Cisco Connected Grid Device Manager Installation and User Guide

January 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

Cisco Connected Grid Device Manager Installation and User Guide

CONTENTS

CHAPTER 1

Introduction 1-1

Overview 1-1

Field Area Router 1-2

Connectivity 1-2

CHAPTER 2

Installation 2-1

Required Expertise 2-1

System Requirements 2-1

Certificate Installation 2-2

Device Manager Installation 2-3

Device Manager Removal 2-4

CHAPTER 3

Using the Device Manager 3-1

Connect to the Device Manager 3-2

The Device Manager 3-3

Task Pad 3-4

Test Connectivity 3-5

Add a Target IP Address 3-5

Ping an IP Address 3-8

Traceroute an IP Address 3-9

Remove a Target IP Address 3-10

Manage Interfaces 3-11

Bring Up an Interface 3-12

Shut Down an Interface 3-13

Change Configuration 3-14

Add a Configuration File 3-14

Change Configuration 3-15

Remove Configuration 3-16

Update Image 3-17

Add a Image 3-17

Update Image 3-18

Remove Image 3-20

Retrieve Report 3-21

Advanced Commands 3-22

Examples 3-22

Disconnect from Device Manager 3-24

Troubleshooting 3-25

CHAPTER 1

Introduction

The Cisco Connected Grid Device Manager is a tool used by field technicians to troubleshoot Field Area Routers (FARs). This chapter contains the following topics:

- Overview
- Connectivity

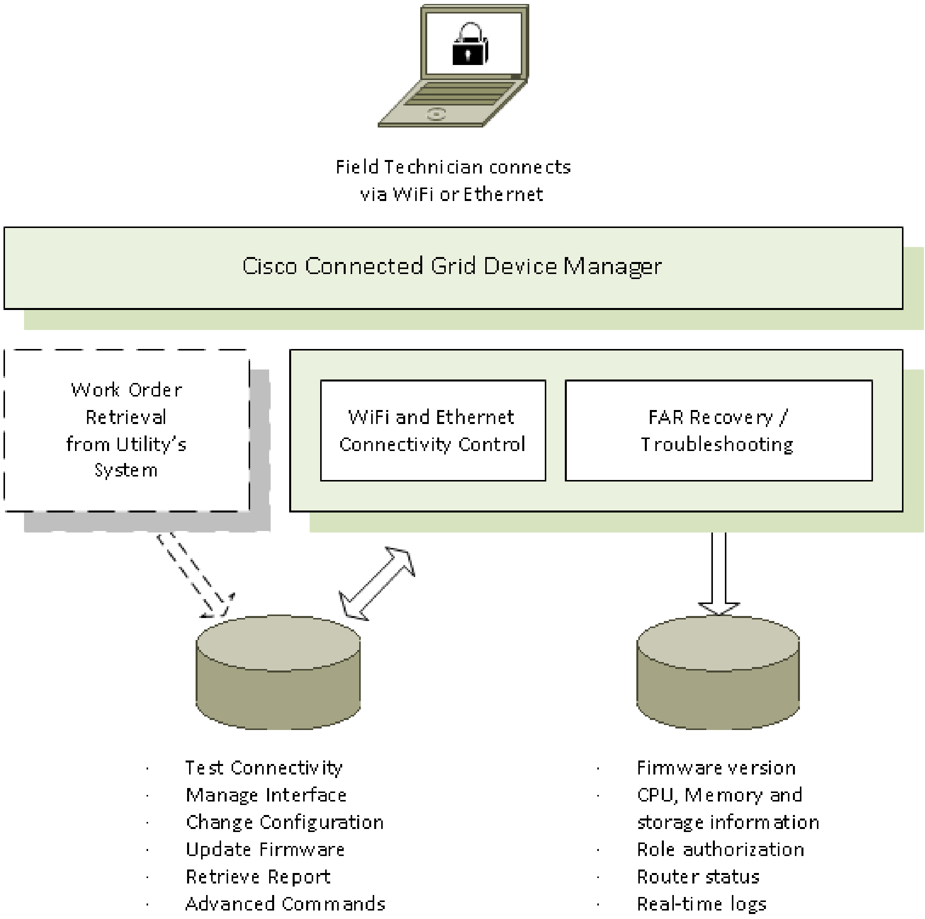
Overview

The Cisco Device Manager is an advanced application used to communicate with FARs. The Device Manager stores configuration information of each registered FAR, displays data, and manages individual FARs through remote, secure communications.

The Device Manager uses a secured Ethernet or WiFi link to connect to a managed FAR for first time deployment or troubleshooting. This tool enables field technicians to manage FARs remotely. The Device Manager restores configuration, reboots the managed FAR, and uploads new image to a FAR.

Note Work order retrieval from the utility's system, such as the Cisco Connected Grid Network Management System, will not be implemented in this release. The field technician must enter the FAR data manually.

The following figure illustrates the features of the Device Manager.



Field Area Router

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

Connectivity

You can connect to the Device Manager either by Ethernet or WiFi. The WiFi connectivity control ensures data traffic between Device Manager and the FAR are protected by WPA Layer 2 security using an asymmetric Pre-Shared Key (PSK) security, once the association and key handshake is complete. The Ethernet connection is secured by https only.

CHAPTER 2

Installation

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

- Required Expertise, page 2-1
- System Requirements, page 2-1
- Certificate Installation, page 2-2
- Device Manager Installation, page 2-3
- Device Manager Removal, page 2-4

Required Expertise

This guide is intended for Field Technicians who have experience with Cisco Field Area Routers (Connected Grid Routers).

System Requirements

The Device Manager has the following system requirements:

- Microsoft Windows XP (Service Pack 3) or Windows 7 with IPv6 enabled on network adapters
- 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

Certificate Installation

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

Note The FAR needs to be properly configured and have the client identity and CA certificates installed to work with the Device Manager. The FAR should be deployed with factory default configurations, which will enable the FAR to communicate with the Device Manager.

To install the certificate on the Device Manager laptop:

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 such as *Cisco123*).

Step 2 Copy the certificate to the laptop, for example to the Desktop.

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

Step 4 Enter the following information:

- Protection password
- Unmark the ‘Enable strong private key protection’
- Mark ‘Include all extended properties’
- Click **Next**

Step 5 Keep the default setting ‘Automatically select the certificate store based on the type of certificate.’ Click **Next**, accept warnings, and then click **Finish**.

Step 6 Verify the client certificate for the Internet Explorer browser:

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

Step 7 Verify the CA certificate in the Internet Explorer browser:

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

Step 8 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 installation directory for the Device Manager is hidden, by default. To view the installation 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**.

Step 9 Configure the C:\ProgramData\Cisco\CGDManager\CGDmanager.ini to specify which certificates to be used for https communication. If you do not know, check your client certificate at the IE browser (see above step). Look at the ‘Issued To’ field and assign this string to CERT_COMMON_NAME.

```
[CGDM]
CERT_COMMON_NAME=ConnGridDevMgr
CA_COMMON_NAME=--AutoDetect--
```

Note Specify the CA_COMMON_NAME certificate, or leave it as '--AutoDetect--'.

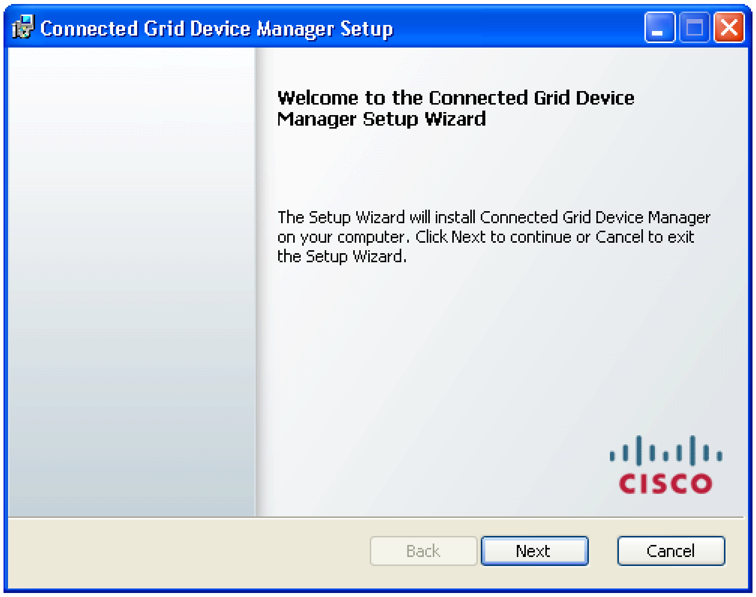
Step 10 If the .ini cannot be saved, this is due to non-native Windows 7 permission issues. Right-click the .ini file, select the 'Properties\Security\Edit', select the user group, and set the permissions for that group to be 'Full Control'.

Device Manager Installation

To install the Device Manager:

Step 1 Double-click Cisco Device Manager Installer to start installation.

Step 2 Click **Next**.

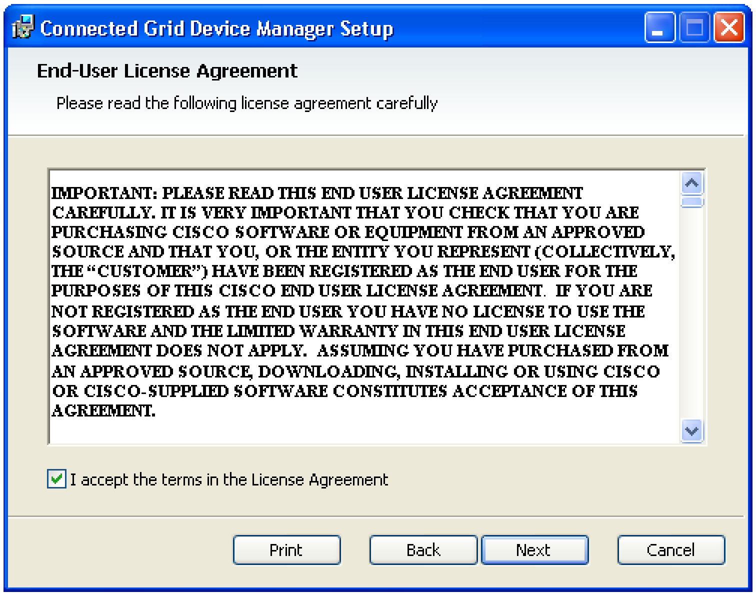


Connected Grid Device Manager Setup

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**.



