Cisco Connected Grid Network Management System User Guide, Release 2.1.0-273

Published: February 2015

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

ılıılı CISCO™

Overview of Cisco Connected Grid Network Management System

This chapter provides an overview of the Cisco Connected Grid Network Management System (Cisco CG-NMS) and describes its role within the Cisco Connected Grid Network.

- Overview of Cisco Connected Grid Network

- How to Use This Guide

- Interface Overview

Overview of Cisco Connected Grid Network

This section provides an overview of the following topics:

- Cisco CG-NMS Features and Capabilities

- Architectural Overview

- Mesh Endpoints

- Grid Security

- Related Software: Cisco Connected Grid Device Manager

The Cisco Connected Grid Network Management System (CG-NMS) is a software platform to manage a multi-service network and security infrastructure for smart grid applications, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), distributed intelligence, and substation automation. CG-NMS is a scalable, highly secure, modular, and open-platform with an extensible architecture. CG-NMS is a multi-vendor, multi-service, communications network management platform that enables network connectivity to an open ecosystem of power grid devices.

CG-NMS is built on a layered system architecture to enable clear separation between network management functionality and applications, such as a distribution management system (DMS), outage management system (OMS), and meter data management (MDM). This clear separation between network management and applications helps utilities roll out Smart Grid projects incrementally, for example with AMI, and extend into distribution automation using a shared, multi-service network infrastructure and a common, network management system across various utility operations.

Features

- Geographic Information System (GIS) map-based, visualization, monitoring, troubleshooting, and alarm notifications

- Group-based configuration management for field-area routers (FARs) and smart meter endpoints

- OS compatible (Guest OS) and provides application management

- Rule-engine infrastructure for customizable threshold-based alarm processing and event generation

- North-bound integration API for transparent integration with utility head-end and operational systems

- High availability and disaster recovery

Cisco CG-NMS provides powerful Geographic Information System (GIS) visualization and monitoring capability. Through the browser-based interface, utility operators manage and monitor devices in a Cisco Connected Grid Field Area Network (FAN) solution, using IPv6 over a Low-power Wireless Personal Area Networks (6LoWPANs). The FAN includes the following devices:

- Cisco 1000 Series Connected Grid Routers (CGRs), also called pole-top or din-rail-mount routers. These devices are referred to as FARs in this document; and identified by model (for example, CGR1000, CGR1120, or CGR1240) on the Field Devices page.

- Cisco 800 Series Integrated Services Routers (ISR 800s) are used in most networks as edge routers or gateways to provide WAN connectivity (cellular, satellite over Ethernet, and WiFi) to an end device (energy-distribution automation devices, and other verticals such as ATMs, connectivity for mobile deployments such as in taxis or trucks). These devices are referred to as FARs in this document; and identified by product ID (for example, C800 or C819) on the Field Devices page. You can use CG-NMS to manage the following hardened Cisco 819H ISRs:

  - C819HG-4G-V-K9

  - C819HG-4G-A-K9

  - C819HG-U-K9

  - C819HGW-S-A-K9

  - C819H-K9

- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR 500) supply RF mesh connectivity to IPv4 and serial Internet of Things (IoT) devices (for example, recloser control, cap bank control, voltage regulator controls, and other remote terminal units).

Note: CGRs, C800s, IR 500s and other types of mesh endpoint devices can coexist on a network, but cannot be in the same device group (see Creating Device Groups and Working with Mesh Endpoint Firmware Images) or firmware management group (see Configuring Firmware Group Settings).

- Cisco ASR 1000 Series Aggregation Services Routers (ASRs) and Cisco ISR 3900 Series Integrated Service Routers (ISRs), referred to as *head-end routers* or HERs in this document.

- Cisco IPv6 RF (radio frequency), PLC (power line communications), and Dual PHY (RF and PLC) mesh endpoints (smart meters and range extenders).

Note: In this document, *mesh endpoints* (MEs) refers to Cisco range extenders and Cisco-compatible smart meters.

CG-NMS typically resides in the utility control center with other utility head-end operational systems, such as an AMI head end, distribution management system, or outage management system. CG-NMS features enterprise-class fault, configuration, accounting, performance, and security (FCAPS) functionality, as defined in the Open Systems Interconnection (OSI) model.

The Cisco CG-NMS North Bound Application Programmable Interface (NB API), allows various utility applications like DMS, OMS, or MDM to pull appropriate, service-specific data for distribution grid information, outage information, and metering data from a shared, multi-server communication network infrastructure. For more information about the Cisco CG-NMS North Bound API, see the *Cisco Connected Grid NMS North Bound API Programming Guide*.

Cisco CG-NMS Features and Capabilities

- **Configuration Management** – Cisco CG-NMS facilitates configuration of large numbers of Cisco CGRs, Cisco ASRs, and MEs. Use Cisco CG-NMS to bulk-configure devices by placing them into configuration groups, editing settings in a configuration template, and then pushing the configuration to all devices in the group.

- **Device and Event Monitoring** – Cisco CG-NMS displays easy-to-read tabular views of extensive information generated by devices, allowing you to monitor your network for errors. Cisco CG-NMS provides integrated Geographic Information System (GIS) map-based visualization of FAN devices such as routers and smart meters. Use CG-NMS to create CGR-specific work orders that include the required certificates to access the router.

- **Firmware Management** – Cisco CG-NMS serves as a repository for Cisco CGR and ME firmware images. Use Cisco CG-NMS to upgrade the firmware running on groups of devices by loading the firmware image file onto the Cisco CG-NMS server, and then uploading the image to the devices in the group. Once uploaded, use CG-NMS to install the firmware image directly on the devices.

- **Zero Touch Deployment** – This ease-of-use feature automatically registers (enrolls) and distributes X.509 certificates and provisioning information over secure connections within a connected grid network.

- **ODM File Upload and Hash Compatibility** – Operational Data Model (ODM) files format commands that execute on Cisco IOS routers. CG-NMS uses the formatted output for periodic metrics collection, router version information, battery information, reading the Hypervisor (virtual machine monitor) version, GPS information, and so on. ODM file hash compatibility and upload are performed while requesting a registration, during periodic inventory updates, or during the tunnel provisioning process.

- **Tunnel Provisioning Between Cisco ASRs and Cisco CGRs** – Protects data exchanged between Cisco ASRs and Cisco CGRs and prevents unauthorized access to Cisco CGRs, to provide secure communication between devices. Cisco CG-NMS can execute CLI commands to provision secure tunnels between Cisco CGRs and Cisco ASRs. Use CG-NMS to bulk-configure tunnel provisioning using groups.

- **IPv6 RPL Tree Polling** – The IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) finds its neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the ME to the CGR that is the root of the routing tree. RPL tree polling is available through the mesh nodes and CGR periodic updates. The RPL tree represents the mesh topology, which is useful for troubleshooting. For example, the hop count information received from the RPL tree can determine the use of unicast or multicast for the firmware download process. CG-NMS maintains a periodically updated snapshot of the RPL tree.

- **Dynamic Multipoint VPN** – For C800 devices, DMVPN does not require CG-NMS to apply device-specific tunnel configuration to the HER during tunnel provisioning.

- **Dual PHY Support** – CG-NMS can communicate with devices that support Dual PHY (RF and PLC) traffic. CG-NMS identifies CGRs running Dual PHY, enables configuration to masters and slaves, and collects metrics from masters. CG-NMS also manages security keys for Dual PHY CGRs. On the mesh side, CG-NMS identifies Dual PHY nodes using unique hardware IDs, enables configuration pushes and firmware updates, and collects metrics, including RF and PLC traffic ratios.

- **OS Migration** – For Cisco CGR 1000 devices running CG-OS, CG-NMS allows you to migrate from CG-OS to IOS.

- **Guest OS (GOS) Support** – For Cisco IOS CGR 1000 devices that support Guest OS, CG-NMS allows approved users to manage applications running on the supported operating systems. CG-NMS supports all phases of application deployment, and displays application status and the Hypervisor version running on the device.

- **Device Location Tracking** – For CGR 1000 and C800 devices, CG-NMS displays real-time location and device location history.

- **Software Security Module (SSM)** – This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices.

- **Diagnostics and Troubleshooting** – The CG-NMS rule engine infrastructure provides effective monitoring of triage-based troubleshooting. Device troubleshooting runs on-demand device path trace and ping on any CGR, range extender, or meter (mesh endpoints).

- **High Availability** – To ensure uninterrupted network management and monitoring, you can deploy the Cisco CG-NMS solution in a High Availability (HA) configuration. By using clusters of load-balanced CG-NMS servers and primary and standby CG-NMS databases, Cisco CG-NMS constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your CG-NMS solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.

- **Power Outage Notifications** – CGEs implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, CGEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. FARs relay the power outage notification to CG-NMS, which then issues push notifications to customers to relate information on the outage.

- **Mesh Upgrade Support** – Over-the-air software and firmware upgrades to field devices such as Cisco CGRs and CGEs (for example, AMI meter endpoints).

- **Audit Logging** – Logs access information for user activity for audit, regulatory compliance, and Security Event and Incident Management (SEIM) integration. This simplifies management and enhances compliance by integrated monitoring, reporting, and troubleshooting capabilities.

- **North Bound APIs** – Eases integration of existing utility applications such as outage management system (OMS), meter data management (MDM), trouble-ticketing systems, and manager-of-managers.

- **Work Orders for Device Manager** – Credentialed field technicians can remotely access and update work orders.

- **Role-Based Access Controls** – Integrates with enterprise security policies and role-based access control for AMI network devices.

- **Event and Issue Management** – Fault event collection, filtering, and correlation for communication network monitoring. CG-NMS supports a variety of fault-event mechanisms for threshold-based rule processing, custom alarm generation, and alarm event processing. Faults display on a color-coded GIS-map view for various endpoints in the utility network. This allows operator-level custom, fault-event generation, processing, and forwarding to various utility applications such as an outage management system. Automatic issue tracking is based on the events collected.

Architectural Overview

Figure 1 provides a high-level view of the systems and communication paths that exist in a typical utility company operating on a Cisco CGR connected grid network in which Zero Touch Deployment is in use.

For Cisco CG-OS CGRs, we recommend a tunnel configuration using FlexVPN. FlexVPN combines all of these features in one GRE tunnel (protected by IPsec).

For Cisco C800s, we recommend using Dynamic Multipoint VPN (DMVPN).

