



CHAPTER 3

Using the Device Manager

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

- [Device Manager Overview, page 3-1](#)
- [How to Use the Device Manager, page 3-2](#)
- [How to Start, page 3-3](#)
- [Connect to the FAR, page 3-3](#)
- [Test Connectivity, page 3-5](#)
- [Manage Interfaces, page 3-10](#)
- [Change Configuration, page 3-12](#)
- [Update Image, page 3-15](#)
- [Retrieve Report, page 3-18](#)
- [Advanced Command, page 3-19](#)
- [Disconnect from the FAR, page 3-25](#)
- [Frequently Asked Questions, page 3-25](#)

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 software 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 (see [Advanced Command](#), page 3-19).



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.



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.



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.



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

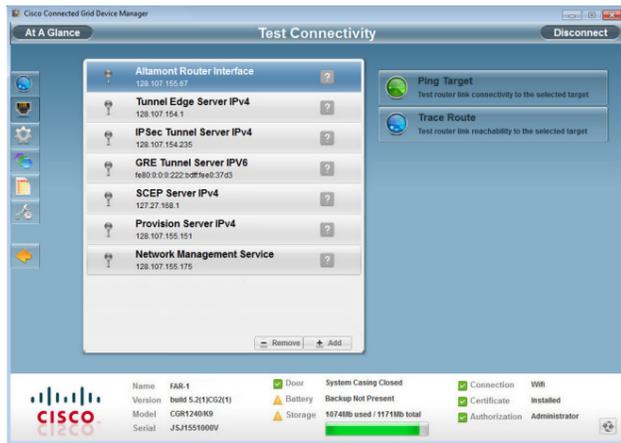
This feature is used to confirm and re-check the connectivity to a device from the FAR. Before you can check the device connection or route to a FAR, you must add a device's IP address to the Device Manager. IP addresses can be either IPv4 or IPv6.

Add a Device IP Address

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

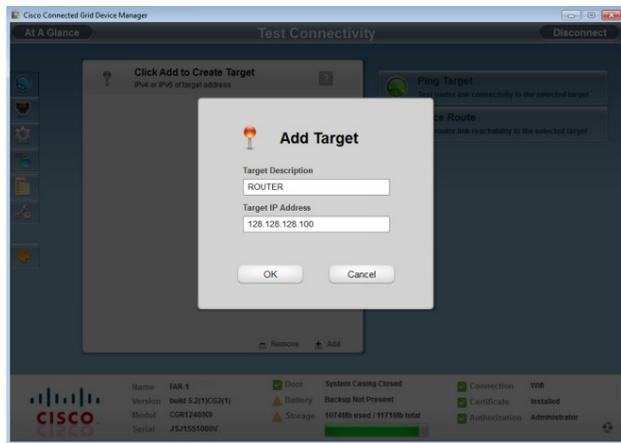
Step 1 Click **Test Connectivity** .

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



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.

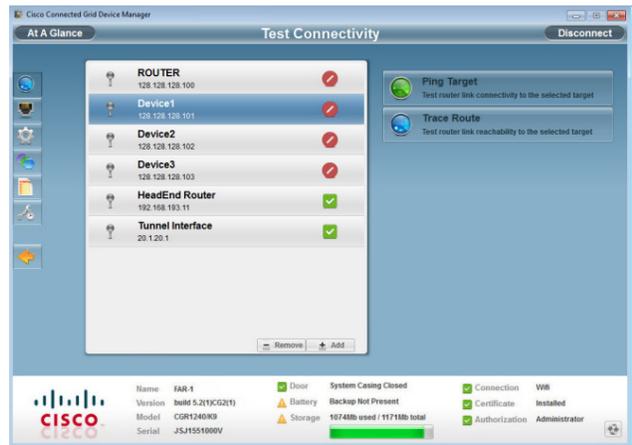


Step 3 Enter a Target Description (or description of the device).

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.