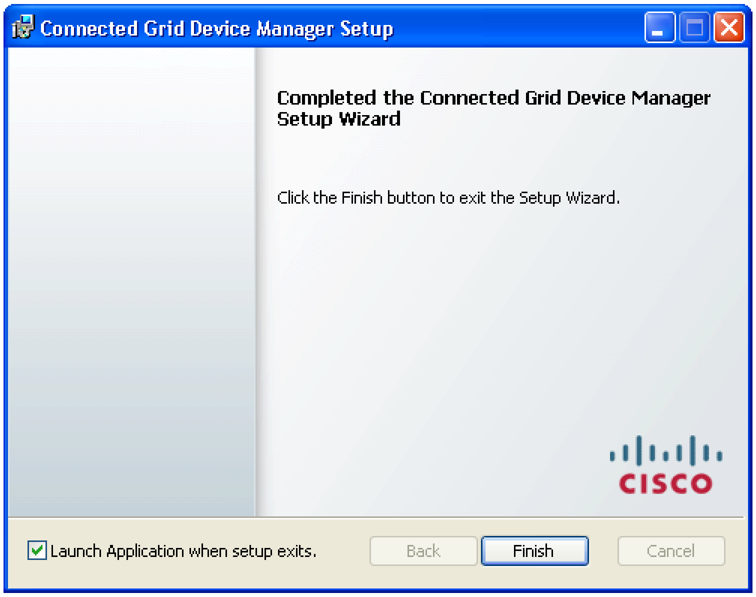
End-User License Agreement

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 Element Manager.



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

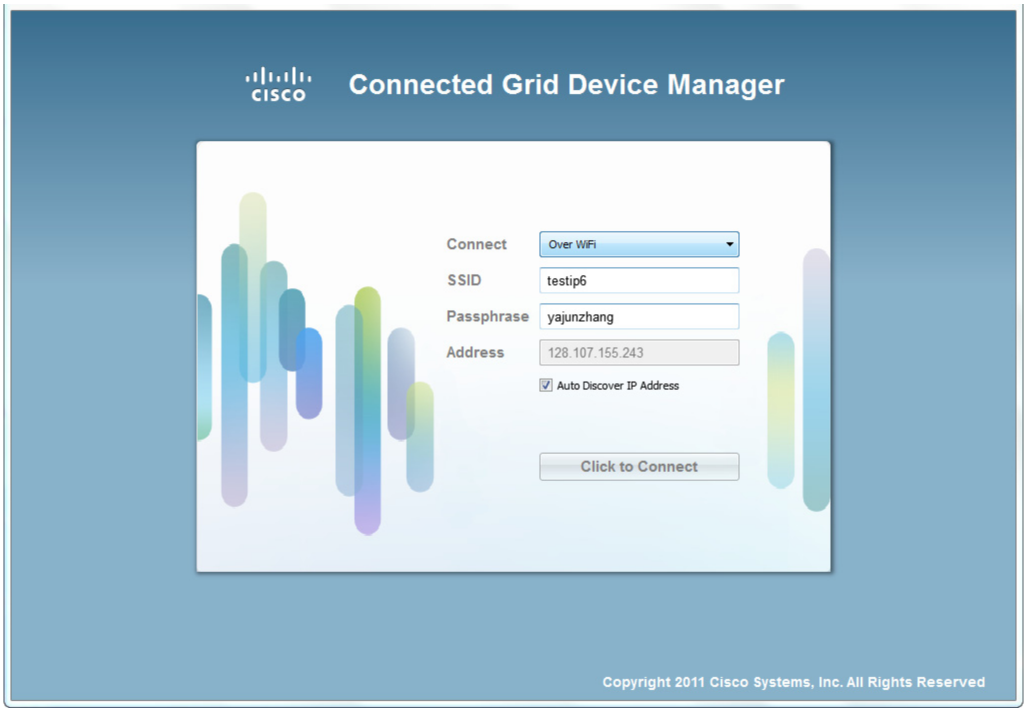
The chapter explains the functionality of Cisco Connected Grid Device Manager, and contains the following topics:

- Connect to the Device Manager, page 3-2
- The Device Manager, page 3-3
- Task Pad, page 3-4
- Test Connectivity, page 3-5
- Manage Interfaces, page 3-11
- Change Configuration, page 3-14
- Update Image, page 3-17
- Retrieve Report, page 3-21
- Advanced Command, page 3-22
- Disconnect from Device Manager, page 3-25
- Troubleshooting, page 3-26

Connect to the Device Manager

To connect to the Device Manager:

Step 1 Double-click Cisco CGD Manager from the desktop, or select **Start** > **All Programs** > **Cisco CGD Manager**.



Connected Grid Device Manager

Connect: Over WiFi

SSID: testip6

Passphrase: yajunzhang

Address: 128.107.155.243

☑ Auto Discover IP Address

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

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

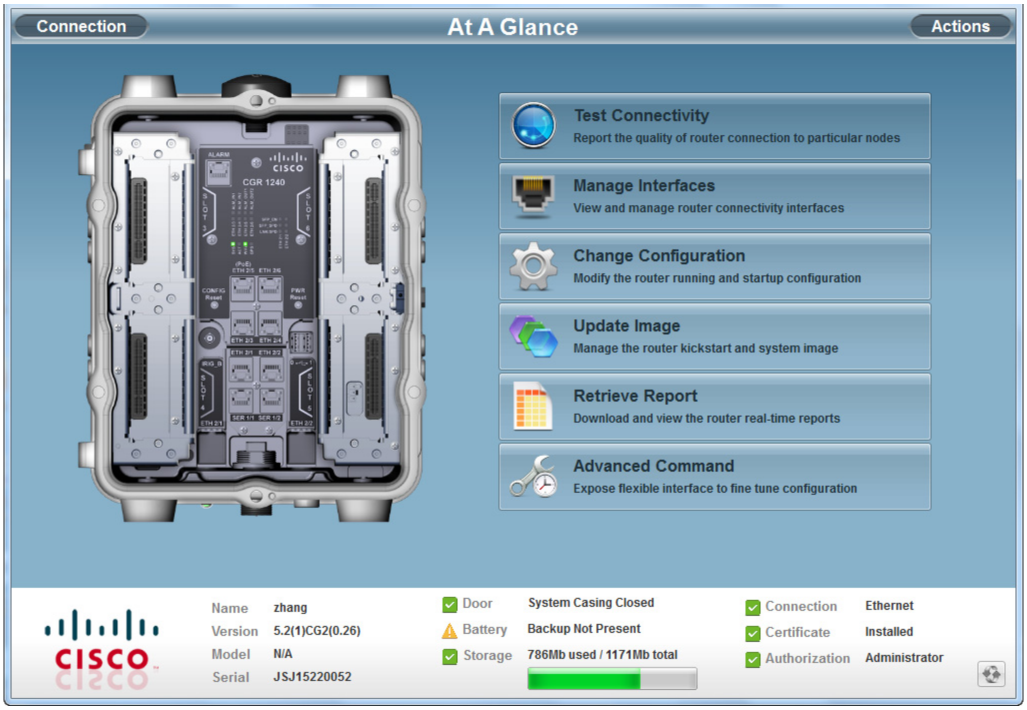
Step 4 *Optional*. Enter the address, or select the checkbox to auto-detect the address. Address values can be an IP address, pole top serial number, or a street address.

Note When Auto Detect is selected, the Device Manager laptop must be connected directly to the FAR via Ethernet or WiFi to automatically located the IP address.

Step 5 Click **Connect**.

The Device Manager

The Device Manager main screen displays after securely connecting.


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
CISCO

Name zhang
Version 5.2(1)CG2(0.26)
Model N/A
Serial JSJ15220052

✓ Door System Casing Closed
⚠ Battery Backup Not Present
✓ Storage 786Mb used / 1171Mb total

✓ Connection Ethernet
✓ Certificate Installed
✓ Authorization Administrator

At the bottom of the screen the FAR information displays:

Table 3-1 Device Manager Information

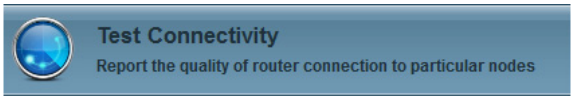
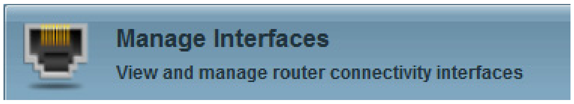
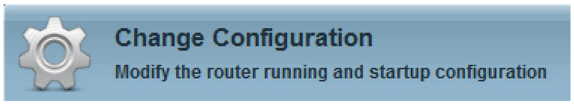
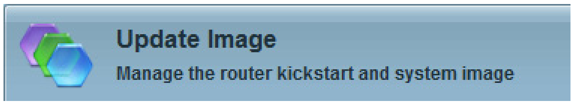
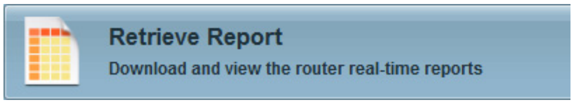
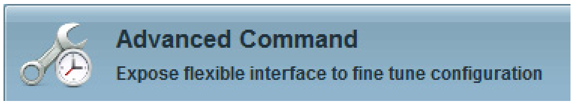
Item	Description	Example
Name	Router name	router
Version	Image version	5.2(1)CG1(0.266)
Model	Router model	CGR1240K9
Serial	Router serial number	JSJ1538000R
Door	Status of the door	System Casing Closed
Battery	Status of the battery	Backup present
Storage	Amount of storage available	605Mb used / 1015 Mb total
Connection	Method of connection	Ethernet
Certificate	Utility signed certificate	Installed
Authorization	Role of authorized user	Administrator

Note The Refresh icon, located on the lower right side, can be used at any time to refresh the FAR information.

Task Pad

The following table lists the available tasks:

Table 3-2 Device Manager Task pad

Task	Description
 Test Connectivity Report the quality of router connection to particular nodes	Reports the link connectivity and quality of the target IP address. This feature helps the Field Technician confirm and re-check the connectivity through troubleshooting. **NOTE**: Ping and traceroute are initiated from the CGR, and not the laptop that the Device Manager is running on.
 Manage Interfaces View and manage router connectivity interfaces	Shuts down or brings the interface up.
 Change Configuration Modify the router running and startup configuration	Updates the FAR configuration with a provided configuration file.
 Update Image Manage the router kickstart and system image	Updates the FAR with an image provided by the Field Technician. The upgrade allows a complete refresh to the FAR with the designated image.
 Retrieve Report Download and view the router real-time reports	Displays logging information.
 Advanced Command Expose flexible interface to fine tune configuration	CLI commands to troubleshoot the router. The Field Technician can select from the list or enter any CLI command (see Advanced Command, page 3-22).