Figure 1   Zero Touch Deployment Architecture
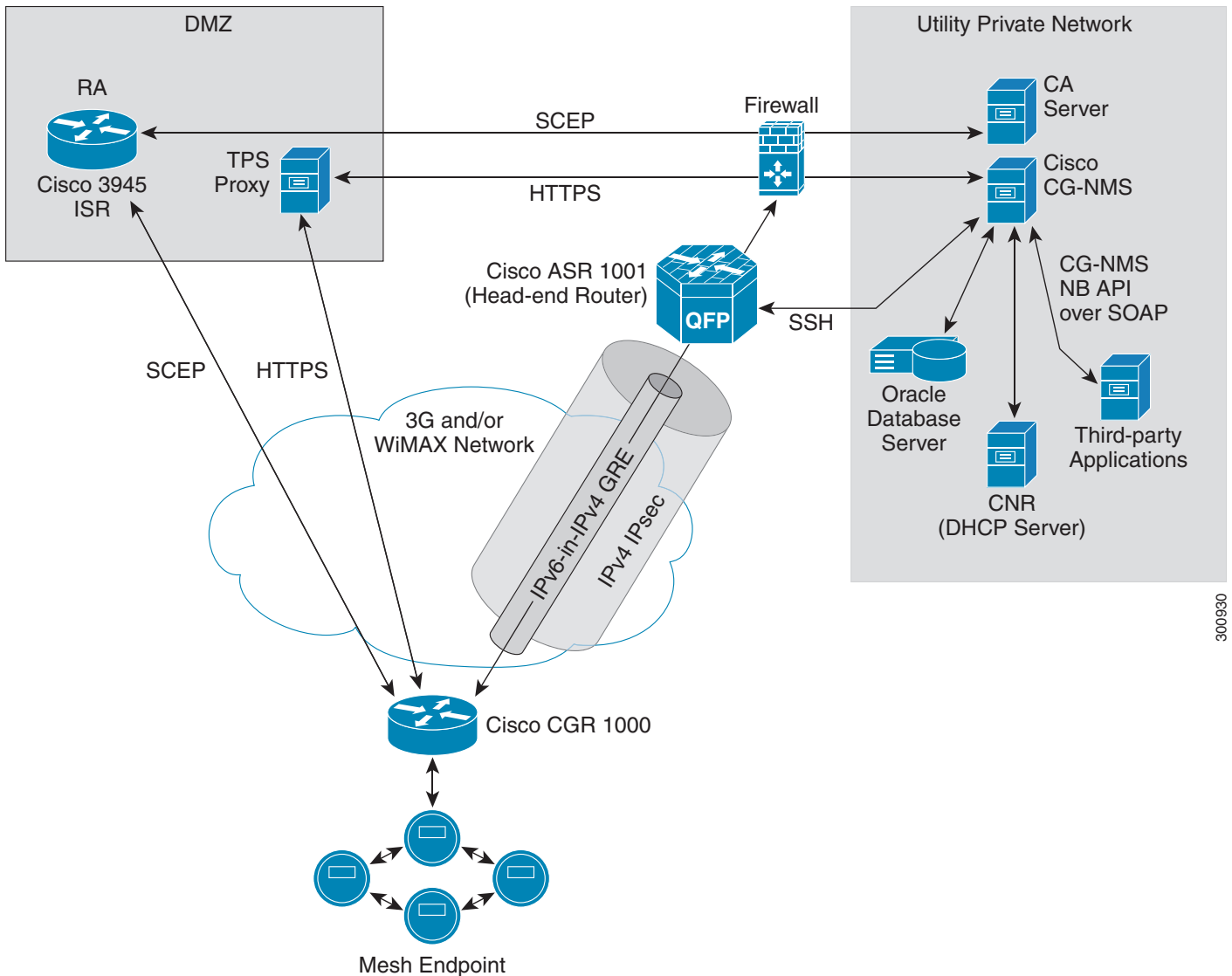
In this example, the firewall provides separation between those items in the utility company public network (DMZ) and its private network.

The utility company private network shows systems that might reside behind the firewall such as the Cisco CG-NMS, the Oracle database server, the Cisco CG-NMS North Bound API, the DHCP server, and the Certificate Authority (CA). The Cisco CG-NMS Tunnel Provisioning Server proxy (TPS proxy) and Registration Authority (RA) might be located in the DMZ.

After installing and powering on the Cisco CGR, it becomes active in the network and registers its certificate with the RA by employing the Simple Certificate Enrollment Protocol (SCEP). The RA (Cisco 3945 ISR), functioning as a CA proxy, obtains certificates for the Cisco CGR from the CA. The Cisco CGR then sends a tunnel provisioning request over HTTPS to the TPS proxy that forwards it to CG-NMS.

Cisco CG-NMS manages collection of all information necessary to configure a tunnel between Cisco CGRs and the head-end router (Cisco ASR 1001). For CG-OS CGR installations, we recommend a network configuration with an outer IPsec tunnel over IPv4 inside which is an IPv6-in-IPv4 GRE tunnel. All traffic from the MEs is over IPv6. The GRE tunnel provides a path for IPv6 traffic to reach the data center. The outer IPsec tunnel secures that traffic. When the tunnel is active, the Cisco CGR (after configuration) connects to the utility company network like a Virtual Private Network (VPN).

## Main Components of a CG-NMS Solution

Component	Description
CG-NMS Application Server	This the heart of CG-NMS deployments. It runs on an RHEL server and allows administrators to control different aspects of the CG-NMS deployment using its browser-based graphical user interface. CG-NMS HA deployments include two or more CG-NMS servers connected to a load balancer.
CG-NMS Database	This Oracle database stores all information managed by your CG-NMS solution, including all metrics received from the MEs and all device properties such as firmware images, configuration templates, logs, event information, and so on.
Software Security Module (SSM)	This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices.
TPS Proxy	Allows FARs to communicate with CG-NMS when they first start up in the field. After CG-NMS provisions tunnels between the FARs and ASRs, the FARs communicate with CG-NMS directly.
Load Balancer	(Optional) CG-NMS uses the Cisco ACE 4710 to provide HA. The load balancer distributes the traffic among the CG-NMS servers in the server cluster in your solution.

High Availability and Tunnel Redundancy

The example in Figure 1 is of a single-server deployment with one database and no tunnel redundancy. However, you could take advantage of Cisco CG-NMS HA support to deploy a cluster of Cisco CG-NMS servers connected to a Cisco ACE 4710 load balancer, as shown in Figure 2. The load balancer sends requests to the servers in a round-robin fashion. If a server fails, the load balancer keeps servicing requests by sending them to the other servers in the cluster.

You could also deploy a standby Cisco CG-NMS database to provide another layer of high availability in the system with minimal data loss.

Figure 2   CG-NMS Server and Database HA

CG-NMS
High Availability

CG-NMS Database
High Availability
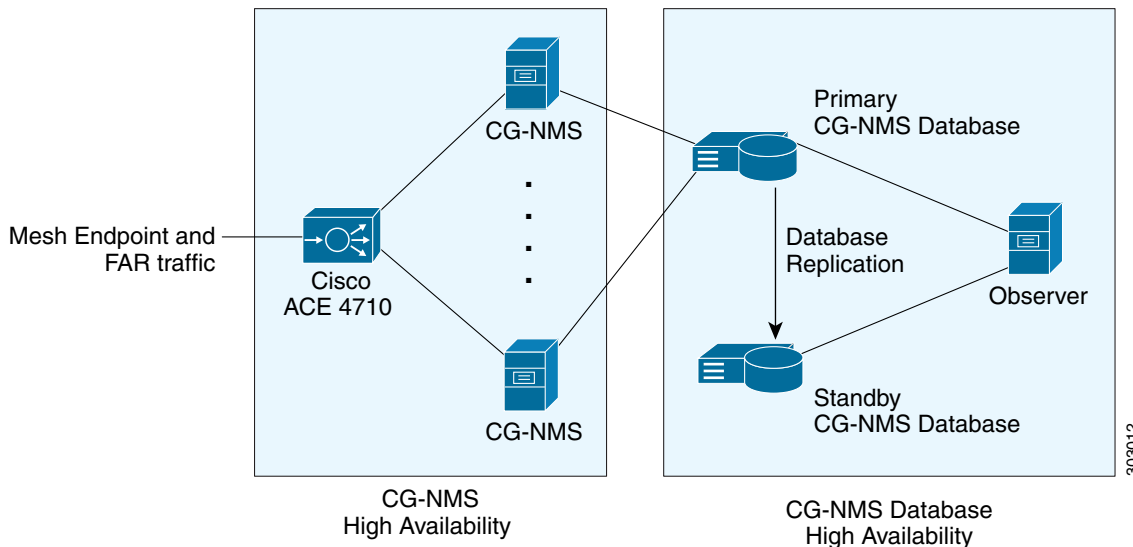
To provide tunnel redundancy, CG-NMS allows you to create multiple tunnels to connect a CGR to multiple ASRs, as shown in Figure 3.

Figure 3   CG-NMS Tunnel Redundancy
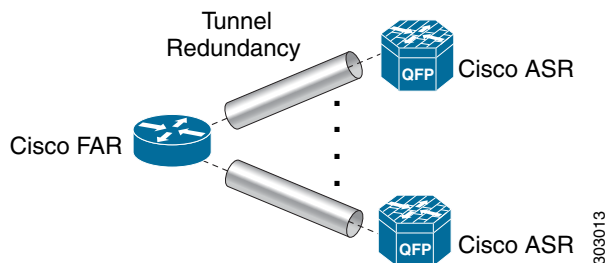
For more information about HA, see Database High Availability.

Mesh Endpoints

The Cisco Field Area Network (FAN) solution brings the first multi-service communications infrastructure to the utility field area network. It delivers applications such as AMI, DA, and Protection and Control over a common network platform.

Advanced meter deployments follow a structured process designed to match the right solution to the needs of the utility company. This process moves in phases that require coordination between metering, IT, operations, and engineering. The first phase for most utilities is identification of goals, followed by analysis of data needs, and business processes. After an evaluation of the business case is complete and a technology chosen, system implementation and validation complete the process.

Once the utility company moves past the business case into system implementation, unforeseen complications can sometimes slow or delay a deployment. The true value of a plug-and-play system is that it saves cost and improves the return on investment by allowing the benefits of advanced metering to be realized sooner.

The features that enable a true plug-and-play RF or PLC mesh network system include:

- **Self initializing endpoints**: CGRs automatically establish the best path for communication through advanced self-discovery – meters and infrastructure deploy without programming.

9

■ **Scalability**: This type of network enables pocketed deployments where each Cisco CG-NMS installation can accept up to 10 million meters/endpoints. Large capacity enables rapid, multi-team deployments to occur in various parts of the targeted AMI coverage area, while saving infrastructure and communication costs.

In a true mesh network, metering and range extender devices communicate to and through one another and decide their own best links, forming the RF Mesh Local Area Network (RFLAN) or PLC LAN. These ME devices become the network and possess dynamic auto-routing functions that eliminate the need for dedicated repeater infrastructure or intermediate (between endpoint and collector) tiered radio relay networks. The result is a substantial reduction in dedicated network infrastructure as well as powerful and more flexible fixed-network communication capability.

Range extenders are installed by the utility company to strengthen mesh coverage and provide redundancy, supplementing network reliability in difficult environmental settings such as dense urban areas where buildings obstruct the normal mesh signal propagation, or in low-meter-density geographically sparse regions and RF-challenged areas. A range extender automatically detects and connects to the mesh after installation or outage recovery, and then provides an alternate mesh path.

In a normal deployment scenario, these MEs form a stable RFLAN or PLC LAN network the same day they are deployed. Once the collector is installed, placing MEs throughout the deployment area is as simple as changing out a meter. MEs form a network and begin reporting automatically.

Mesh endpoints send and receive information. A two-way mesh system allows remote firmware upgrades, as well as system settings changes and commands for time-of-use periods, demand resets, and outage restoration notifications. Not having to physically "touch the meter" is a major value, especially when entering the advanced demand response metering domain that requires time-of-use (TOU) schedule changes and interval data acquisition changes to meet specific client needs. These commands can be sent to groups or to a specific ME. Meter commands can be scheduled, proactive, on-demand, or broadcast to the entire network.