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

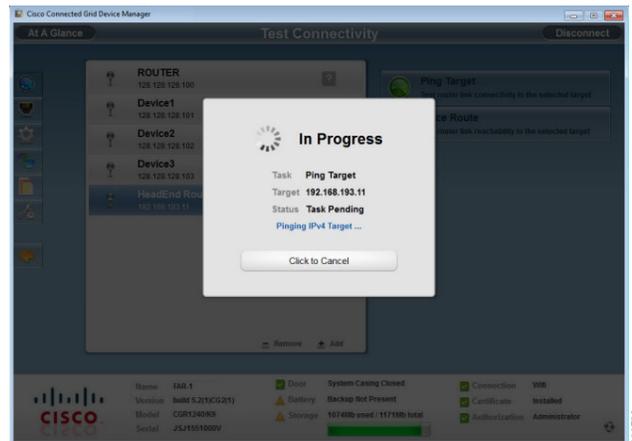
Ping a Device IP Address

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

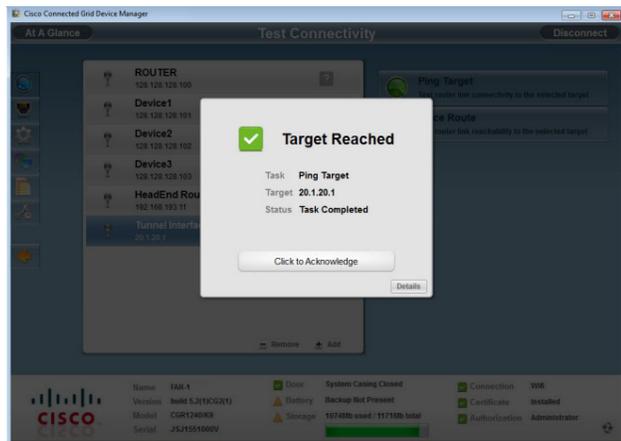
Follow these steps to test connectivity between the FAR and the device:

- Step 1** Select a target IP address from the list.
- Step 2** Click **Ping Target**  to test the connectivity to the selected IP address.

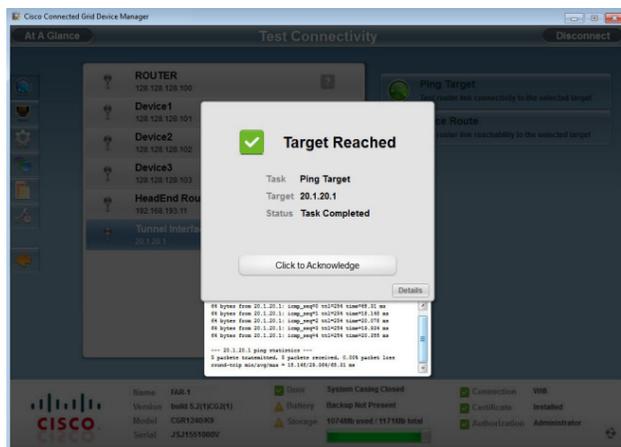
The following example shows the Device Manager is attempting to ping the IPv4 address.



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.



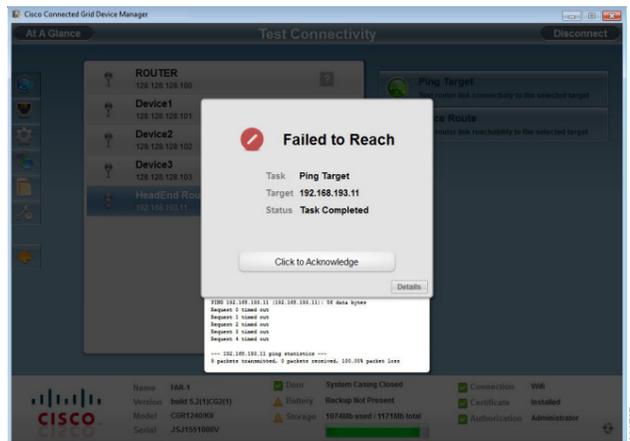
Step 3 Select **Click to Acknowledge** to close the window, or you can also click **Details** to view the ping details (shown below).



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.



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

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

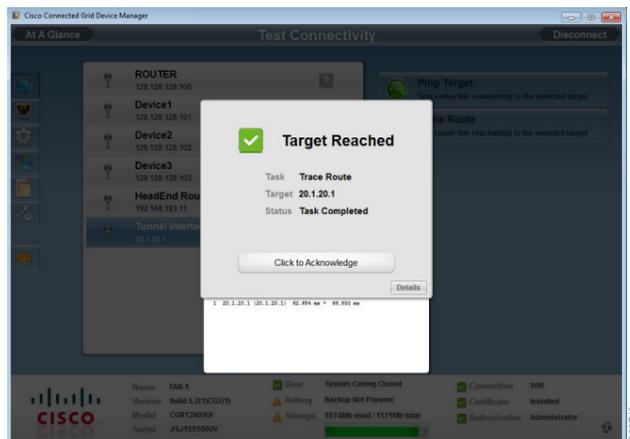
Traceroute a Device IP Address

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.