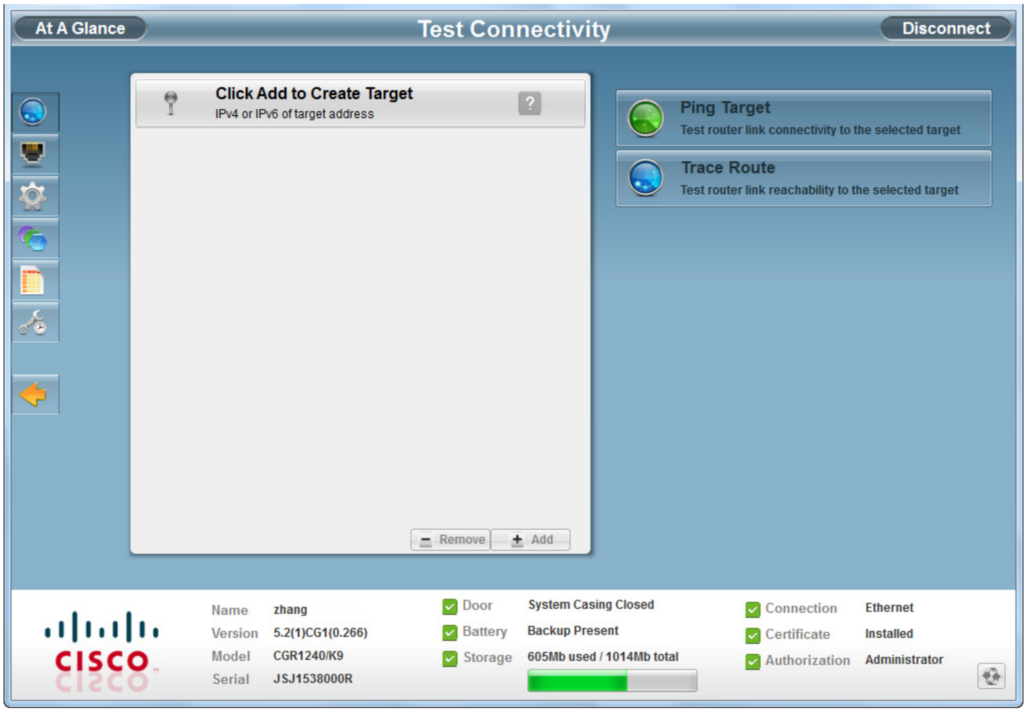
Test Connectivity

This feature reports the link connectivity and quality of the target IP address, and is used to confirm and re-check the connectivity through troubleshooting. Before you can check the connection or route to a FAR, you must add a target IP address.

Add a Target IP Address

To add a target IP address (the FAR you are trying to reach):

Step 1 Click **Test Connectivity** .



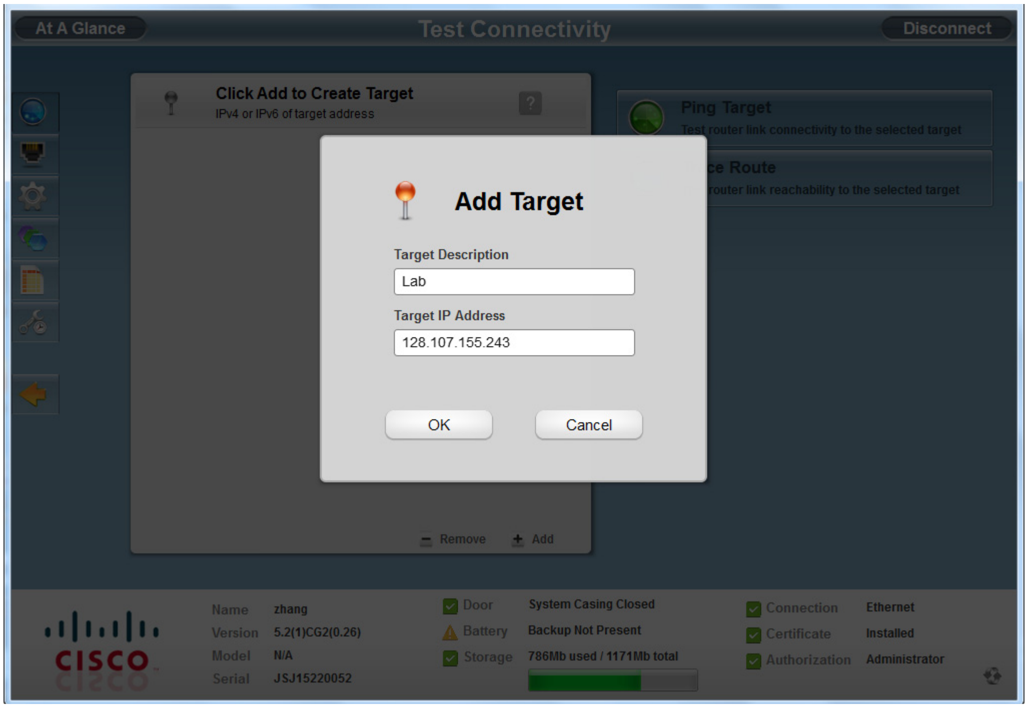
Click Add to Create Target
IPv4 or IPv6 of target address

Ping Target
Test router link connectivity to the selected target

Trace Route
Test router link reachability to the selected target

Name	zhang	☑ Door	System Casing Closed	☑ Connection	Ethernet
Version	5.2(1)CG1(0.266)	☑ Battery	Backup Present	☑ Certificate	Installed
Model	CGR1240/K9	☑ Storage	605Mb used / 1014Mb total	☑ Authorization	Administrator
Serial	JSJ1538000R				

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


At A Glance
Test Connectivity
Disconnect
Click Add to Create Target
IPv4 or IPv6 of target address
?
Ping Target
Test router link connectivity to the selected target
ce Route
router link reachability to the selected target
Add Target
OK
Cancel
Remove
Add

Target Description: Lab

Target IP Address: 128.107.155.243

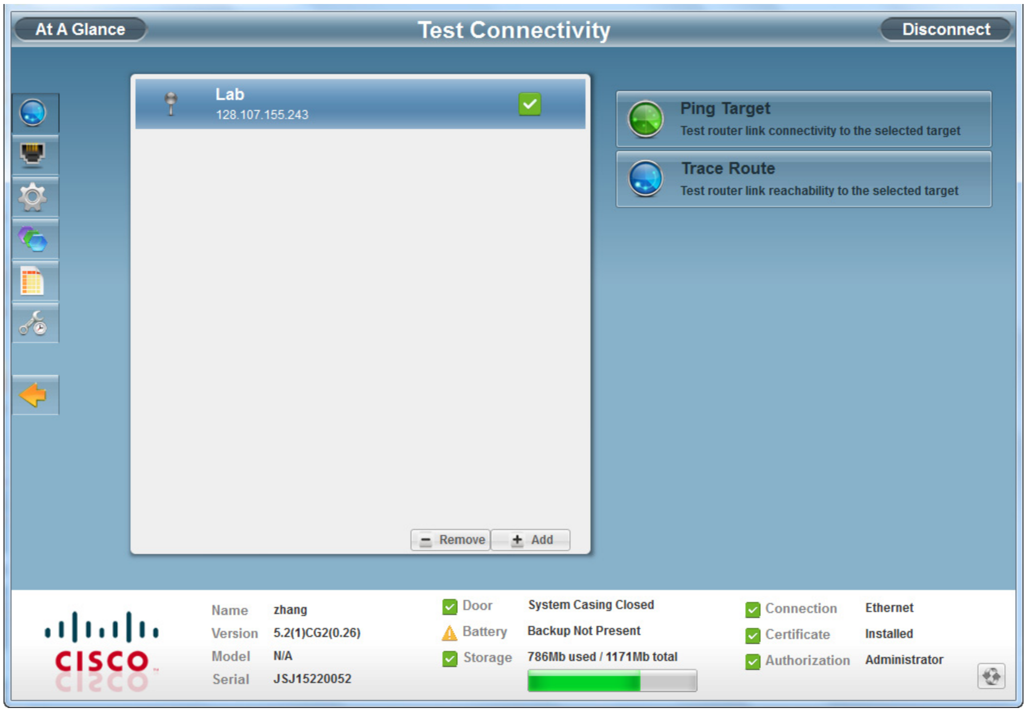
Name	zhang	Door	System Casing Closed	Connection	Ethernet
Version	5.2(1)CG2(0.26)	Battery	Backup Not Present	Certificate	Installed
Model	N/A	Storage	786Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ15220052				

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

Step 4 Enter the Target IP Address (FAR IP address).

Step 5 Click **OK**.

Connectivity to the IP address is verified and displays with a green checkmark to the right of the target IP address. If the IP address is unreachable, the icon to the right displays as a red slash.


At A Glance
Test Connectivity
Disconnect
Ping Target
Test router link connectivity to the selected target
Trace Route
Test router link reachability to the selected target
Remove
Add
cisco

Lab ✓
128.107.155.243

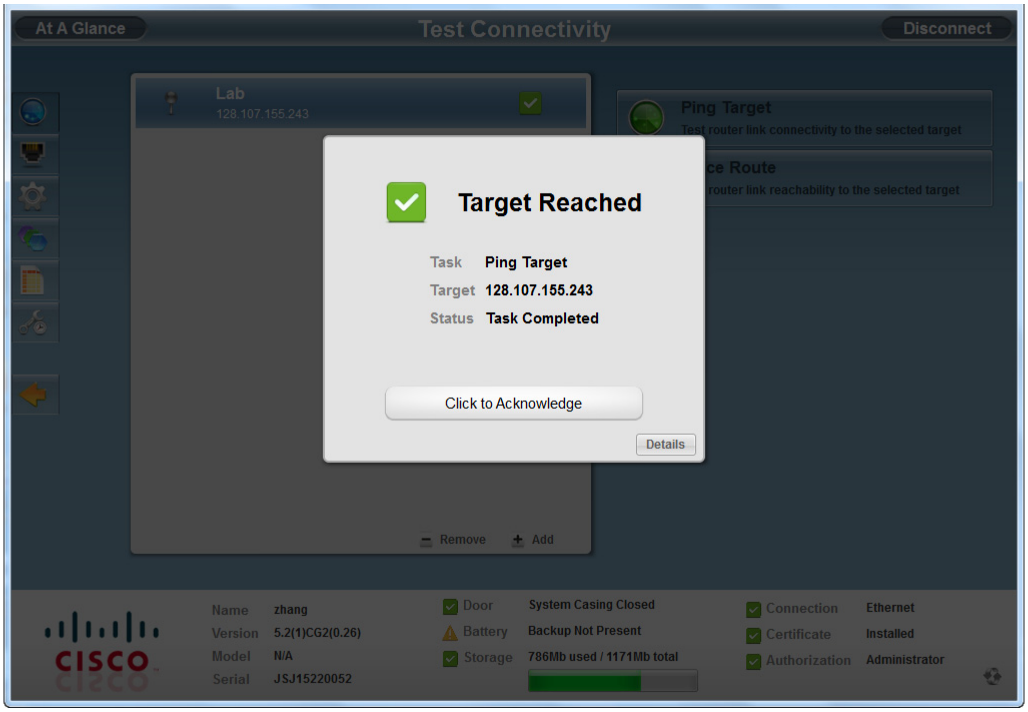
Name	zhang	✓ Door	System Casing Closed	✓ Connection	Ethernet
Version	5.2(1)CG2(0.26)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	N/A	✓ Storage	786Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ15220052				

Ping an IP Address

To test the router link connectivity to a selected IP address:

Step 1 Select the target IP address from the list.