Communication between the data center/network operations center (NOC) and the collector is accomplished by widely available and cost-efficient mass marketed TCP/IP-based public wide area network (WAN) or with the utility company owned WAN. The flexibility and open standard public WAN architectures currently available and in the future create an environment that allows continued ongoing cost reduction and future options, without being tied into one type of connectivity over the life of the asset. It is best if the AMI system avoids using highly specialized WAN systems.

After deployment is complete, the system can transmit scheduled hourly (and sub hourly) data to support utility applications such as billing reads, advanced demand response initiatives, load research, power quality, and transformer asset monitoring.

Easy access and reliable on-demand capability allow the utility to perform grid diagnostics and load research system-wide or for selected groups of meters. Other standard features support outage management, tamper detection, and system performance monitoring.

Grid Security

Designed to meet the requirements of next-generation energy networks, Cisco Grid Security solutions take advantage of our extensive portfolio of cybersecurity and physical security products, technologies, services, and partners to help utility companies reduce operating costs while delivering improved cybersecurity and physical security for critical energy infrastructures.

Cisco Grid Security solutions provide:

■ **Identity management and access control**: Secure utility facilities, assets, and data with user authentication and access control are custom-built for grid operations.

■ **Thread defense**: Build a layered defense that integrates with firewall, VPN, intrusion prevention, and content security services to detect, prevent, and mitigate threats.

■ **Data center security**: Turn network, computing, and storage solutions into a secure, shared pool of resources that protects application and data integrity, secures communications between business processes and applications within the utility, and secures connectivity to external resources such as providers of renewable energy.

- **Utility compliance**: Improve risk management and satisfy compliance and regulatory requirements such as NERC-CIP with assessment, design, and deployment services.

- **Security monitoring and management**: Identify, manage, and counter information security threats and maintain compliance through ongoing monitoring of cyber events.

Related Software: Cisco Connected Grid Device Manager

The Cisco Connected Grid Device Manager (Device Manager or CGDM) is a Windows-based application used by field technicians to remotely manage Cisco CGRs. For some activities, the CGDM retrieves information from CG-NMS.

How to Use This Guide

This section has the following topics to help you quickly find information:

- Common Tasks

- CGR Tasks

- Mesh Endpoint Tasks

- Administration Tasks

- Document Conventions

Common Tasks

Table 1 lists tasks that users perform on both FARs and MEs. The ability to perform tasks is role-based. For information about user roles, see System-Defined User Roles.

Table 1   Common Tasks

Task	Use
Device Viewing Tasks	
View devices	Working with Router Views, Viewing Mesh Endpoints in Default View
View detailed device information	Displaying Detailed Device Information
Device Labeling Tasks	
Add labels	Adding Labels in Bulk
Remove labels	Removing Labels in Bulk
Search and Device Filtering Tasks	
Use filters	Using Filters to Control the Display of Devices
Diagnostics and Troubleshooting Tasks	
Ping	Pinging Devices
Traceroute	Tracing Routes to Devices
Download logs	Downloading Logs
Monitoring Tasks	
View and search events	Monitoring Events
View and search issues	Monitoring Issues, Viewing Device Severity Status on the Issues Status Bar
View tunnel status	Monitoring Tunnel Status

Table 1   Common Tasks (continued)

Task	Use
General Tasks	
Change password	Resetting Passwords
Set time zone	Configuring the Time Zone
Set user preferences	Setting User Preferences

CGR Tasks

Table 2 lists CGR tasks. For information about user roles, see System-Defined User Roles.

Table 2   CGR Tasks

Task	Use
Router Configuration Group Tasks	
Add CGRs to configuration groups	Creating Device Groups
Delete a configuration group	Deleting Device Groups
List devices in a configuration group	Listing Devices in a Configuration Group
Assign devices to groups	Adding FARs to CG-NMS Adding HERs to CG-NMS Moving Devices to Another Configuration Group Manually Moving Devices to Another Configuration Group in Bulk
Rename configuration groups	Renaming a Device Configuration Group
Router Configuration Tasks	
Change device configuration properties	Changing Device Configuration Properties
Edit configuration templates	Editing the ROUTER Configuration Template
Push configurations	Pushing Configurations to Endpoints
Manage applications	Managing GOS Applications
Tunnel Provisioning Tasks	
Configure tunnel provisioning	Configuring Tunnel Provisioning
Edit tunnel provisioning templates	Configuring Tunnel Provisioning Templates
Reprovision tunnels	Tunnel Reprovisioning Factory Reprovisioning
Firmware Management Tasks	
Add firmware groups	Adding Firmware Groups
Assign devices to firmware groups	Assigning Devices to a Firmware Group
Upload images to firmware groups	Uploading a Firmware Image to a FAR Group
Work Order Tasks	
Create work orders	Creating Work Orders

Mesh Endpoint Tasks

Table 3 lists ME tasks. For information about user roles, see System-Defined User Roles.

Table 3   Mesh Endpoint Tasks

Task	Use
ME Configuration Group Tasks	
Add mesh endpoint configuration groups	Creating Device Groups
Delete mesh endpoint configuration groups	Deleting Device Groups
Rename mesh endpoint configuration groups	Renaming a Device Configuration Group
Assign mesh endpoint devices to a configuration group	Moving Devices to Another Group
List devices in a configuration group	Listing Devices in a Configuration Group
ME Configuration Tasks	
Change mesh endpoint configuration properties	Changing Device Configuration Properties
Edit mesh endpoint configuration templates	Editing the ENDPOINT Configuration Template
Push configuration to mesh endpoints	Pushing Configurations to Endpoints
Add mesh endpoint firmware groups	Creating Device Groups
Assign devices to firmware groups	Moving Devices to Another Group
Upload images to firmware groups	Uploading a Firmware Image to a Mesh Endpoint Group

Administration Tasks

Table 4 lists administration tasks.

Table 4   Administration Tasks

Task	Use
System Management Tasks	
Set password policies	Managing the Password Policy
Define roles	Managing Roles
Manage user accounts	Managing Users
Access Management Tasks	
Manage active sessions	Managing Active Sessions
Display the audit trail	Displaying the Audit Trail
Manage certificates	Managing Certificates
Configure data retention	Configuring Data Retention
Manage licenses	Managing Licenses
Manage logging	Managing Logs

Table 4   Administration Tasks (continued)

Task	Use
Configure server settings	Configuring Server Settings
Manage the syslog	Managing the Syslog
Configure tunnel settings	Configuring Provisioning Settings

Document Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x	y	z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

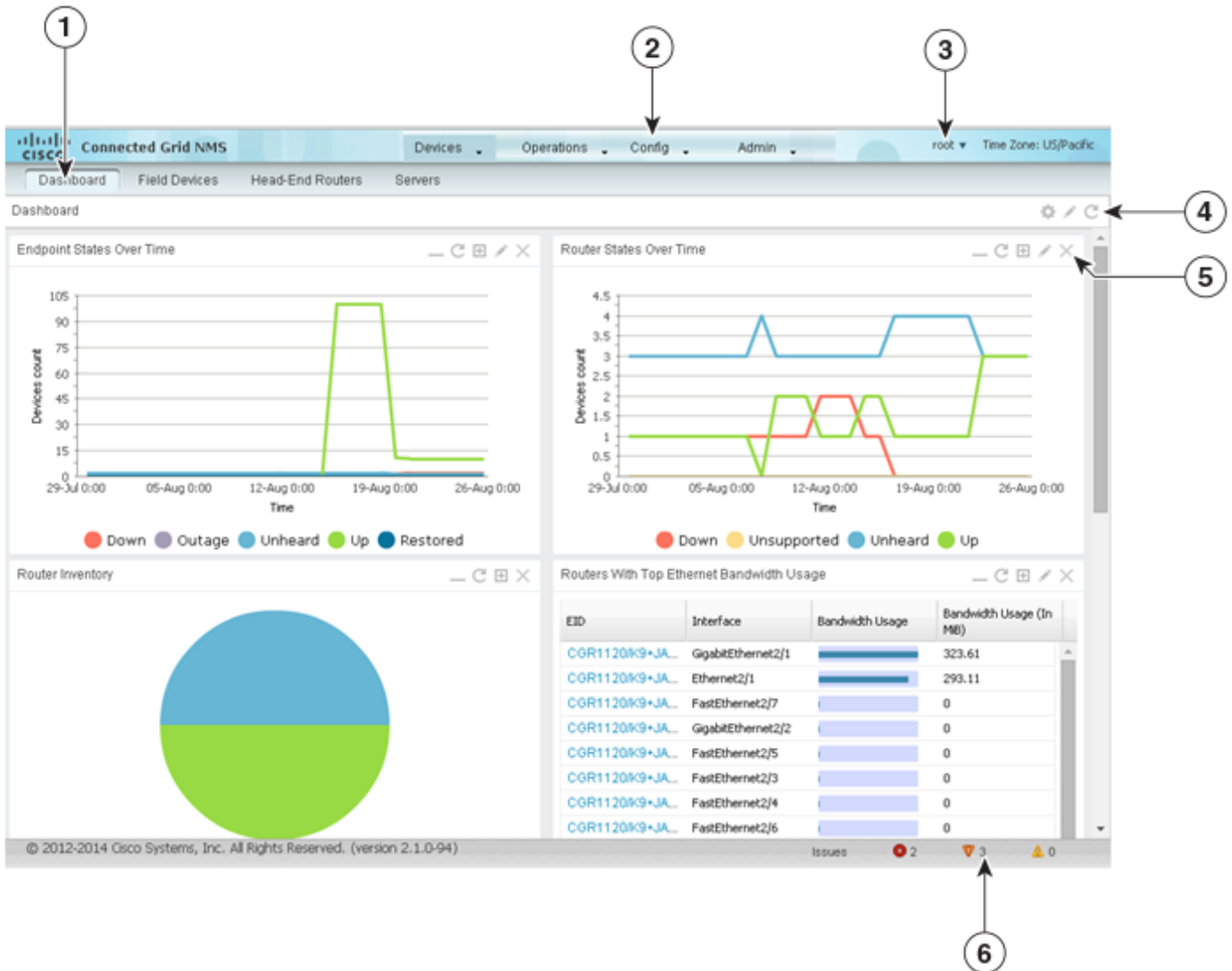**Regulatory:** Provided for additional information and to comply with regulatory and customer requirements.

Interface Overview

This section provides a general overview of the CG-NMS GUI, including:

- Common Page Controls

- Icons

- Main Menus

The CG-NMS dashboard (Figure 4) displays after login (see Using the Dashboard).

Figure 4   CG-NMS Dashboard

1	Submenu tabs	4	Dashboard title bar buttons:
			■ Settings
			■ Interval
			■ Refresh
2	Main menus	5	Dashlet buttons:
			■ Show/Hide
			■ Export
			■ Refresh
			■ Interval/Filter Applied
			■ Close
3	User menu	6	Issues Status bar

Common Page Controls

This section describes buttons, tabs, user-entry fields, and available settings on CG-NMS pages.