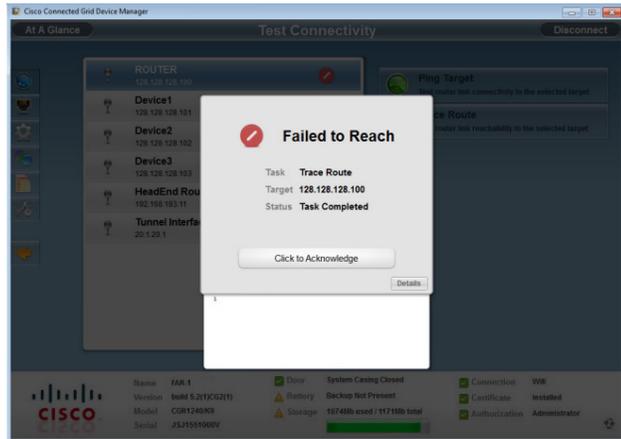
Step 2 Click **Traceroute**  to trace the route.



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**.



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:

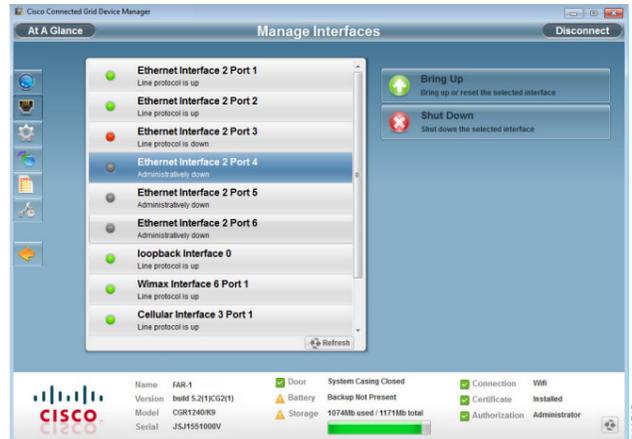
Step 1 Select the target IP address from the list.

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.



Follow these steps to view or manage selected router interfaces:

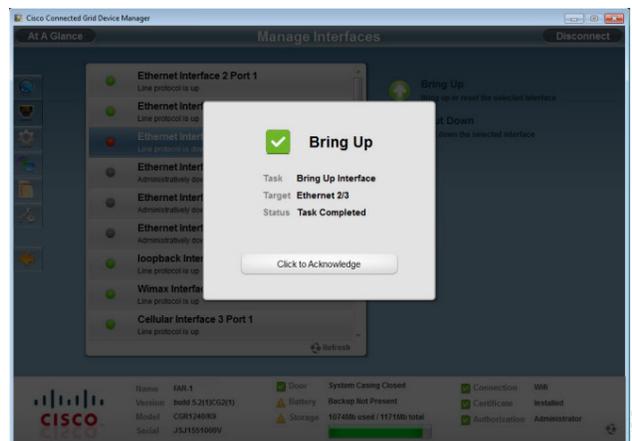
-
- Step 1** Click **Manage Interfaces** .
- Step 2** Select an interface and then go to either [Bring Up an Interface, page 3-11](#) or [Shut Down an Interface, page 3-12](#).
-

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**.



Step 2 Select **Click to Acknowledge**.

Shut Down an Interface

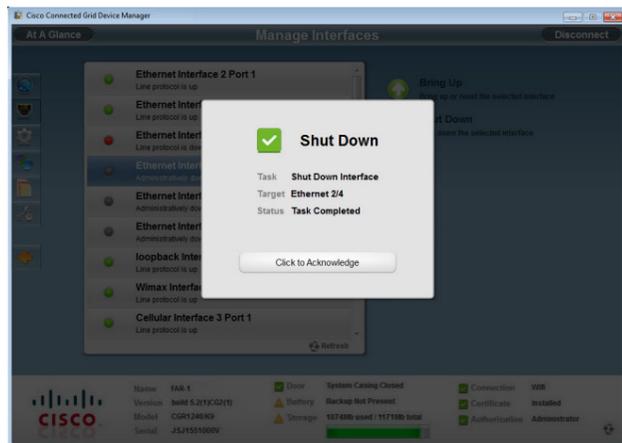


Caution

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**.



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.