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



Lab
128.107.155.243

Ping Target
Test router link connectivity to the selected target

ce Route
router link reachability to the selected target

Target Reached

Task	Ping Target
Target	128.107.155.243
Status	Task Completed

Name	zhang
Version	5.2(1)CG2(0.26)
Model	N/A
Serial	JSJ15220052

✓	Door	System Casing Closed
⚠	Battery	Backup Not Present
✓	Storage	786Mb used / 1171Mb total

✓	Connection	Ethernet
✓	Certificate	Installed
✓	Authorization	Administrator

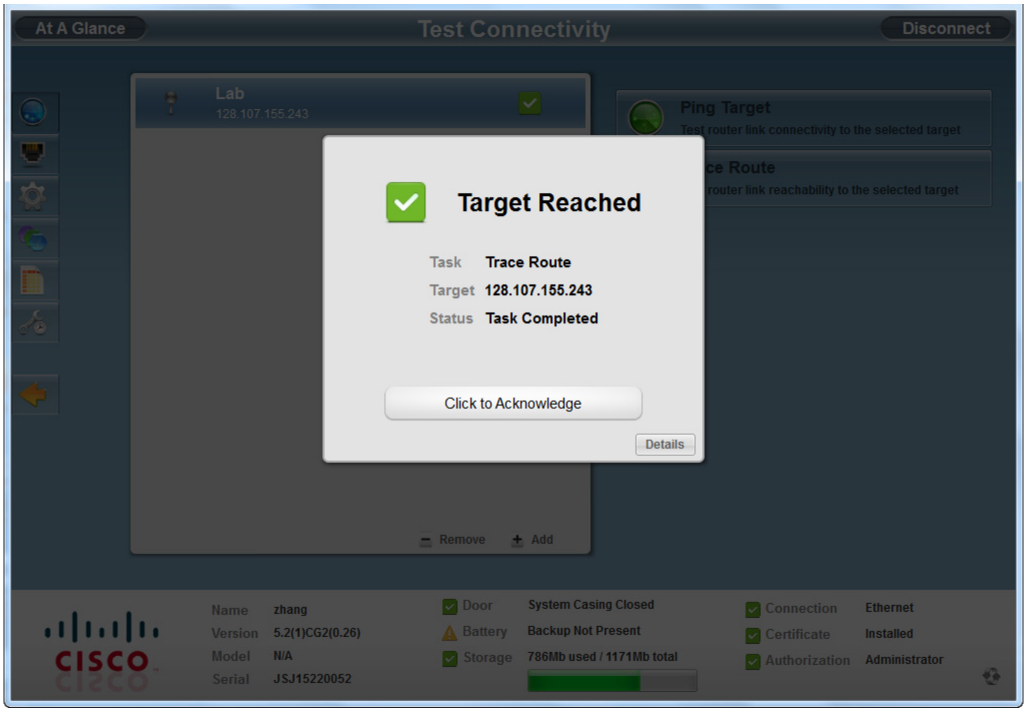
Step 3 Select **Click to Acknowledge** that the target IP address was reached. You can also click **Details** to view the the ping/traceroute details.

Traceroute an IP Address

To trace the route of the IP address:

Step 1 Select the target IP address from the list.

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


At A Glance
Test Connectivity
Disconnect
Lab
128.107.155.243
Ping Target
Test router link connectivity to the selected target
ce Route
router link reachability to the selected target
Remove
Add

Target Reached

Task	Trace Route
Target	128.107.155.243
Status	Task Completed

Name	zhang	Door	System Casing Closed	Connection	Ethernet
Version	5.2(1)CG2(0.26)	Battery	Backup Not Present	Certificate	Installed
Model	N/A	Storage	786Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ15220052				

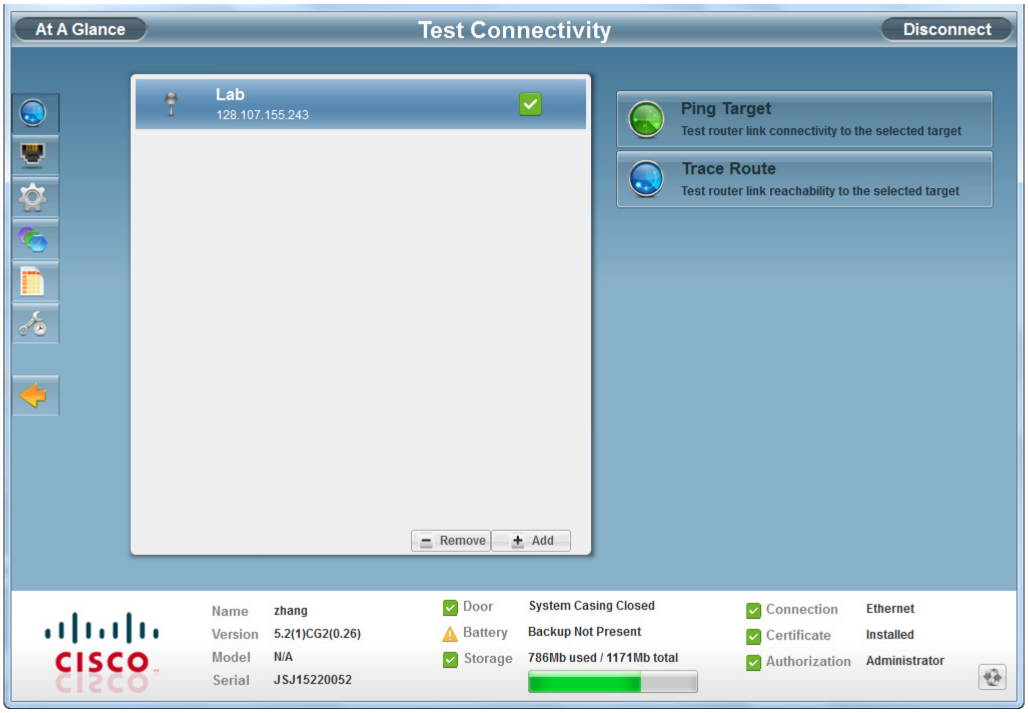
Step 3 Select **Click to Acknowledge** that the target IP address was reached.

You can also click **Details** to view the the ping/traceroute details.

Remove a Target IP Address

To remove a target IP address:

Step 1 Select the target IP address from the list.



Lab
128.107.155.243

Ping Target
Test router link connectivity to the selected target

Trace Route
Test router link reachability to the selected target

Name	zhang	✓ Door	System Casing Closed	✓ Connection	Ethernet
Version	5.2(1)CG2(0.26)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	N/A	✓ Storage	786Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ15220052				

Step 2 Click **Remove**.

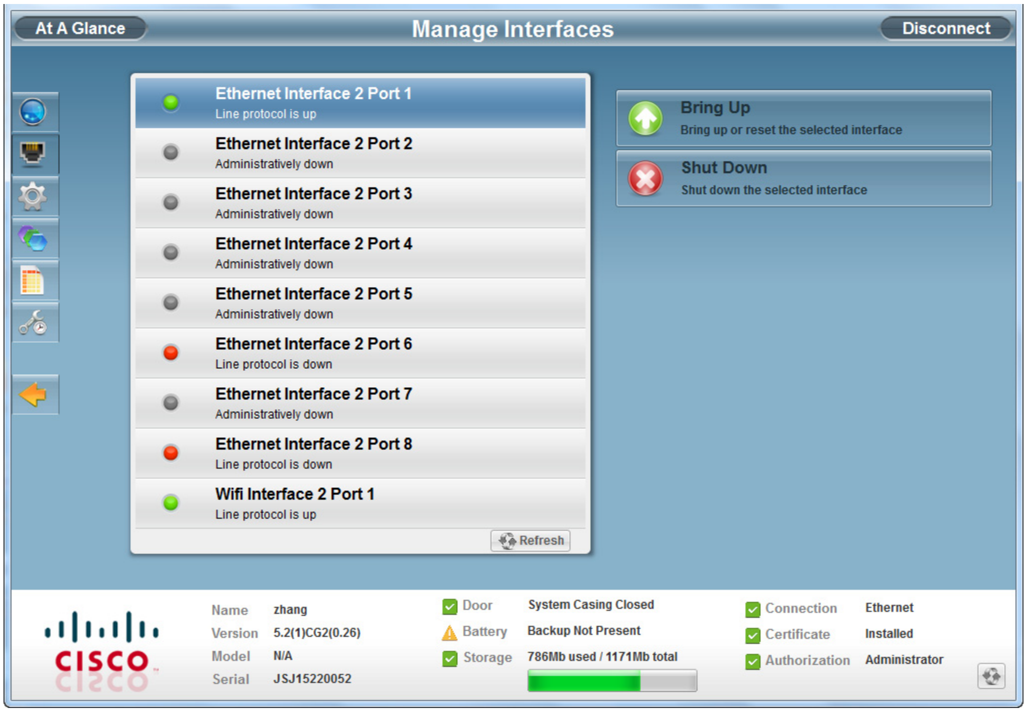
Manage Interfaces

The feature is used to bring up or shut down an interface. The status of the interface is as follows:

- Green means the line protocol is up
- Red means the line protocol is down
- Grey means the interface is shut down

To view or manage selected router interfaces:

Step 1 Click **Manage Interfaces** .