Navigating the Main Window

As shown in Figure 5, the top of the CG-NMS window contains the main menus: Devices, Operations, Config, and Admin (3). Roll over these menus to display and select menu options. Submenus display as tabs below the main menus. Each page contains controls for functions specific to that page.

Figure 5   Main Window Elements
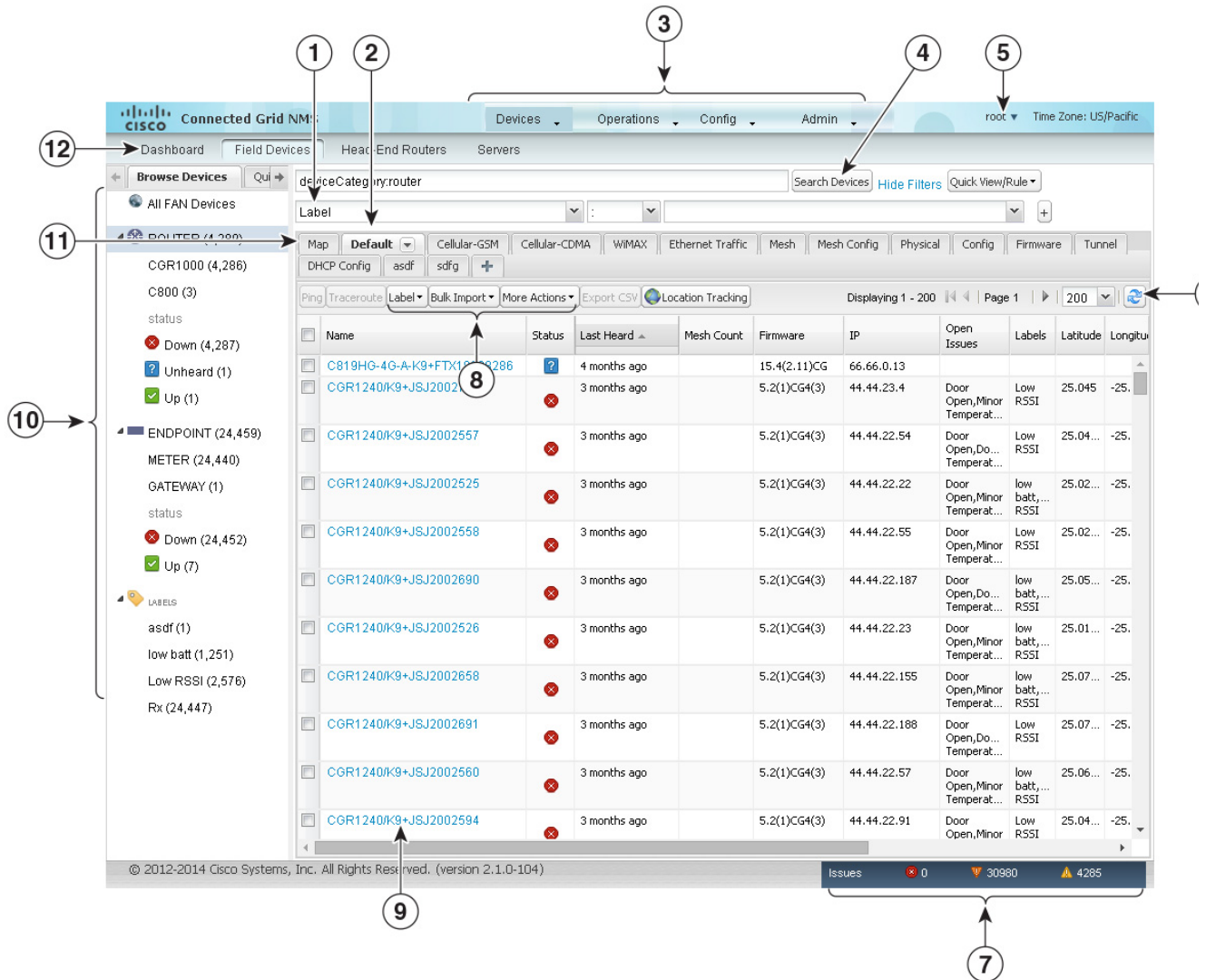
1	Filter label drop-down menu	**7**	Issues Status bar
2	Default list view settings tab	**8**	Device management drop-down menus
3	Main menus	**9**	Device EID link to Device Info page
4	Search query field	**10**	Browse Devices pane
5	User menu	**11**	Map tab
6	Refresh button	**12**	Submenu tabs

Setting User Preferences

Access the <*user name*> drop-down menu in the upper-right of the menu bar (5) to change display settings and the user password, set the local time zone, and log out.

Working with Views

Use the Browse Devices pane (10) to view default and custom groups of devices. At the top of the Browse Devices pane the total number of registered devices displays in parenthesis. The total number of devices in groups displays in parenthesis next to the group name.

You can refine the List display using filters (see Using Filters to Control the Display of Devices). Built-in filters are automatically deployed by clicking a device group in the Browse Devices pane. Use the Quick View tab to access saved custom filters.

Click the device Name or EID (element identifier) link (9) to display a device information page. You can generate work orders directly from the Device Info page, and perform some device-specific tests such as sending a ping the device to determine if it responds in your network. Click the **<<Back** link in the Device Info page to return to the page you were on when you clicked the device EID link. Click the refresh button (6) on any page to update the List view.

When you enable the Issues Status bar (7) in User Preferences, a tally of issues by alarm state displays at the bottom of the browser window (see Viewing Device Severity Status on the Issues Status Bar).

Using the Tabs

When you are on a page, the main menu tab (3) is darkened (for example, in Figure 5 Devices is the main menu for the Routers page). On each page, use the tabs (12) below the main menu bar to access those submenu pages. The tab is lightened when you are on that page (for example, the Routers tab in Figure 5).

Each device page has tabs in the main window (2 and 8) to view associated information. The active tab is lightened when you are on that tab (for example, the Default tab in Figure 5). These tabs are configurable (see Editing Device Views). Click the drop-down arrow on the Default tab to display the Edit/Delete View dialog where you can change the column display in List view. Column widths in List view are also configurable, and you can sort columns in ascending or descending order.

Working with Devices

With device check boxes selected, you can perform device management from the drop-down menus above the list (7):

- Label: Add and remove device label

- Bulk Import: Perform label management, change device properties, and remove devices

- More Actions: Create work orders for routers, refresh router mesh keys, block mesh devices, and remove devices

Navigating Page Views

By default, device management pages display in List view, which displays devices in a sortable table. On the Routers and Mesh pages, select the Map tab (11) to display devices on a GIS map (see Viewing Routers in Map View and Viewing Mesh Endpoints in Map View).

Working with Filters

Create custom filters by clicking the Show Filters link (the Hide Filters link displays in the same place in Figure 5) and using the provided filter parameters (1) to build the appropriate syntax in the Search Devices field (4). Click the Quick Views tab to display saved custom filters (see Creating and Editing Quick View Filters).

Completing User-entry Fields

Figure 6 shows an errored user-entry field. CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button. These errors occur for example, on an invalid character entry (such as, @, #, !, or +) or when an entry is expected and not completed.

Figure 6   Errored Group Name User-entry Field
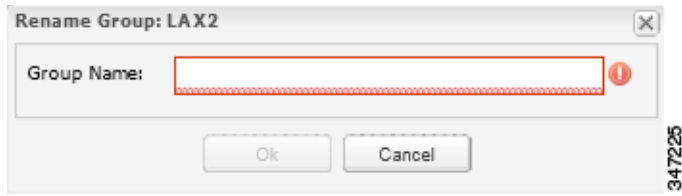
Icons

Table 5 lists the icons that display in the UI.

Table 5   CG-NMS Icons

Icon	Description
	This router icon is used for both CGRs and ISRs (FARs), and HERs.
	This is the server icon.
	This is the DA gateway (IR 500) device icon.
	This is a meter icon.
	This is an undefined endpoint icon.
	The up icon indicates that the device is up and online.
	The down icon indicates that the device is down.
	The unheard icon indicates that the device has not yet registered with CG-NMS.
	The outages icon indicates that the device is under power outage.
	The restored icon indicates that the device has recovered from an outage.
	The default group icon indicates that this is the top-level device group. All devices appear in this group after successful registration.
	This is the Add Group icon.

Table 5   CG-NMS Icons (continued)

Icon	Description
	These are the Edit and Delete Group icons.
	On the Events page, click this button to initiate an export of event data to a CSV file.
	The Group icon indicates that this is a custom device group.
	The Custom Label icon indicates a group of devices. Use labels to sort devices into logical groups. Labels are not dependent on device type; devices of any type can belong to any label. A device can also have multiple labels.
	On the Dashboard page, click this button to set the refresh data interval and add dashlets.
	On the Dashboard page, click this button to initiate an export of dashlet data to a CSV file.
	On the Dashboard page, click this button to refresh dashlet data.
	On the Dashboard page, click this button to change the data retrieval interval setting and add filters to the dashlets. On line-graph dashlets, this button not only provides access to the data retrieval interval setting and filters, but you can also access graph-specific data settings. This icon is green when a filter is applied.
	On the Dashboard page in the dashlet title bar, click this button to show/hide the dashlet. When the dashlet is hidden, only its title bar displays in the Dashboard.
	In Map view, this is the RPL tree root device icon. This can be a CGR or mesh device, as set when Configuring RPL Tree Polling. The colors reflect the device status: Up, Down, and Unheard. The RPL tree connection displays as blue or orange lines. ■ Orange lines indicate that the link is up. ■ Blue lines indicate that the link is down.
	In Map view, this is a device group icon. The colors reflect the device status: Up, Down, and Unheard.

Table 5   CG-NMS Icons (continued)

Icon	Description
	On the Events and Issues pages, and on the Issues Status bar, these icons indicate the event severity level, top-to-bottom, as follows: ■ Critical ■ Major ■ Minor ■ Info Each event type has a preset severity level. For example, a Router Down event is a Major severity level event.
	On the Firmware Update page, click the Schedule Install and Reload button to configure firmware updates.
	On the Firmware Update page, click the Set as Backup button to set the selected image as the firmware image backup.

Main Menus

This section describes the CG-NMS menus available in the title bar at the top of the page.

Devices Menu

The Devices menu provides access to the Dashboard and the device management pages:

■ Dashboard–This user-configurable page displays information about the connected grid

■ Field Devices–This page displays a top-level view of registered routers and mesh endpoints in your grid.

■ Head-End Routers–This page displays a top-level view of registered HERs in your grid.

■ Servers–This page displays a top-level view of NMS and database servers in your network.

Operations Menu

The Operations menu provides access to the following tabs:

■ Events–This page displays events that have occurred in your grid.

■ Issues–This page displays unresolved network events for quick review and resolution by the administrator.

■ Tunnel Status–This page lists provisioned tunnels and displays information about the tunnels and their status.

■ Work Orders–Use this page to create and monitor work orders.

Config Menu

The Config menu provides access to the following tabs:

■ App Management–Use this page to manage applications on IOS-based CGRs.

■ Device Configuration–Use this page to configure device properties.

- Firmware Update–Use this page to view the current firmware image on a device, install a new image on one or multiple devices, and change the firmware group of a device.

- Router File Management–Use this page to view device file status, and upload and delete files from FARs.