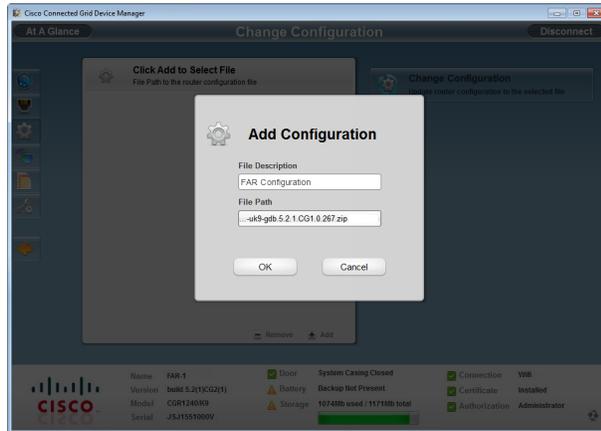
Note

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.

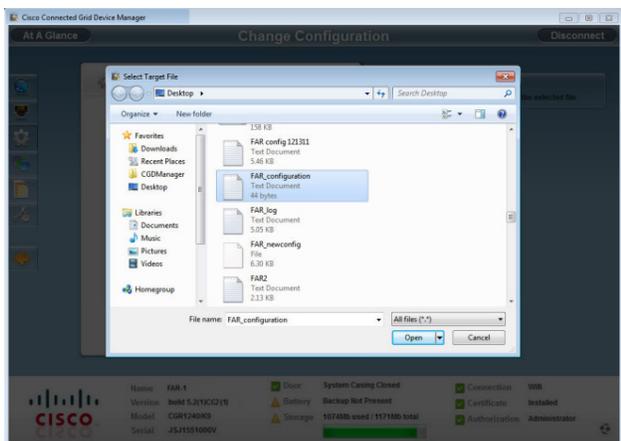
Add a Configuration File

Follow these steps to add a configuration file:

- Step 1** Click **Change Configuration** .
- Step 2** Click **Add**.



- Step 3** Enter a file description.
- Step 4** Click to navigate to where the configuration file is located and select the file.



- 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.



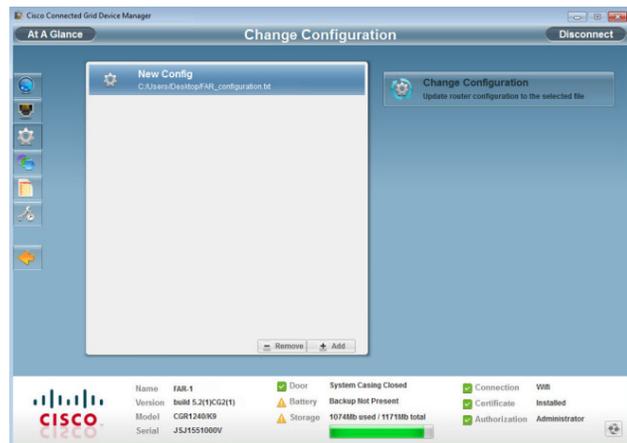
Caution

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.

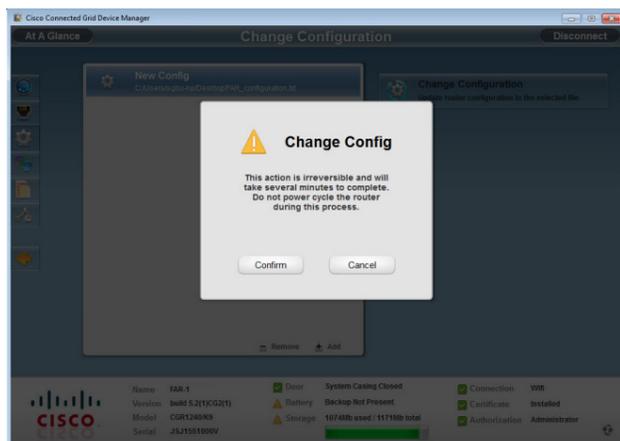
Once this task starts, there is no way to cancel the event. Be careful when using this feature.

Follow these steps to update the FAR configuration file:

- Step 1** Select the configuration file from the list.