At A Glance | Manage Interfaces | Disconnect

	Interface	Status
●	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	Administratively down
●	Ethernet Interface 2 Port 6	Line protocol is down
●	Ethernet Interface 2 Port 7	Administratively down
●	Ethernet Interface 2 Port 8	Line protocol is down
●	Wifi Interface 2 Port 1	Line protocol is up

Refresh

Bring Up
Bring up or reset the selected interface

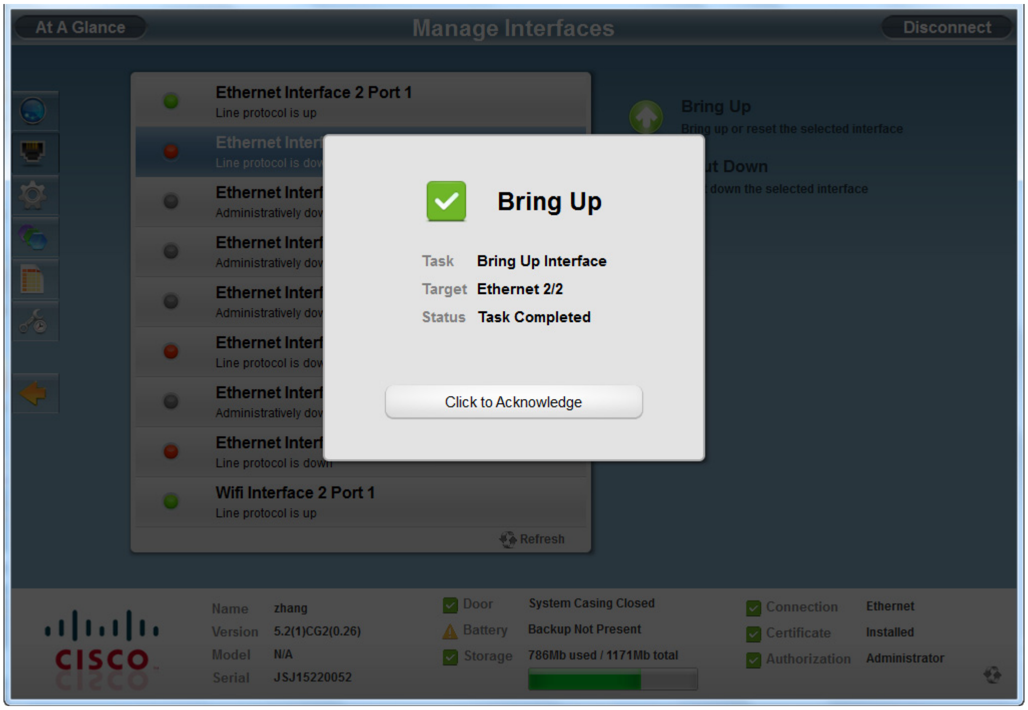
Shut Down
Shut down the selected interface

Name	zhang	✓ Door	System Casing Closed	✓ Connection	Ethernet
Version	5.2(1)CG2(0.26)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	N/A	✓ Storage	786Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ15220052				

Bring Up an Interface

To bring up an interface:

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



Bring Up

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

Name	zhang	Door	System Casing Closed	Connection	Ethernet
Version	5.2(1)CG2(0.26)	Battery	Backup Not Present	Certificate	Installed
Model	N/A	Storage	786Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ15220052				

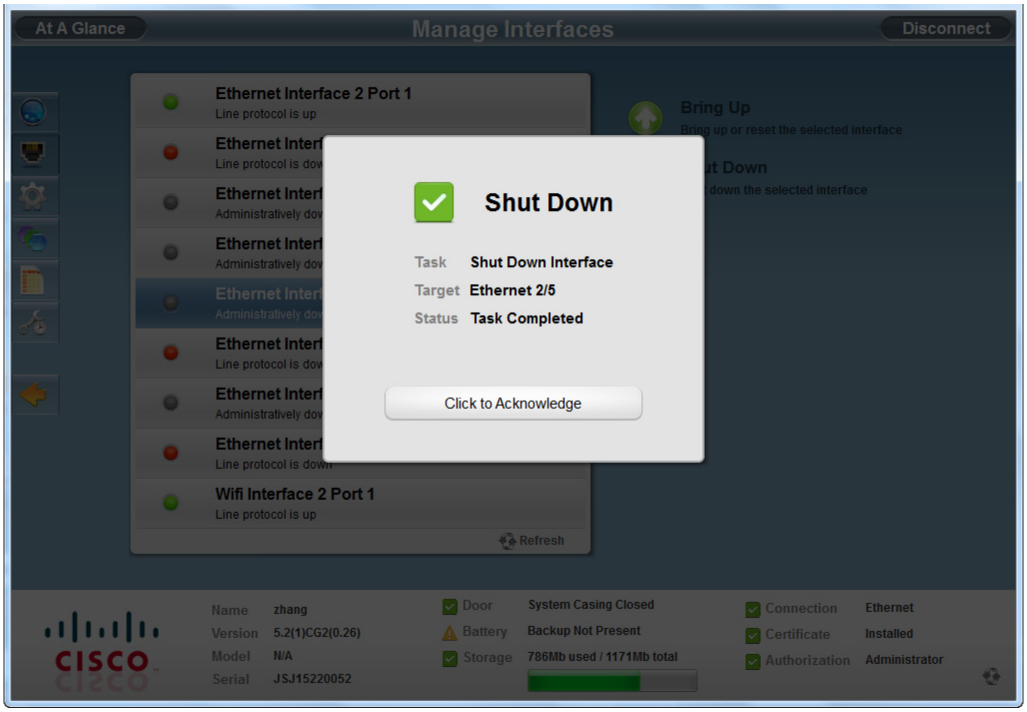
Step 2 Select **Click to Acknowledge**.

Shut Down an Interface

To shut down an interface:

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

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



Shut Down

Task Shut Down Interface
Target Ethernet 2/5
Status Task Completed

Name zhang
Version 5.2(1)CG2(0.26)
Model N/A
Serial JSJ15220052

✓ Door System Casing Closed
⚠ Battery Backup Not Present
✓ Storage 786Mb used / 1171Mb total

✓ Connection Ethernet
✓ Certificate Installed
✓ Authorization Administrator

Step 2 Select **Click to Acknowledge**.

Change Configuration

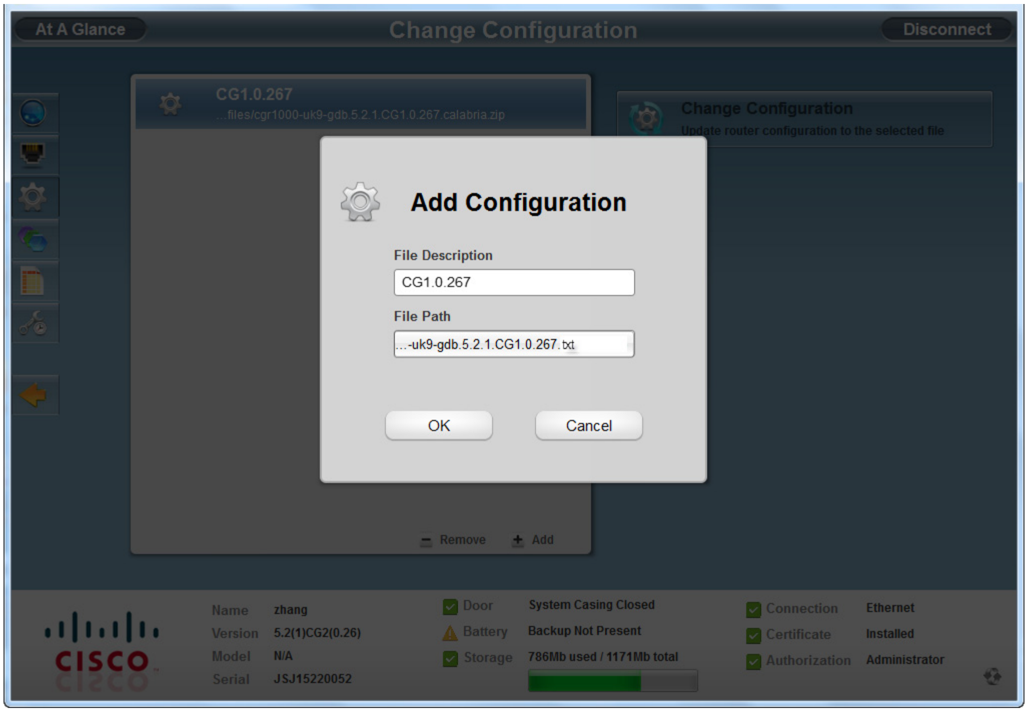
This feature is used to change configuration of a FAR or CGR. Although configuration can be done directly through the CLI of the router, use this feature to change or update the router configuration with a configuration file. Before you can change the router configuration, you must add a configuration file to the Device Manager.

Add a Configuration File

To add a configuration file:

Step 1 Click **Change Configuration** .

Step 2 Click **Add**.



Add Configuration

File Description: CG1.0.267

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

CG1.0.267
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.calabria.zip

Change Configuration
Update router configuration to the selected file

Name zhang
Version 5.2(1)CG2(0.26)
Model N/A
Serial JSJ15220052

Door System Casing Closed
Battery Backup Not Present
Storage 786Mb used / 1171Mb total

Connection Ethernet
Certificate Installed
Authorization Administrator

Step 3 Enter a file description.

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

Step 5 Click **OK**.

Change Configuration

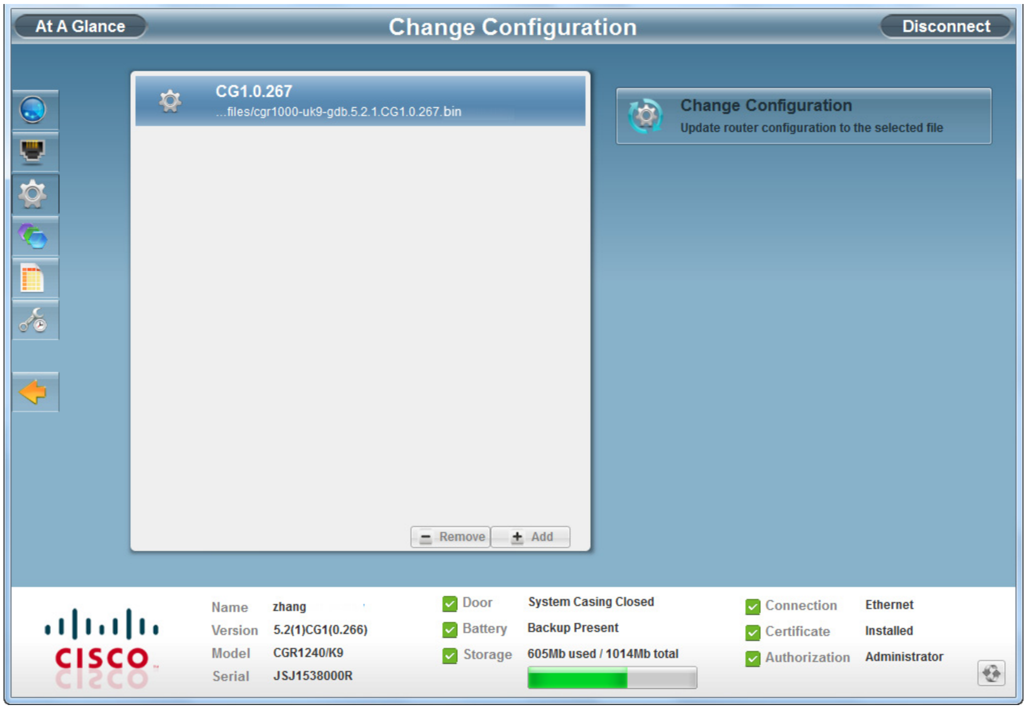
This feature is used to update a complete router configuration. Information in this configuration file must include version, username and password, Ethernet and WiFi interfaces, CGDM, and IP https configuration.

