ensure there is no third-party wireless client tool controlling the WiFi interface. For example, if you are using a third-party client tool (such as Intel PROSet Wireless Client Tool), change the settings from that tool to enable Windows Wireless Zero Configuration.

You can also refer to the following steps to enable Windows Wireless Zero Configuration:

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**.

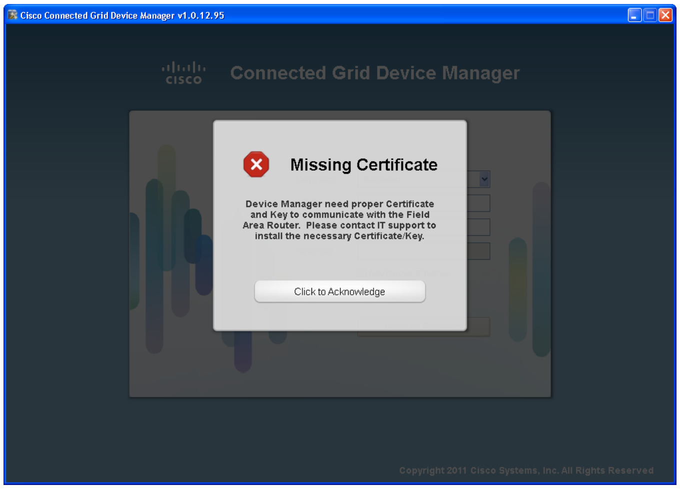
Step 5 Click **Wireless Networks** tab.

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 into Device Manager"

The following message displays when you try to log into Device Manager:



Cisco Connected Grid Device Manager v1.0.12.95
Connected Grid Device Manager

Missing Certificate

Device Manager need proper Certificate and Key to communicate with the Field Area Router. Please contact IT support to install the necessary Certificate/Key.

Click to Acknowledge
Copyright 2011 Cisco Systems, Inc. All Rights Reserved

See Certificate Installation, page 2-2 for details on installing the certificate.

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