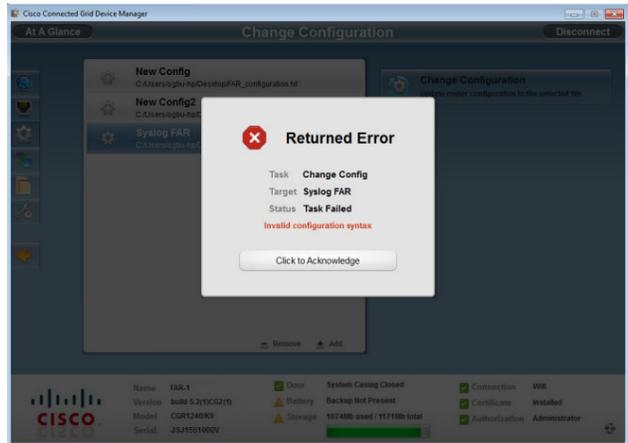


- Step 2** Click **Change Configuration**.



- 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.



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.

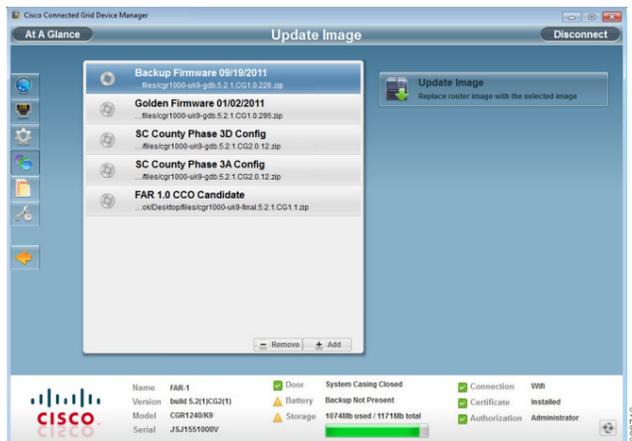
Add an Image

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.



Update Image



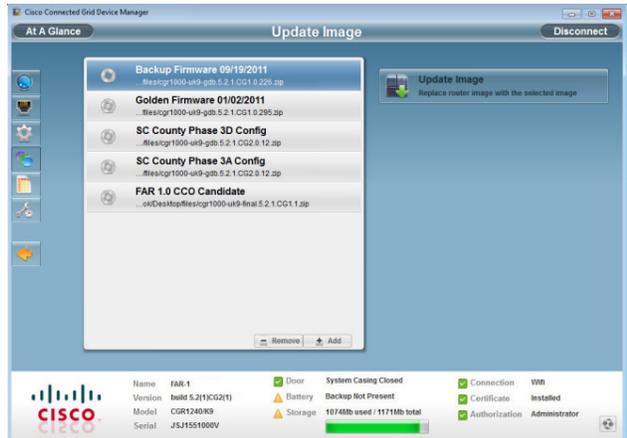
Caution

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

Once this task 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**.



- 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

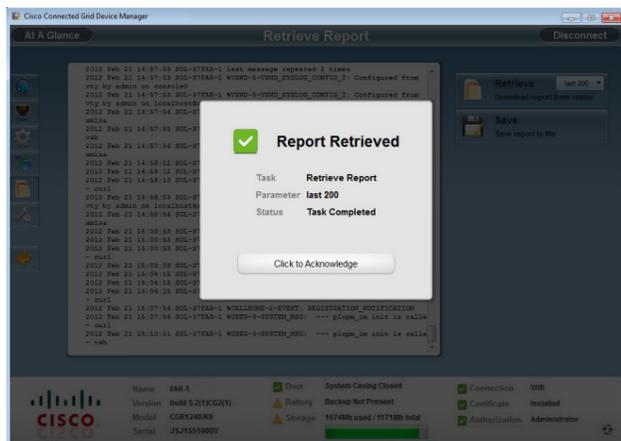
Follow these steps to retrieve the router real-time reports:

Step 1 Click **Retrieve Report** .



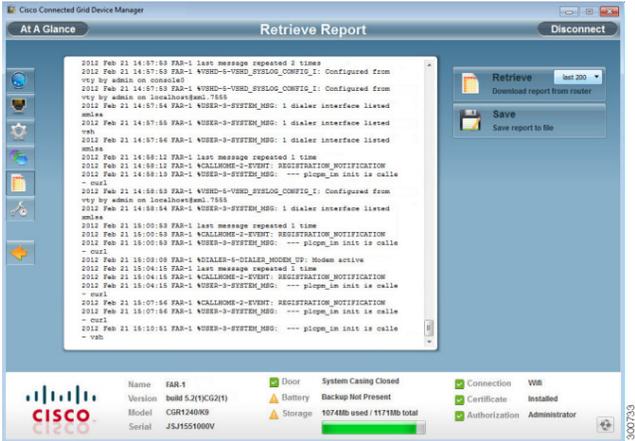
Step 2 Select the number of lines in the log from the drop-down.