Caution Changing the router configuration will update the configuration file to the FAR and reboot the router. 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.

To change a router configuration file:

Step 1 Select the configuration file from the list.



CG1.0.267
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.bin

Change Configuration
Update router configuration to the selected file

Name	zhang	☑ Door	System Casing Closed	☑ Connection	Ethernet
Version	5.2(1)CG1(0.266)	☑ Battery	Backup Present	☑ Certificate	Installed
Model	CGR1240/K9	☑ Storage	605Mb used / 1014Mb total	☑ Authorization	Administrator
Serial	JSJ1538000R				

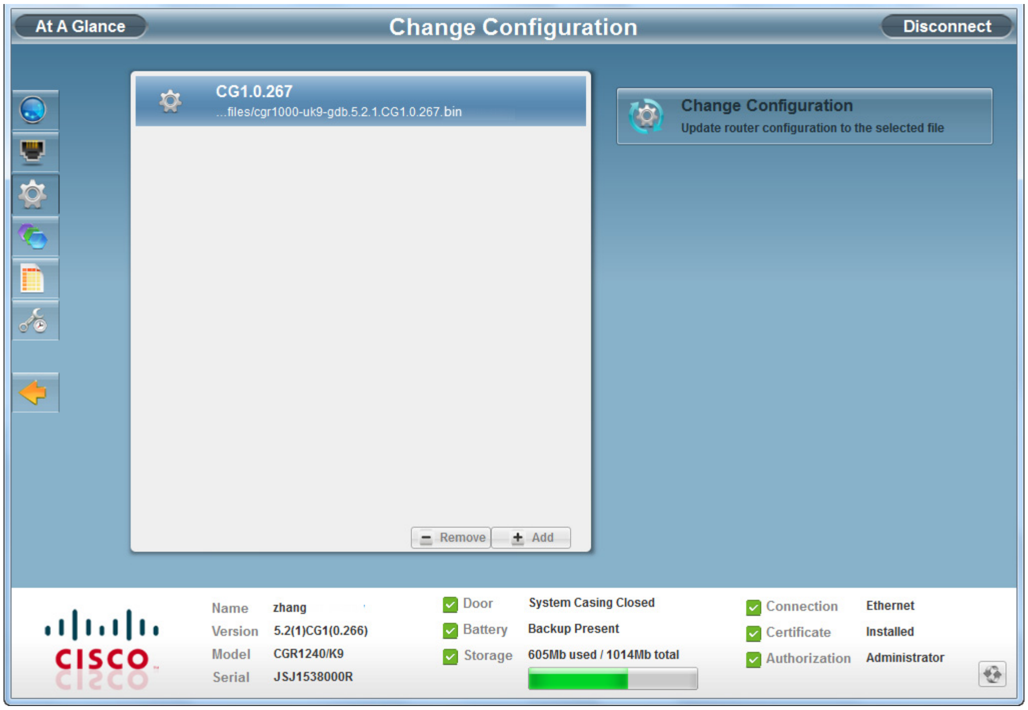
Step 2 Click **Change Configuration**.

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

Remove Configuration

To remove a configuration file:

Step 1 Select the configuration file from the list.



CG1.0.267
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.bin

Name zhang
Version 5.2(1)CG1(0.266)
Model CGR1240/K9
Serial JSJ1538000R

☑ Door System Casing Closed
☑ Battery Backup Present
☑ Storage 605Mb used / 1014Mb total

☑ Connection Ethernet
☑ Certificate Installed
☑ Authorization Administrator

Step 2 Click **Remove**.

Update Image

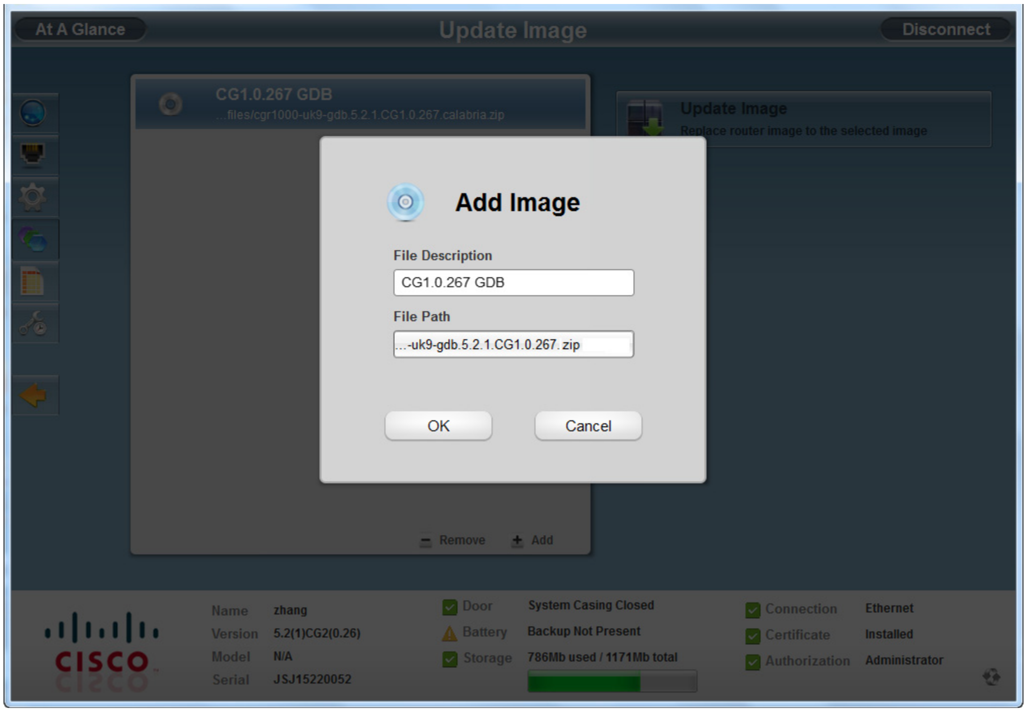
This feature adds an image to the Device Manager. The image can then be used to update the router, and includes information on FPGA, 3G, wireless drivers, and so on.

Add an Image

To add an image:

Step 1 Click **Update Image** .

Step 2 Click **Add**.


At A Glance
Update Image
Disconnect
CG1.0.267 GDB
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.calabria.zip
Update Image
Replace router image to the selected image
Add Image
OK
Cancel
Remove
Add
CISCO

File Description: CG1.0.267 GDB

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

Name	zhang	Door	System Casing Closed	Connection	Ethernet
Version	5.2(1)CG2(0.26)	Battery	Backup Not Present	Certificate	Installed
Model	N/A	Storage	786Mb used / 1171Mb total	Authorization	Administrator
Serial	JSJ15220052				

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.

Update Image

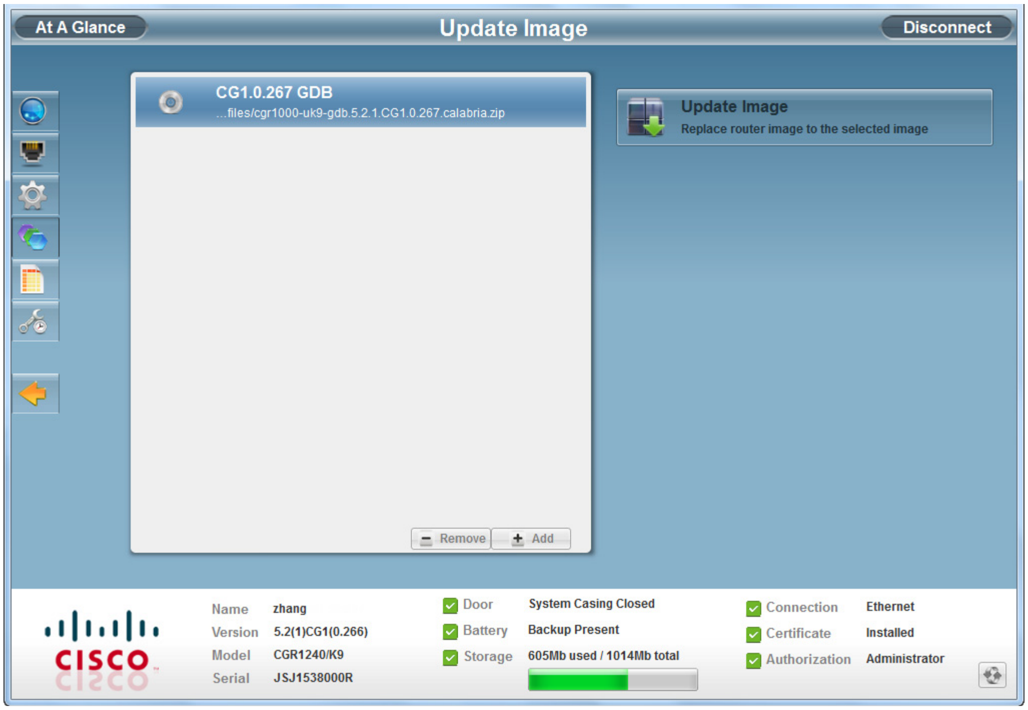
To update an image:

Caution Updating the router will take several minutes 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.

Step 1 Select an image.

Step 2 Click **Update Image**.