- Rules–Use this page to create rules to check for event conditions and metric thresholds.

- Tunnel Provisioning–Use this page to provision tunnels for devices.

Admin Menu

The Admin menu is divided into two areas for managing system settings and user accounts:

- Access Management pages:

  - Password Policy–Use this page to set password conditions that user passwords must meet.

  - Remote Authentication–Use this page to configure remote authentication for CGDM users.

  - Roles–Use this page to define user roles.

  - Users–Use this page to manage user accounts.

- System Management pages:

  - Active Sessions–Use this page to monitor CG-NMS sessions.

  - Audit Trail–Use this page to track user activity.

  - Certificates–Use this page to manage certificates for CSMP (CoAP Simple Management Protocol), CGDM, and the browser (Web) used by CG-NMS.

  - Data Retention–Use this page to determine the number of days to keep event, issue, and metric data in the NMS database.

  - License Center–Use this page to view and manage license files.

  - Logging–Use this page to change the log level for the various logging categories and download logs.

  - Provisioning Settings–Use this page to configure the CG-NMS URL, and the Dynamic Host Configuration Protocol v4 (DHCPv4) Proxy Client and DHCPv6 Proxy Client settings to create tunnels between CGRs and ASRs.

  - Server Settings–Use this page to view and manage server settings.

  - Syslog Settings–Use this page to view and manage syslog settings.

Installing Cisco CG-NMS

This chapter describes how to install CG-NMS and related software, and includes the following topics:

- Before You Install CG-NMS

- Installing and Setting Up the CG-NMS Database

- Installing and Setting Up CG-NMS

- Installing and Configuring the CG-NMS TPS Proxy

- Configuring CG-NMS for Dual-PHY

- Backing Up and Restoring the CG-NMS Database

Before You Install CG-NMS

Use the procedures in the following sections to prepare for your CG-NMS installation:

- CG-NMS Map View Requirements

- System Requirements

- Obtaining CG-NMS and CNR Licenses

- Installing the Linux Packages Required for Installing Oracle

- Obtaining CG-NMS RPM Packages

- Configuring NTP Service

- CG-NMS Installation Overview

CG-NMS Map View Requirements

On any device tab, click the Map button in the main pane to display a GIS map of device locations. In its Map View pane, CG-NMS uses a GIS map to display device locations. However, before you can use this feature, you must configure your firewall to enable access for all CG-NMS operator systems to Cisco-provided GIS map tile servers. Only CG-NMS operator browsers are allowed access to the GIS map tile servers.

Note: The operator browsers will not have access to other Google sites. No Internet access is required for the CG-NMS application server.

You must also assign a fully qualified domain name (FQDN) for each CG-NMS server installation and provide Cisco at ask-cgnms-pm@cisco.com with the following:

- The number of CG-NMS installation environments (test and production)

- The FQDN of the CG-NMS server

- For cluster deployments, the FQDN of any load balancer in the deployment

Note: The FQDN is only used to provision and authorize access to the licensed Cisco CG-NMS installation and make API calls to Enterprise Google Map to download the map tiles. No utility operational data or asset information is ever used (that is, sent over Internet) to retrieve Google map tiles. Map tiles are retrieved only using geographic location information.

FQDN INFORMATION EXAMPLE

For example, your non-cluster installation has a domain named UtilityA.com, and cgnms1 as the hostname with an FQDN of cgms1.UtilityA.com. You would email ask-cgnms-pm@cisco.com and include the FQDN, cgms1.UtilityA.com.

In a cluster deployment with one or more CG-NMS servers and a load balancer with the FQDN of loadbalancer-vip, which directs traffic to the cgnms-main or cnms-dr cluster (DR installations). You would email ask-cgnms-pm@cisco.com and include the FQDN, loadbalancer-vip.UtilityA.com.

System Requirements

Table 1 lists the required hardware and software versions associated with this release.

Table 1   Minimum Hardware and Software Requirements for Cisco CG-NMS and Supporting Systems

Component	Minimum Hardware Requirement	Minimum Software Release

Cisco CG-NMS application server (or comparable system that meets the minimum hardware and software requirements)	Cisco Unified Computing System (UCS) C250 M2 Extended Memory Rack-Mount Server (or comparable system that meets the minimum hardware and software requirements).
	
	■ Processor:
	  – Intel Xeon x5680 2.27 GHz (64-bit)
	  – 4 cores, 2 sockets (8 virtual CPUs)
	■ RAM: 16 GB
	■ Disk space: 500 GB
	■ Hardware Security Module (HSM) or Software Security Module (SSM)
		■ Red Hat Enterprise Linux 6.4, 64-bit with all packages installed (software development and web server)
		■ Internet connection
		
		When you access CG-NMS from a client browser, the browser connects to the Internet to download the necessary data files from the GIS maps provider.
		
		■ A license to use SafeNet for mesh endpoint security
		
		Note: CG-NMS software bundle includes required Java version.

Database server for CG-NMS	Cisco Unified Computing System (UCS) C250 M2 Extended Memory Rack-Mount (or comparable system that meets the minimum hardware and software requirements). ■ Processor: Intel Xeon x5680 (3.33 GHz) 64-bit processor (minimum 20 core CPU [10x2]) ■ RAM: 96 GB ■ Disk space: 16 disks (15K RPM) in RAID-10 configuration; total capacity 2.4 TB (300 GB per disk) ■ Hardware Security Module (HSM) or Software Security Module (SSM)	■ Oracle 11g Enterprise Edition (11.2.0.3 64-bit) ■ Red Hat Linux 6.4, 64-bit with all packages installed (software development and web server) ■ Before installing Oracle, install the Linux packages referenced in the "Installing Cisco CG-NMS" chapter of the CG-NMS User Guide. Specifically, the following section: "Installing the Linux Packages Required for Installing Oracle"

Table 1   Minimum Hardware and Software Requirements for Cisco CG-NMS and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release

Cisco CG-NMS Client	The client must meet the following minimum requirements to connect to the CG-NMS application server and view CG-NMS displays:
	
	■ Windows 7 or Win2000 R2 Server
	
	■ RAM: 8 GB
	
	■ Processor: 2 GHz
	
	■ Resolution: 1024 x 768
		■ Adobe Flash Version 9.0.115 or later (required for viewing charts)
		
		■ Supported browsers:
		
		  – Internet Explorer (IE): 9.0 or 10.0
		
		  – Mozilla Firefox: 3.5 or higher
		
		  – Windows 7 works with IE 9.0 with 128-bit cipher and IE 10.0
		
		  – Win 2008 R2 Server works with IE 8.0 with 256-bits cipher and IE 9.0

Cisco Network Registrar (CNR) (used as a DHCP server)	Server must have the following minimum requirements:
	
	■ Free disk space: 146 GB
	
	■ RAM: 4 GB (small network), 8 GB (average network), 16 GB (large network)
	
	■ Hard drives:
	
	  – SATA drives with 7500 RPM drive > 500 leases/second *or*
	
	  – SAS drives with 15K RPM drive > 1000 leases/second
		The following software environment must exist before installing Cisco Network Registrar, software release 7.2 on the server:
		
		■ Operating System: Linux Red Hat Enterprise Linux 5
		
		■ Java Runtime Environment (JRE) 7.0 (1.7.0_60) or equivalent Java Development Kit (JDK)
		
		■ User interfaces: Web browser and command-line interface (CLI) (Browser versions listed below):
		
		  – Internet Explorer (IE) 8.0, 9.0 (with 9.0.x Flash plug-in) and later
		
		  – Mozilla Firefox 3.0 or later

Cisco 1000 Series Connected Grid Router	–	Cisco IOS Release 15.4(2)CG Cisco CG-OS Release CG4(2) and later
Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	–	Cisco IOS-XE 15.4(1)S, (dated 11/19/13 or later)
Cisco 3900 Series ISR (Integrated Service Router)	–	Cisco IOS Release 15.4(2)T
Cisco 819H ISR (Integrated Service Router)	–	C800-UNIVERSALK9-M Version 15.4(2.12)CG015

Table 1 Minimum Hardware and Software Requirements for Cisco CG-NMS and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release
Cisco CG-NMS TPS proxy	Cisco UCS C200 M2 High-Density Rack Server (or comparable system that meets the minimum hardware and software requirements). ■ RAM: 16 GB ■ Disk space: 150 GB	■ Red Hat Enterprise Linux 6.4, 64-bit with all packages installed (software development and web server) ■ Internet connection When you access CG-NMS from a client browser, the browser connects to the Internet to download the necessary data files from the GIS maps provider. **Note:** CG-NMS software bundle includes required Java version.
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the CG-NMS application servers	Luna SA appliance: ■ Release 6.10.0 firmware **Note:** Contact Safenet to determine if you can run a higher version. ■ Release 5.4.1-2 software Luna SA client software: ■ Release 5.4.1-2 software
Software Security Module (SSM)	■ Windows XP or Windows 2000 R2 Server ■ RAM: 8 GB ■ Processor: 2 GHz	Red Hat Enterprise Linux 6.4
Cisco UCS C200 M2 High-Density Rack Server or comparable system compliant with the minimum hardware and software requirements	■ RAM: 16 GB ■ Disk space: 100 GB ■ Processor: 3 GHZ, 2-core CPU	-

Note: If deploying a CG-NMS server cluster, all nodes in the cluster should run on similar hardware. Additionally, all nodes must run the same version of CG-NMS.

Obtaining CG-NMS and CNR Licenses

■ Contact your Cisco partner to obtain the necessary licenses to use CG-NMS and CNR.

■ Obtain a license to use SafeNet as your HSM for mesh endpoint security.

Installing the Linux Packages Required for Installing Oracle

Install these packages in this order before you install the Oracle database:

1. libaio-devel-0.3.106-5.i386.rpm

2. libaio-devel-0.3.106-5.x86_64.rpm

3. sysstat-7.0.2-11.el5.x86_64.rpm

4. unixODBC-libs-2.2.11-10.el5.i386.rpm

5. unixODBC-libs-2.2.11-10.el5.x86_64.rpm

6. unixODBC-2.2.11-10.el5.i386.rpm

7. unixODBC-2.2.11-10.el5.x86_64.rpm

8. unixODBC-devel-2.2.11-10.el5.i386.rpm

9. unixODBC-devel-2.2.11-10.el5.x86_64.rpm

Obtaining CG-NMS RPM Packages

Before you install and set up your CG-NMS system, ensure that you have the following packages:

RPM Package	Description
cgms-*version_number*.x86_64.rpm	Contains the CG-NMS installer. This is the main RPM that contains the CG-NMS application server itself. Install this package on the CG-NMS application servers.
cgms-oracle-*version_number*.x86_64.rpm	Contains the scripts and tools to create the CG-NMS Oracle database. This package contains the Oracle database template and management scripts. Install this package on the CG-NMS database server system.
cgms-tools-*version_number*.x86_64.rpm	Contains a few optional command-line tools. If needed, install this package on the system running the CG-NMS application server.
cgms-ssm-*version_number*.x86_64.rpm	Contains the Software Security Module (SSM). Install this package on the system running the CG-NMS application server.
cgms-tpsproxy-*version_number*.x86_64.rpm	Contains the TPS proxy application. Install this package on the CG-NMS TPS proxy system.