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



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

The following example shows 200 lines.



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).

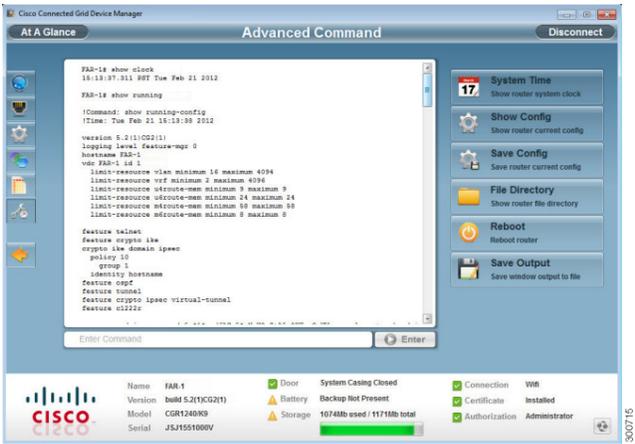
Advanced Command

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.



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$5sNmH2rZtA5o9KFzeQwKVn. 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_gos/third-party/src/linux/kernel/wr13/linux-2.6.27_wr130/drivers/i2c/busses/ih/
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

```

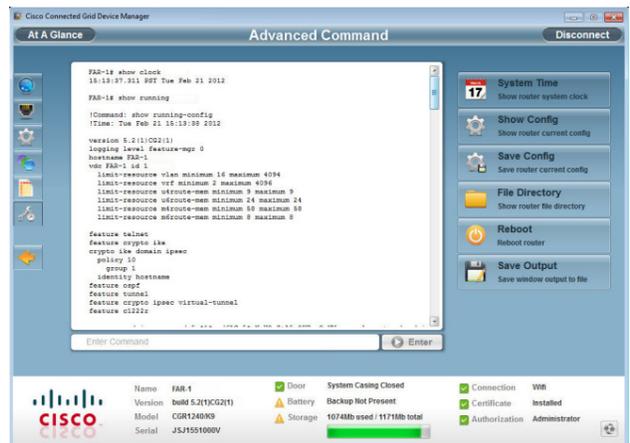
```

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](#).



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”

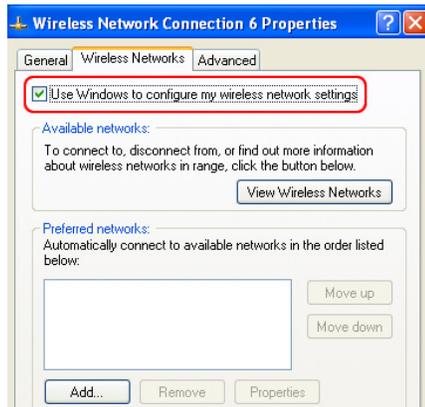
If the Device Manager is connected to the FAR over Ethernet and the IP address is configured, ensure that you can ‘ping’ this IP address from the Device Manager computer. If the IP address is auto-detected, ensure that the Device Manager computer Ethernet is connected to the FAR directly, and that FAR 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:

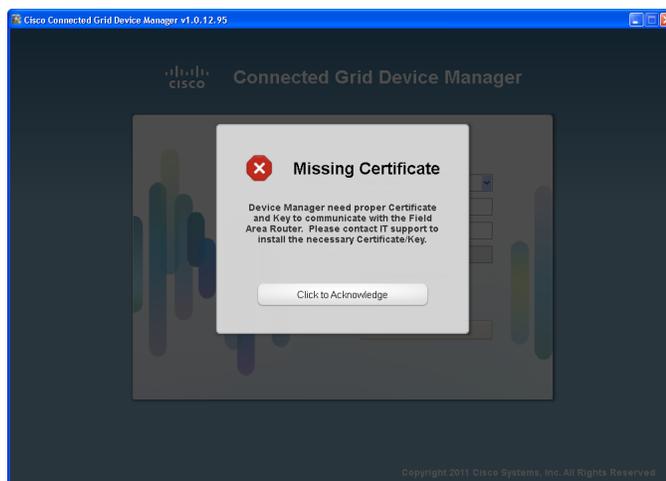
- Step 1** Click **Start > Settings > Control Panel**.
- Step 2** Double-click **Network Connections**.
- Step 3** Right-click **Wireless Network Connection**.



- 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 manage your WiFi interface.

“I cannot log into Device Manager”

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



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.