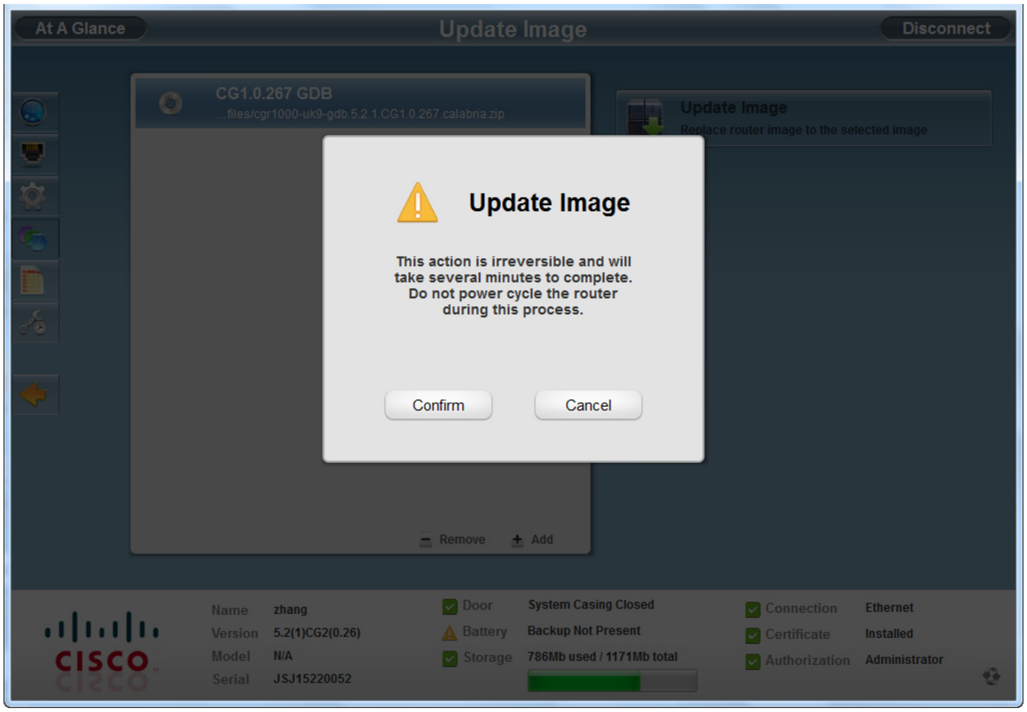


CG1.0.267 GDB
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.calabria.zip

Update Image
Replace router image to the selected image

Name	zhang	✓ Door	System Casing Closed	✓ Connection	Ethernet
Version	5.2(1)CG1(0.266)	✓ Battery	Backup Present	✓ Certificate	Installed
Model	CGR1240/K9	✓ Storage	605Mb used / 1014Mb total	✓ Authorization	Administrator
Serial	JSJ1538000R				

Step 3 Click **Confirm**.



CG1.0.267 GDB
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.calabria.zip

Update Image
Replace router image to the selected image

Update Image

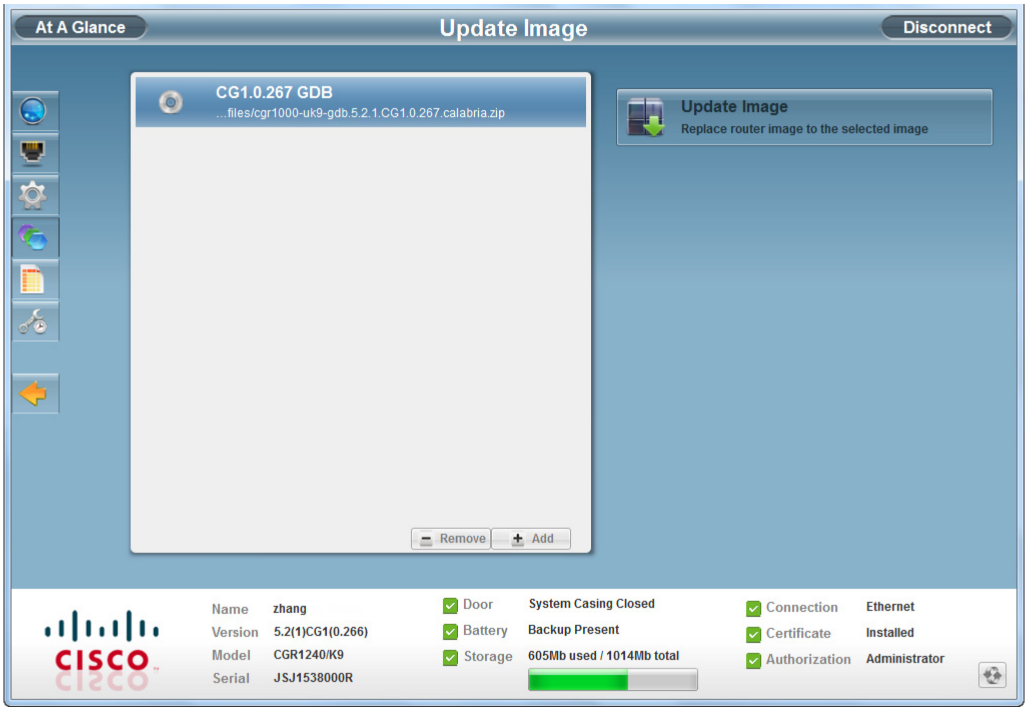
This action is irreversible and will take several minutes to complete. Do not power cycle the router during this process.

Name	zhang	✓ Door	System Casing Closed	✓ Connection	Ethernet
Version	5.2(1)CG2(0.26)	⚠ Battery	Backup Not Present	✓ Certificate	Installed
Model	N/A	✓ Storage	786Mb used / 1171Mb total	✓ Authorization	Administrator
Serial	JSJ15220052				

Remove Image

To remove an image:

Step 1 Select an image.



CG1.0.267 GDB
...files/cgr1000-uk9-gdb.5.2.1.CG1.0.267.calabria.zip

Update Image
Replace router image to the selected image

Name zhang
Version 5.2(1)CG1(0.266)
Model CGR1240/K9
Serial JSJ1538000R

☑ Door System Casing Closed
☑ Battery Backup Present
☑ Storage 605Mb used / 1014Mb total

☑ Connection Ethernet
☑ Certificate Installed
☑ Authorization Administrator

Step 2 Click **Remove**.

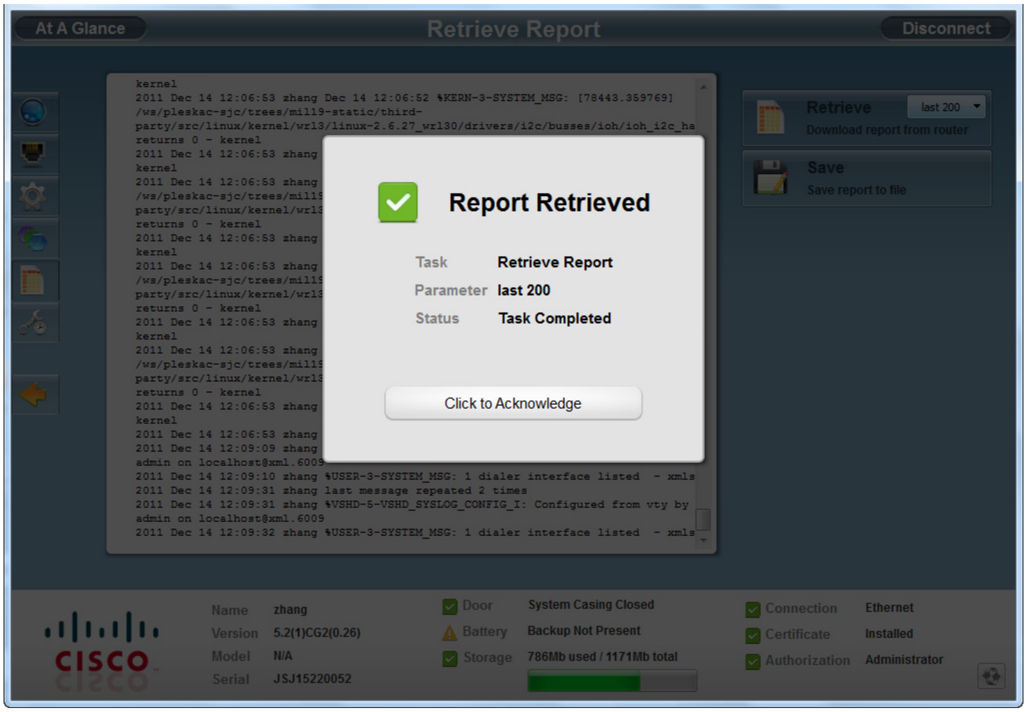
Retrieve Report

To retrieve the router real-time reports:

Step 1 Click **Retrieve Report** 📋.

Step 2 Select the number of lines in the log from the drop-down on the Retrieve Report button.

Step 3 Click **Retrieve** to display the real-time reports.



```
kernel
2011 Dec 14 12:06:53 zhang Dec 14 12:06:52 %KERN-3-SYSTEM_MSG: [78443.359769]
/ws/pleskac-sjc/trees/mil19-static/third-
party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/drivers/i2c/busses/ioh/ioh_i2c_ha
returns 0 - kernel
2011 Dec 14 12:06:53 zhang
kernel
2011 Dec 14 12:06:53 zhang
/ws/pleskac-sjc/trees/mil19
party/src/linux/kernel/wrl3
returns 0 - kernel
2011 Dec 14 12:06:53 zhang
kernel
2011 Dec 14 12:06:53 zhang
/ws/pleskac-sjc/trees/mil19
party/src/linux/kernel/wrl3
returns 0 - kernel
2011 Dec 14 12:06:53 zhang
kernel
2011 Dec 14 12:06:53 zhang
/ws/pleskac-sjc/trees/mil19
party/src/linux/kernel/wrl3
returns 0 - kernel
2011 Dec 14 12:06:53 zhang
kernel
2011 Dec 14 12:06:53 zhang
2011 Dec 14 12:09:09 zhang
admin on localhost@xml.6009
2011 Dec 14 12:09:10 zhang %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmls
2011 Dec 14 12:09:31 zhang last message repeated 2 times
2011 Dec 14 12:09:31 zhang %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on localhost@xml.6009
2011 Dec 14 12:09:32 zhang %USER-3-SYSTEM_MSG: 1 dialer interface listed  - xmls
```

Report Retrieved

Task	Retrieve Report
Parameter	last 200
Status	Task Completed

Retrieve last 200
Download report from router

Save
Save report to file

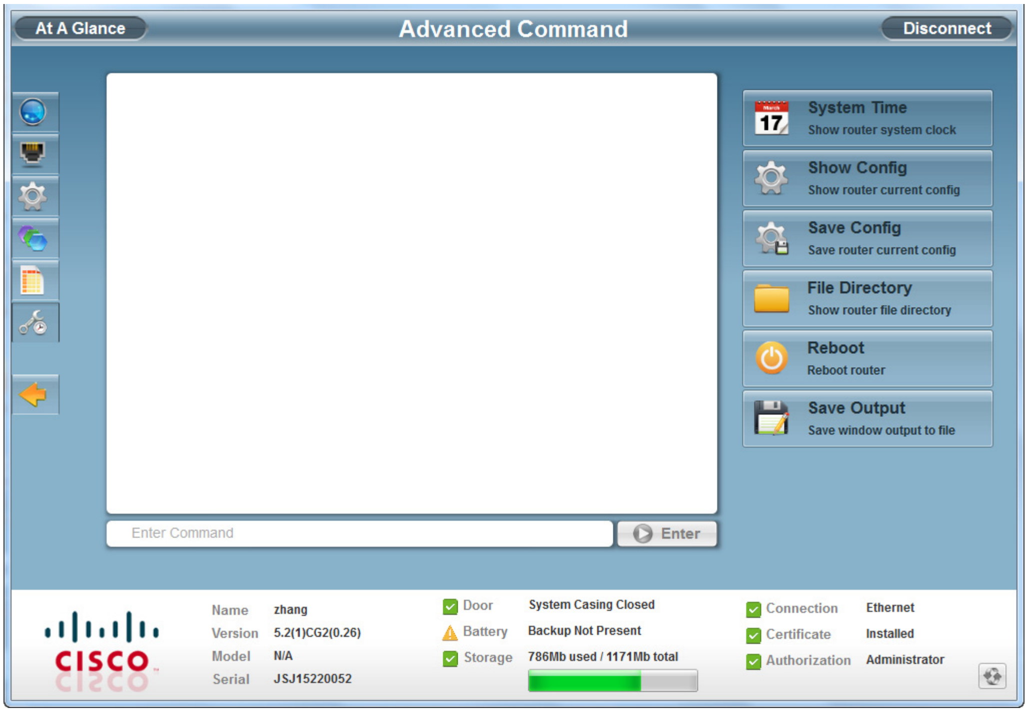
Name	zhang	☑ Door	System Casing Closed	☑ Connection	Ethernet
Version	5.2(1)CG2(0.26)	⚠ Battery	Backup Not Present	☑ Certificate	Installed
Model	N/A	☑ Storage	786Mb used / 1171Mb total	☑ Authorization	Administrator
Serial	JSJ15220052				

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

Step 5 Click **Save** to save the selected report to a systemlog.txt file (see SYSTEM LOG, page 3-24).