Configuring NTP Service

Configure all RHEL servers (including all servers that run CG-NMS) in your CG-NMS deployment to have their NTP service enabled and configured to use the same time servers as the rest of the system.

Caution: Before certificates are generated, synchronize the clocks of all system components.

To configure NTP on your RHEL servers:

1. Configure the /etc/ntp.conf file.

   For example:

   ```
   cat /etc/ntp.conf
   ...
   # Use the same NTP servers on all our Connected Grid systems.
   server 0.ntp.example.com
   server 1.ntp.example.com
   server 2.ntp.example.com
   ...
   ```

2. Restart the NTP daemon and ensure that it is set to run at boot time.

```
service ntpd restart
chkconfig ntpd on
```

3. Check the configuration changes by checking the status of the NTP daemon.

This example shows that the system at 192.0.2.1 is configured to be a local NTP server. This server synchronizes its time using the NTP server at 10.0.0.0.

```
# ntpq -p
     remote           refid     st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.1       198.51.100.1    3 u   309 1024  377    0.694    0.899   0.435
 LOCAL(0)        .LOCL.         10 l    36   64  377    0.000    0.000   0.001
```

For information about configuring NTP on RHEL servers, refer to RHEL documentation.

CG-NMS Installation Overview

Complete the following procedures to install CG-NMS:

1. Installing and Setting Up the CG-NMS Database.

2. Installing and Setting Up CG-NMS.

3. Installing and Configuring the CG-NMS TPS Proxy.

Installing and Setting Up the CG-NMS Database

Complete the following procedures to finish your CG-NMS installation:

■ Installation and Setup Overview

■ Downloading and Unpacking Oracle Database

■ Running the Oracle Database Installer

■ Setting Up the CG-NMS Database

■ Additional CG-NMS Database Topics

Installation and Setup Overview

The following topics provide an overview of CG-NMS deployment:

■ Single-Server Deployment

■ High Availability Deployment

Single-Server Deployment

To install and set up CG-NMS database for a single-server database deployment:

1. Log in to the database server.

2. Downloading and Unpacking Oracle Database.

3. Running the Oracle Database Installer.

4. Setting Up the CG-NMS Database.

High Availability Deployment

To install and set up CG-NMS database for HA:

1. Log in to the primary CG-NMS database server.

2. Downloading and Unpacking Oracle Database.

3. Running the Oracle Database Installer.

4. Log in to the standby database server.

5. Downloading and Unpacking Oracle Database.

6. Running the Oracle Database Installer.

7. Setting Up CG-NMS Database for HA.

Downloading and Unpacking Oracle Database

To download the Oracle database:

1. Log in to your server as root.

2. Download Oracle 11g Enterprise Edition (11.2.0.3 64-bit).

3. To avoid display-related errors when installing the Oracle Database software, as root run this command:

   ```
   # xhost + local:oracle
   ```

4. Create the **oracle** user and **dba** group:

   ```
   # groupadd dba
   # adduser -d /home/oracle -g dba -s /bin/bash oracle
   ```

5. Unpack the Oracle Database zip archives.

   ```
   p10404530_112030_Linux-x86-64_1of7.zip
   p10404530_112030_Linux-x86-64_2of7.zip
   p10404530_112030_Linux-x86-64_3of7.zip
   p10404530_112030_Linux-x86-64_4of7.zip
   p10404530_112030_Linux-x86-64_5of7.zip
   p10404530_112030_Linux-x86-64_6of7.zip
   p10404530_112030_Linux-x86-64_7of7.zip
   ```

Running the Oracle Database Installer

Note: Before running the installer, disable the firewall.

To install the Oracle database:

1. Switch to user **oracle** and run the Oracle database installer:

   ```
   # su - oracle
   # setenv DISPLAY <desktop>
   # path_to_DB_installation_folder/database/runInstaller
   ```

2. Click **Yes**, and then click **Next**.

3. Click **Install database software only**, and then click **Next**.

4. Click **Single instance database installation**, and then click **Next**.

5. Select **English** as the language in which the database runs, and then click **Next**.

6. Click **Enterprise Edition (4.29GB)**, and then click **Next**.

7. Select the default installation values, and then click **Next**.

- Oracle Base–**/home/oracle/app/oracle**
- Software Location–**/home/oracle/app/oracle/product/11.2.0/dbhome_1**

Later you will create the environment variables ORACLE_BASE and ORACLE_HOME based on the values of the Oracle Base and Software Location properties.

8. On the **Create Inventory** page, keep the default values, and then click **Next**.

- Inventory Directory–**/home/oracle/app/oraInventory**
- oraInventory_Group Name–**dba**

9. On the **Privileged Operating System Groups** page, keep the default values, and then click **Next**.

- Database Administrator (OSDBA) Group–**dba**
- Database Operator (OSOPER) Group–**dba**

10. (optional) On the **Perform Prerequisite Checks** page, install any required software or run supplied scripts.

The installer might require the installation of additional software based on your system kernel settings, and may also instruct you to run scripts to configure your system and complete the database installation.

11. Click **Fix & Check Again**.

Keep doing this until all requirements are met.

Caution: Do not ignore errors on this page. If there are errors during database installation, CG-NMS may not function properly.

12. Click **Next**.

13. On the **Summary** page, verify the database settings, and then click **Finish** to start the installation process.

14. When prompted, run the supplied configuration scripts.

Because the installer runs as the user oracle, it cannot perform certain installation operations that require root privileges. For these operations, you will be prompted to run scripts to complete the installation process. When prompted, open a terminal window and run the scripts as root.

15. If the installation succeeds, click **Close** on the **Finish** page.

Setting Up the CG-NMS Database

Complete the following procedures to set up the CG-NMS database:

- CG-NMS Database Setup Overview

- Defining Oracle Database Environment Variables

- Installing CG-NMS Oracle Database Scripts

- Creating the CG-NMS Oracle Database

- Starting the CG-NMS Oracle Database

CG-NMS Database Setup Overview

To set up the CG-NMS database:

1. Defining Oracle Database Environment Variables.

2. Installing CG-NMS Oracle Database Scripts.

3. Creating the CG-NMS Oracle Database.

4. Starting the CG-NMS Oracle Database.

Defining Oracle Database Environment Variables

Before installing the CG-NMS Oracle database, switch to the **oracle** user account and define the following Oracle database environment variables.

Table 2 **Oracle Database Environment Variables**

Variable	Description
ORACLE_BASE	Defines the path to the Oracle root directory on your system. For example: `$ export ORACLE_BASE=/home/oracle/app/oracle` If this variable is not set, the CG-NMS setup script displays an error.
ORACLE_HOME	Defines the path to the Oracle home of the CG-NMS database. For example: `$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1` **Note:** Do not have any trailing backslashes in the ORACLE_HOME environment variable.

Table 2   Oracle Database Environment Variables (continued)

Variable	Description
PATH	Defines the path to the Oracle binaries. For example: `$ export PATH=$PATH:$ORACLE_HOME/bin`
LD_LIBRARY_PATH	Defines the path to the libraries. For example: `$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`

ORACLE_SID	Defines the Oracle System ID (SID).
	
	 If you are only using one database server or installing an HA deployment, set this variable on the *primary* database server to **cgms**:
	
	 `$ export ORACLE_SID=cgms`
	
	 If deploying a standby database server, set this variable on the *standby* database server to **cgms_s**:
	
	 `$ export ORACLE_SID=cgms_s`
	
	 If this variable is not set, the CG-NMS setup script displays an error.

You can set these variables manually, as shown in the following example:

On a Single or Primary Database Server	On a Standby Database Server

`$ `**`su - oracle`**
`$ export ORACLE_BASE=/home/oracle/app/oracle`
`$ export`
`ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db`
`home_1`
`$ export PATH=$PATH:$ORACLE_HOME/bin`
`$ export`
`LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
`$ export ORACLE_SID=cgms`
	`$ `**`su - oracle`**
	`$ export ORACLE_BASE=/home/oracle/app/oracle`
	`$ export`
	`ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db`
	`home_1`
	`$ export PATH=$PATH:$ORACLE_HOME/bin`
	`$ export`
	`LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
	`$ export ORACLE_SID=cgms_s`

You can also use a .bashrc file to define these variables.

Installing CG-NMS Oracle Database Scripts

CG-NMS is packaged with scripts and Oracle database templates.

To install the Oracle scripts on your Oracle server:

1. Log in as the root user.

2. Securely copy the CG-NMS Oracle script RPM to your Oracle server:

   ```
   $ scp cgms-oracle-version_number.x86_64.rpm root@oracle-machine:~
   $ rpm –ivh cgms-oracle-version_number.x86_64.rpm
   ```

3. Create the cgms directory and download the scripts and templates to it:

```
$ cd $ORACLE_BASE/app/oracle
$ mkdir cgms
$ cd cgms
$ cp -R /opt/cgms-oracle/scripts .
$ cp -R /opt/cgms-oracle/templates .
$ cp -R /opt/cgms-oracle/tools .
$ cd ..
$ chown -R oracle:dba cgms
```

Creating the CG-NMS Oracle Database

To create the CG-NMS Oracle database in a single-database-server deployment, run the setupCgmsDb.sh script as the user *oracle*. This script starts the Oracle Database and creates the CG-NMS database.

This script creates the user **cgms_dev** used by CG-NMS to access the database. The default password for this user account is **cgms123**.

The default password for the sys DBA account is **cgmsDba123**.

Note: We strongly recommend that you change all default passwords. Do not use special characters such as, @, #, !, or + when using the encryption_util.sh script. The script cannot encrypt special characters.

Note: This script might run for several minutes. To check the setup progress, run the command:
```
$ tail -f /tmp/cgmsdb_setup.log
```

```
$ su - oracle
$ export DISPLAY=localhost:0
$ cd $ORACLE_BASE/cgms/scripts
$ ./setupCgmsDb.sh
09-13-2012 10:38:07 PDT: INFO: ======== CGMS Database Setup Started ==========
09-13-2012 10:38:07 PDT: INFO: Log file: /tmp/cgmsdb_setup.log

Are you sure you want to setup CG-NMS database (y/n)? y

09-13-2012 10:38:08 PDT: INFO: User response: y
09-13-2012 10:38:08 PDT: INFO: CGMS database does not exist.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:38:14 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:38:18 PDT: INFO: User entered CG-NMS DB password.
09-13-2012 10:38:18 PDT: INFO: Stopping listener ...
09-13-2012 10:38:18 PDT: INFO: Listener already stopped.
09-13-2012 10:38:18 PDT: INFO: Deleting database files ...
09-13-2012 10:38:18 PDT: INFO: Creating listener ...
09-13-2012 10:38:19 PDT: INFO: Listener creation completed successfully.
09-13-2012 10:38:19 PDT: INFO: Configuring listener ...
09-13-2012 10:38:19 PDT: INFO: Listener successfully configured.
09-13-2012 10:38:19 PDT: INFO: Creating database. This may take a while. Please be patient ...
09-13-2012 10:42:55 PDT: INFO: Database creation completed successfully.
09-13-2012 10:42:55 PDT: INFO: Updating /etc/oratab ...
09-13-2012 10:42:55 PDT: INFO: /etc/oratab updated.
09-13-2012 10:42:55 PDT: INFO: Configuring database ...
09-13-2012 10:42:56 PDT: INFO: Starting listener ...
09-13-2012 10:42:56 PDT: INFO: Listener start completed successfully.
09-13-2012 10:42:56 PDT: INFO: Starting database configuration ...
09-13-2012 10:43:17 PDT: INFO: Database configuration completed successfully.
```

```
09-13-2012 10:43:17 PDT: INFO: Starting Oracle ...
09-13-2012 10:43:17 PDT: INFO: Starting Oracle in mount state ...
ORACLE instance started.

Total System Global Area 1.6836E+10 bytes
Fixed Size     2220032 bytes
Variable Size 8589934592 bytes
Database Buffers 8187281408 bytes
Redo Buffers   56487936 bytes
Database mounted.
09-13-2012 10:43:26 PDT: INFO: Opening database for read/write ...

Database altered.

09-13-2012 10:43:29 PDT: INFO: ========== CGMS Database Setup Completed Successfully ==========
```