Advanced Command

This feature is used to access the CLI of the FAR, and use commands to fine-tune or troubleshoot the router.



Name zhang
Version 5.2(1)CG2(0.26)
Model N/A
Serial JSJ15220052

✓ Door System Casing Closed
⚠ Battery Backup Not Present
✓ Storage 786Mb used / 1171Mb total

✓ Connection Ethernet
✓ Certificate Installed
✓ Authorization Administrator

Note All interactive commands are not supported over this console. For example, configuration can be executed using: `conf t ; int wifi2/1 ; shut ; end`

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

See the *Cisco NXOS CLI Reference Guide* for a complete list of available commands.

Examples

The following contains sample command examples.

SHOW CLOCK

```
router# show clock
12:14:28.702 PST Wed Dec 14 2011
```

COPY RUNNING STARTUP

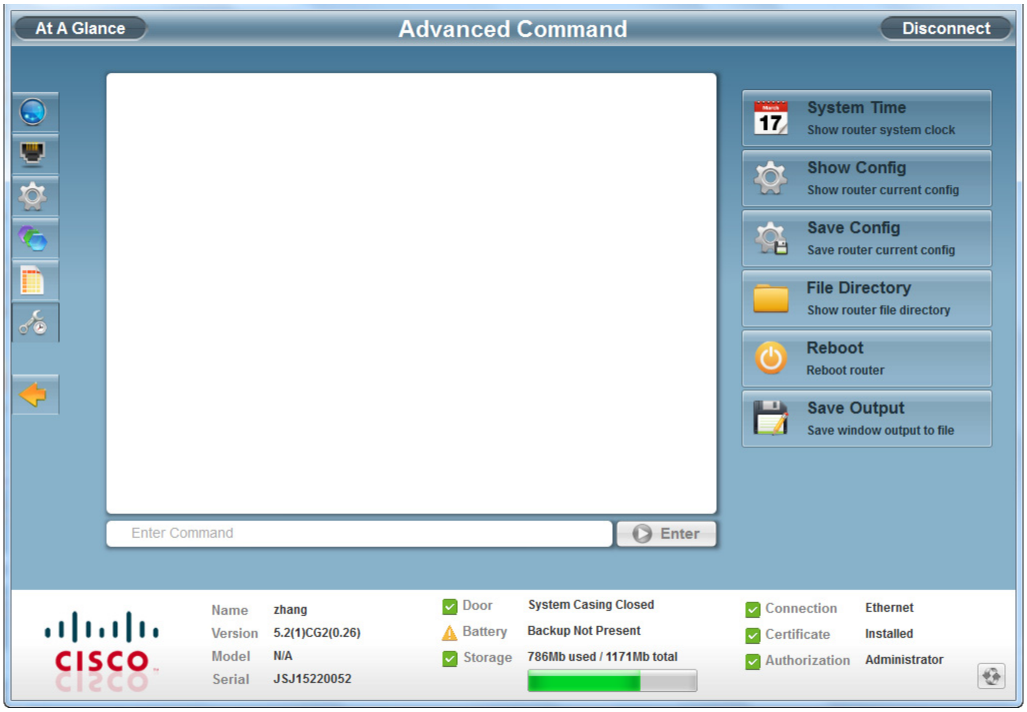
```
router# show running

!Command: show running-config
!Time: Wed Dec 14 12:14:39 2011

version 5.2(1)
snmp-server system-shutdown

logging level feature-mgr 0
hostname zhang
vdc zhang 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

username adminbackup password 5 !  role network-operator
username admin password 5 $1$H0rqzKsl$WF2saMKCRzUdOMjrUzGiC/  role network-admin
ip domain-lookup
crypto key param rsa label CISCO modulus 2048
crypto ca trustpoint CISCO
     enrollment profile CISCO
     rsakeypair CISCO  2048
     revocation-check  none
     serial-number
     fingerprint AE:5C:DE:F2:A6:33:DE:F4:1D:5A:51:04:7D:6A:8B:D7:E0:8B:57:6C
crypto ca profile enrollment CISCO
     enrollment url http://172.27.168.17:80/certsrv/mscep/mscep.dll
snmp-server user admin network-admin auth md5 0xa83c3c6162634360c38f97848fad6556 priv
0xa83c3c6162634360c38f97848fad6556 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

vrf context management
vlan 1
wifi ssid testip6
  authentication key-management wpa2
  wpa2-psk ascii encrypted 7 bwnzfzcffj


interface Dialer1
  shutdown

interface Ethernet2/1
  ip address 128.107.155.243/23
  ipv6 address use-link-local-only
  no shutdown

interface Ethernet2/2
  no shutdown

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6
  no shutdown

interface Ethernet2/7

interface Ethernet2/8
  no shutdown

interface Wifi2/1
  no shutdown
  ssid testip6
  ipv6 address use-link-local-only
clock timezone PST -8 0
clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60
line console
line vty
  session-limit 16
boot kickstart bootflash:/cgr1000-uk9-kickstart.5.2.1.CG2.0.26.SSA.gbin
boot system bootflash:/cgr1000-uk9.5.2.1.CG2.0.26.SSA.gbin
ip route 0.0.0.0/0 128.107.154.1

cgdm
  registration start trustpoint CISCO
ip http secure-server
ip http secure-port 8443
ip http secure-server trustpoint CISCO
```

SYSTEM LOG

```
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.959333]
/ws/pleskac-sjc/trees/mil19-static/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/dr
ivers/i2c/busses/ioh/ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.959350]  - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960121]
/ws/pleskac-sjc/trees/mil19-static/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/dr
ivers/i2c/busses/ioh/ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960138]  - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960453]
/ws/pleskac-sjc/trees/mil19-static/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/dr
ivers/i2c/busses/ioh/ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960471]  - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960780]
/ws/pleskac-sjc/trees/mil19-static/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/dr
ivers/i2c/busses/ioh/ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.960798]  - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.961230]
/ws/pleskac-sjc/trees/mil19-static/third-party/src/linux/kernel/wrl3/linux-2.6.27_wrl30/dr
ivers/i2c/busses/ioh/ioh_i2c_hal.c:ioh_i2c_wait_for_xfer_complete returns 0 - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.961248]  - kernel
2011 Dec 14 11:50:15 zhang Dec 14 11:50:15 %KERN-3-SYSTEM_MSG: [77445.961558]
. . .
```

Disconnect from Device Manager

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 Connect to the Device Manager, page 3-2 to connect to Device Manager again.



Name zhang
Version 5.2(1)CG2(0.26)
Model N/A
Serial JSJ15220052

✓ Door System Casing Closed
⚠ Battery Backup Not Present
✓ Storage 786Mb used / 1171Mb total

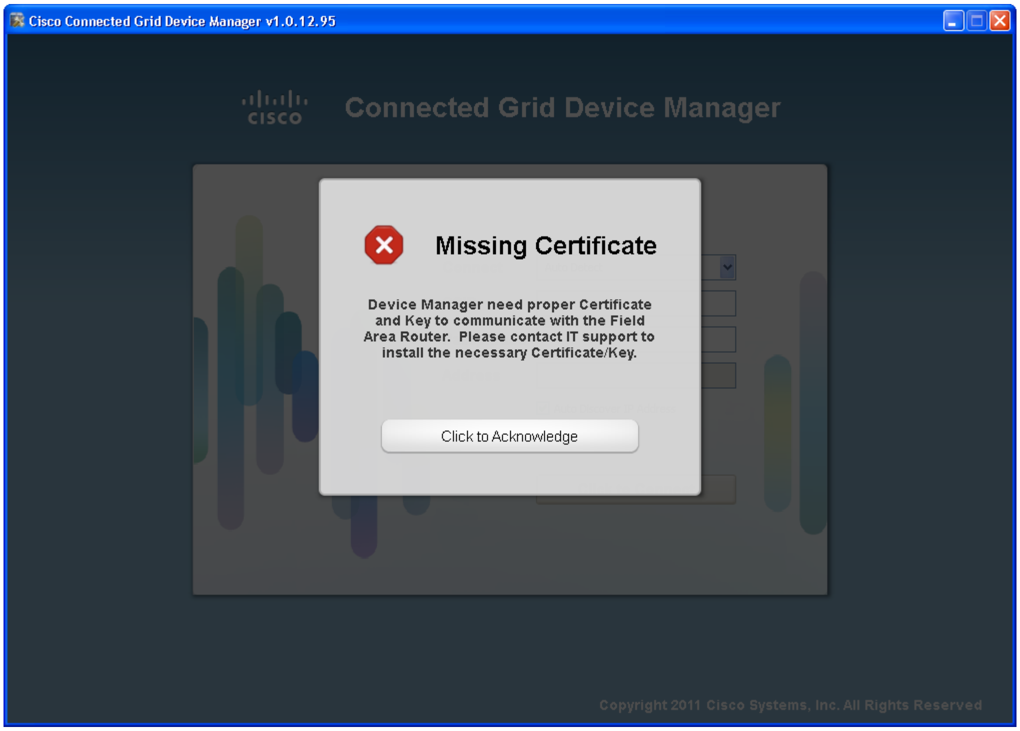
✓ Connection Ethernet
✓ Certificate Installed
✓ Authorization Administrator

Troubleshooting

This section contains information on troubleshooting the Device Manager.

Missing Certificate

The following message displays when you try to log into 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.

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