Starting the CG-NMS Oracle Database

To start the CG-NMS Oracle database:

1. Run the script:

   ```
   $ su - oracle
   $ cd $ORACLE_BASE/cgms/scripts
   $ ./startOracle.sh
   ```

2. Configure a cron job that starts CG-NMS database at bootup by running this script:

   ```
   ./installOracleJob.sh
   ```

Additional CG-NMS Database Topics

The following procedures discuss database management:

- Stopping the CG-NMS Oracle Database

- Removing the CG-NMS Database

- Upgrading the CG-NMS Database

- Changing the SYS DBA and CG-NMS Database Passwords

- CG-NMS Database Helper Scripts

Stopping the CG-NMS Oracle Database

Typically, you do not have to stop the Oracle database during the installation procedure. However, if it becomes necessary to stop the Oracle database, use the stop script in the scripts directory:

```
su - oracle
cd $ORACLE_BASE/cgms/scripts
./stopOracle.sh
...
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
...
```

Removing the CG-NMS Database

Caution: The following script is destructive. Do not use this script during normal operation.

To remove the CG-NMS database, run this script:

```
cd $ORACLE_BASE/cgms/scripts
./deleteCgmsDb.sh
```

Upgrading the CG-NMS Database

To upgrade the CG-NMS database:

1. Add the database files (a total of 15 files).

   ```
   ALTER TABLESPACE USERS ADD DATAFILE '&oracle_base/oradata/&sid_caps/users<02 to 15>.dbf' SIZE 5M
   AUTOEXTEND ON;
   ```

This is required for scaling the system.

2. Enable block-change tracking (required for incremental backup):

   ```
   ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
   '&oracle_base/oradata/&sid_caps/rman_change_track.f' REUSE;
   ```

3. Disable parallel execution:

   ```
   set parallel_max_servers = 0 scope=both
   ```

   Caution: The incremental CG-NMS backup script enables the Oracle block-change tracking feature to improve backup performance. To take advantage of this feature, delete your CG-NMS database and run the setupCgmsDb.sh script before performing the first incremental backup. To avoid losing data, run these commands:
   ```
   sqlplus sys/password@cgms as sysdba
   ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
   '/home/oracle/app/oracle/oradata/CGMS/rman_change_track.f' REUSE;
   exit;
   ```

Changing the SYS DBA and CG-NMS Database Passwords

To change default CG-NMS database password for the cgms_dba user:

1. On the CG-NMS server, run the setupCgms.sh script and change the password for the cgms_dba user.

   Caution: The password for the CG-NMS database and the cgnms_dba user password must match or CG-NMS cannot access the database.

   ```
   # cd /opt/cgms/bin
   # ./setupCgms.sh
   ...
   Do you want to change the database password (y/n)? y
   09-13-2012 17:15:07 PDT: INFO: User response: y
   Enter database password:
   Re-enter database password:
   09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
   09-13-2012 17:15:34 PDT: INFO: Database password configured.
   ...
   ```

For information about running the setupCgms.sh script, see Setting Up CG-NMS.

2. On the Oracle server, run the change_password.sh script and change the password for the cgms_dba user:

```
$ ./change_password.sh
09-13-2012 10:48:32 PDT: INFO: ======== Database Password Util Started =========
09-13-2012 10:48:32 PDT: INFO: Log file: /tmp/cgms_oracle.log

Are you sure you want to change CG-NMS database password (y/n)? y
09-13-2012 10:48:33 PDT: INFO: User response: y

Enter current password for SYS DBA:
Re-enter current password for SYS DBA:
09-13-2012 10:48:41 PDT: INFO: User entered current SYS DBA password.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:48:54 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:49:03 PDT: INFO: User entered CG-NMS DB password.
User altered.
...
```

Note: You can also use this script to change the password for the sys user (SYS DBA).

3. On the CG-NMS server, run the cgms_status.sh script to verify the connection between CG-NMS and the CG-NMS database:

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

CG-NMS Database Helper Scripts

Table 3 describes helper CG-NMS database scripts available in the $ORACLE_BASE/cgms/scripts/ directory:

Table 3   CG-NMS Database Helper Scripts

Script	Description
change_password.sh	Use this script to change the passwords for the database administration and CG-NMS database user accounts. The CG-NMS database user account is used by CG-NMS to access the database.
backup_archive_log.sh	Use this script to back up the archive logs.
backupCgmsDb.sh	Use this script to back up the CG-NMS database. This script supports full and incremental backups.
restoreCgmsDb.sh	Use this script to restore the CG-NMS database from a backup.
setupCgmsDb.sh	Use this script to set up CG-NMS database.
startOracle.sh	Use this script to start the CG-NMS database.
stopOracle.sh	Use this script to stop the CG-NMS database.
setupStandbyDb.sh	(CG-NMS database HA installations only) Use this script to set up the standby database server.
setupHaForPrimary.sh	(CG-NMS database HA installations only) Use this script to set up the primary database server.
getHaStatus.sh	Run this script to verify that the database is set up for HA.

Installing and Setting Up the SSM

The Software Security Module (SSM) is a low-cost alternative to a Hardware Security Module (HSM). CG-NMS uses the CSMP protocol to communicate with meters, DA Gateway (IR500 devices), and range extenders. SSM uses CiscoJ to provide cryptographic services such as signing and verifying CSMP messages, and CSMP Keystore management. SSM ensures Federal Information Processing Standards (FIPS) compliance, while providing services. You install SSM on the CG-NMS application server or other remote server. SSM remote-machine installations use HTTPS to securely communicate with CG-NMS.

This section describes SSM installation and set up, including:

- Installing or Upgrading the SSM Server

- Uninstalling the SSM Server

- Integrating SSM and CG-NMS

With the SSM server installed, configured, and started and with CG-NMS configured for SSM, you can view the CSMP certificate on **Admin > Certificates > Certificate for CSMP**.

Note: See Setting Up an HSM Client for information on the Hardware Security Module (HSM).

BEFORE YOU BEGIN

Ensure that the installations meets the hardware and software requirements listed in Table 1.

Installing or Upgrading the SSM Server

To install the SSM server:

1. Run the cgms-ssm-<version>-<release>.<architecture>.rpm rpm script:

```
[root@VMNMS demossm]# rpm -Uvh cgms-ssm-<version>.x86_64.rpm
Preparing...                ########################################### [100%]
   1:cgms-ssm              ########################################### [100%]
```

2. Get the CG-NMS configuration details for the SSM. SSM ships with following default credentials:

- ssm_csmp_keystore password: **ciscossm**

- csmp alias name: **ssm_csmp**

- key password: **ciscossm**

- ssm_web_keystore password: **ssmweb**

```
[root@VMNMS demossm]# cd /opt/cgms-ssm/bin/
[root@VMNMS bin]# ./ssm_setup.sh

oftware Security Module Server
1.Generate a new keyalias with self signed certificate for CSMP
2.Change CSMP keystore password
3.Print CG-NMS configuration for SSM
4.Change SSM server port
5.Change SSM-Web keystore password
Select available options.Press any other key to exit
Enter your choice :
```

3. Enter 3 at the prompt, and complete the following when prompted:

```
Enter current ssm_csmp_keystore password :ciscossm
Enter alias name : ssm_csmp
Enter key password :ciscossm

security-module=ssm
ssm-host=<Replace with IPv4 address of SSM server>
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

4. To connect to this SSM server, copy paste the output from 3. into the cgms.properties file.

Note: You must include the IPv4 address of the interface for CG-NMS to use to connect to the SSM server.

5. (Optional) Run the ssm_setup.sh script to:

- Generate a new key alias with self-signed certificate for CSMP
- Change SSM keystore password
- Change SSM server port
- Change SSM-Web keystore password

Note: If you perform any of the above operations, you must run the SSM setup script, select "Print CG-NMS configuration for SSM," and copy and paste all details into the cgms.properties file.

6. Start the SSM server:

```
[root@VMNMS ~]# service ssm start
Starting Software Security Module Server:              [  OK  ]
```

Monitoring SSM Log Files

You can monitor SSM logs in /opt/cgms-ssm/log/ssm.log

The default metrics report interval is 900 secs (15 min.), which is the minimum valid value. Only servicing metrics are logged. If there are no metrics to report, no messages are in the log.

You can change the metrics report interval by setting the **ssm-metrics-report-interval** field (in secs) in the /opt/cgms-ssm/conf/ssm.properties file.

Note: Your SSM must server is up and running before starting the CG-NMS server.

Uninstalling the SSM Server

This section presents steps to completely uninstall the SSM server, including the steps for a fresh installation.

Note: Do not use this procedure for upgrades. Use the procedure in Installing or Upgrading the SSM Server.

To uninstall the SSM server:

1. Stop the SSM server:

```
service ssm stop
```

2. Copy and move the /opt/cgms-ssm/conf directory and contents to a directory outside of /opt/cgms-ssm.

3. Uninstall the cgms-ssm rpm:

   `rpm -e cgms-ssm`

Fresh installations only

4. Install a new SSM server.

5. Copy and overwrite the /opt/cgms-ssm/conf directory with the contents moved in 2..

Integrating SSM and CG-NMS

Note: You must install and start the SSM server before switching to SSM.

To switch from using the Hardware Security Module (HSM) for CSMP-based messaging and use the SSM:

1. Stop CG-NMS.

   `service cgms stop`

2. Run the ssm_setup.sh script on the SSM server.

3. Select option 3 to print CG-NMS SSM configuration.

4. Copy and paste the details into the cgms.properties to connect to that SSM server.

   EXAMPLE

   ```
   security-module=ssm
   ssm-host=127.107.155.85
   ssm-port=8445
   ssm-keystore-alias=ssm_csmp
   ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
   ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
   ```

5. To set up the HSM, specify the following properties in the cgms.properties file (see also, Setting Up an HSM Client):

   ```
   security-module=ssm/hsm (required; hsm : Hardware Security Module default.)
   hsm-keystore-name=testGroup1 (optional; hsm partition name; testGroup1 default)
   hsm-keystore-password=TestPart1 (optional; encrypted hsm partition password; TestPart1 default)
   ```

6. Ensure that the SSM up and running and you can connect to it.

7. Start CG-NMS.

Installing and Setting Up CG-NMS

Complete the following procedures to finish your CG-NMS installation:

- Installation and Setup Overview

- Installing CG-NMS

- Generating and Installing Certificates

- Setting Up CG-NMS

- Starting CG-NMS

- Checking CG-NMS Status

- Running the CG-NMS Database Migration Script

- Accessing the CG-NMS Web GUI

BEFORE YOU BEGIN

To install CG-NMS, first obtain the CG-NMS installation RPM:

`cgms-version_number.x86_64.rpm`

Note: Ensure that /etc/hosts and /etc/resolv.conf files are correctly configured on the CG-NMS server.

Installation and Setup Overview

These topics provide an overview of the two types of CG-NMS installations:

- Single-Server Deployment
- Cluster Deployment (HA)

Single-Server Deployment

To install and set up CG-NMS for a single-server deployment:

1. Log in to the RHEL server that will host CG-NMS.

2. Installing CG-NMS.

3. Setting Up CG-NMS.

4. Running the CG-NMS Database Migration Script.

5. Checking CG-NMS Status.

6. Accessing the CG-NMS Web GUI

Cluster Deployment (HA)

To install and set up CG-NMS for HA deployments, repeat the steps in Single-Server Deployment, but only run the CG-NMS database migration script once.

Installing CG-NMS

To install the CG-NMS application:

1. Run the CG-NMS installation RPM:

   $ **rpm -ivh cgms-***version***.x86_64.rpm**

2. Verify installation and check the RPM version:

   $ rpm -qa | **grep -i cgms**
   cgms-1.0

Setting Up CG-NMS

To set up CG-NMS, run the setupCgms.sh script.

Note: If deploying a CG-NMS server cluster, the setupCgms.sh script must be run on every node in the cluster.

Caution: The CG-NMS certificate encrypts data in the database. The setupCgms.sh script runs database migration, which requires access to the CG-NMS certificate in the keystore. You must set up certificates must before running setupCgms.sh. The script results in an error if it migrates the database and cannot access the certificate (see Generating and Installing Certificates).

Caution: Ensure that the database password entered while running the setupCgms.sh script is valid. If you enter an invalid password multiple times, Oracle might lock your user account. You can unlock your account on the database server. For more information about unlocking your password, see Unlocking the CG-NMS Database Password.

This example uses the setupCgms.sh script to set up a single-server CG-NMS system that uses one database.

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms

Do you wish to configure another database server for this CG-NMS ? (y/n)? n

09-13-2012 17:11:18 PDT: INFO: User response: n
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y
```

```
Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n

09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n
09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

The setupCgms.sh script lets you configure these settings:

- Configuring Database Settings

- Configuring Database HA

- Configuring the CG-NMS Database Password

- Configuring the Keystore Password

- Configuring the Web root User Password

- Configuring FTPS Settings

Configuring Database Settings

To configure the database settings, the setupCgms.sh script prompts you for this information:

- IP address of the primary CG-NMS database server

- Port number of the CG-NMS database server

  Press Enter to accept the default port number (1522).

- Database System ID (SID), which is cgms for the primary database server

  Press Enter to accept the default SID (cgms). This SID identifies the server as the primary database server.

```
Do you want to change the database settings (y/n)? y
09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

Configuring Database HA

To configure the standby database settings, the setupCgms.sh script prompts you for the following information:

- IP address of the standby CG-NMS database server

- Port number of the standby CG-NMS database server

  Enter **1522**.

- Database System ID (SID), which is cgms for the primary database server

  Enter **cgms_s**. This SID identifies the server as the standby database server.

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.
```

For information about setting up database HA, see Setting Up CG-NMS Database for HA.

Configuring the CG-NMS Database Password

When prompted to change the CG-NMS database password, enter the password of the cgms_dba user account on the database server. If using the default password, do not change the database password now.

```
Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
```

Configuring the Keystore Password

To configure the keystore password:

```
Do you want to change the keystore password (y/n)? y
09-13-2012 10:21:52 PDT: INFO: User response: y

Enter keystore password: keystore_password
Re-enter keystore password: keystore_password

09-13-2012 10:21:59 PDT: INFO: Configuring keystore password. This may take a while. Please wait ...
09-13-2012 10:22:00 PDT: INFO: Keystore password configured.
```

Configuring the Web root User Password

To change the password of the root user account that lets you access the CG-NMS browser-based interface, enter **y** and provide the password:

```
Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n
```

Configuring FTPS Settings

If deploying a cluster, provide the FTPS settings required for downloading logs. FTPS securely transfers files between cluster nodes. If the FTPS settings are not configured, you can only download logs from the CG-NMS node where you are currently logged in.

```
Do you want to change the FTP settings (y/n)? y
09-13-2012 17:16:45 PDT: INFO: User response: y

Enter FTP user password:
Re-enter FTP user password:

09-13-2012 17:16:49 PDT: INFO: Configuring FTP settings. This may take a while. Please wait ...
09-13-2012 17:16:57 PDT: INFO: FTP settings configuration completed successfully
```

Checking CG-NMS Status

Before you can start CG-NMS, check its connection to the CG-NMS database by running this command:

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

This command provides the IP address or hostname and status of the CG-NMS database, and also verifies the connection to the CG-NMS database. If the connection is not verified, you cannot start CG-NMS.

Running the CG-NMS Database Migration Script

CG-NMS uses a special database migration system that lets you quickly migrate your CG-NMS database without having to perform a database dump and restore. Each database migration creates or modifies some of the tables in the CG-NMS database so that CG-NMS can keep a record of migrations already performed.

Before launching CG-NMS the first time, run the database migration script to set up the CG-NMS tables in the database:

```
# cd /opt/cgms/bin
# ./db-migrate
```

Note: This script runs for a few minutes before launching CG-NMS for the first time. Running this script after upgrading to a new version of CG-NMS takes longer depending on the amount of data in the CG-NMS database.

Note: If deploying a CG-NMS server cluster, run the db-migrate script on only one cluster node.

The **db-migrate** command prompts you for the database password. The default password is **cgms123**.

Caution: Ensure that the password entered while running the db-migrate script is the correct password. If you enter an incorrect password multiple times, Oracle might lock your user account. If so, you have to unlock your account on the database server. For more information about unlocking your password, see Unlocking the CG-NMS Database Password.

Accessing the CG-NMS Web GUI

CG-NMS has a self-signed certificate for its Web GUI. You must add a security exception in your browser to access the CG-NMS GUI. Once you start CG-NMS, you can access its web GUI at:

https://*nms_machine_IP_address*/

The initial default username is root; the password is **root123**.

CG-NMS uses the default password of **root123** unless the password was changed when the setup script ran.

For more information on the setup script, see Setting Up CG-NMS.

Note: If the CG-NMS includes the Hardware Security Module (HSM), the Firefox browser will not connect to CG-NMS. To work around this issue, open Firefox Preferences, navigate to **Advanced**, and click the **Encryption** tab. Under Protocols, clear the **Use TLS 1.0** check box. Reconnect to CG-NMS and ensure that the page loaded properly.

First-Time Log In

When you log in to CG-NMS for the first time, a pop-up window (Figure 1) prompts you to change the password.

Figure 1   CG-NMS Initial Password Change

Note: CG-NMS supports a maximum 32-character password length.

Configuring the Time Zone

To configure the time zone, follow these steps:

1. From the *username* drop-down menu (top right), choose **Time Zone**.

2. Select a time zone.

3. Click **Update Time Zone**.

4. Click **OK**.

Changing the Sorting Order of Columns

In all pages where CG-NMS displays a list with column headings, you can change the sort order of columns using the Sort drop-down menu, as shown in this example:

Filtering Lists

CG-NMS lets you define filters. In the following example, typing "ro" in the Filters field of the User Name column drop-down menu lists the active sessions for users with user names that start with "ro." To reset the filter, you can click the **Clear Filter** button.

In the following example, typing the search string **deviceType:cgmesh status:up** in the Search Devices field lists the mesh endpoint devices with an Up status.
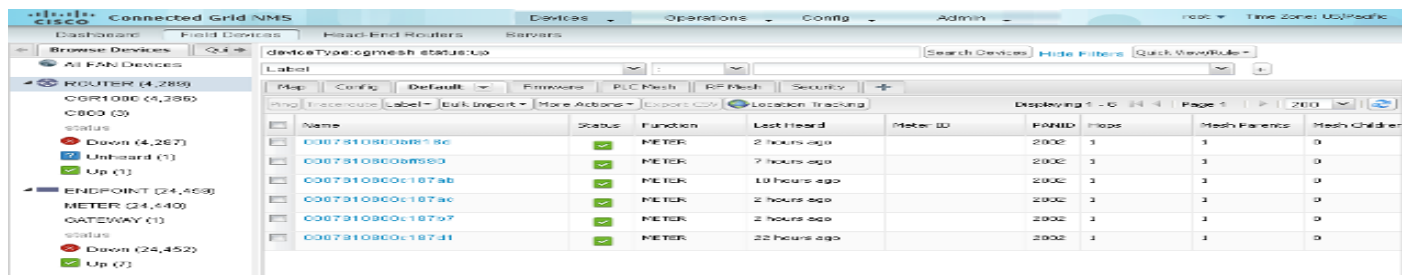
Setting User Preferences

CG-NMS lets you set these user preferences from the *<user name>* drop-down menu (top right):
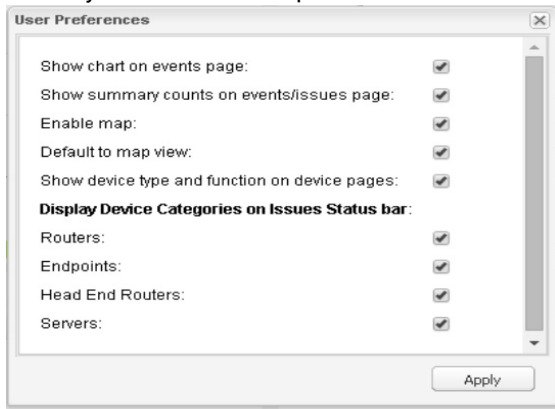
- Enable the display of the Events chart on the Events page (**Operations > Events**).

- Enable the display of event counts on the Events page (**Operations > Events**) and issues counts on the Issues page (**Operations > Issues**). The counts display in the left pane next to the event or issue status.

- Enable the display of the Map View pane (**Devices > Field Devices**).

- Set the default display to Map View (**Devices > Field Devices**).

- Set the device type for issues that display on the Issues Status bar.

Logging Out

To log out of CG-NMS, click **Log Out** in the *<user name>* drop-down menu (top right).

CG-NMS CLIs

This section presents the following commands to manage CG-NMS:

- Starting CG-NMS

- Checking CG-NMS Status

- Stopping CG-NMS

- CG-NMS Log File Location

- CG-NMS Helper Scripts

- Upgrading CG-NMS

- Uninstalling CG-NMS

Starting CG-NMS

To start CG-NMS, run this command:

`service cgms start`

To configure CG-NMS so that it runs automatically at boot time, run this command:

`chkconfig cgms on`

Checking CG-NMS Status

To check CG-NMS status, run this command:

`service cgms status`

Stopping CG-NMS

To stop CG-NMS, run this command:

`service cgms stop`
Note: The application typically takes approximately 10 seconds to stop. Run **ps | grep java** to verify that no Java processes are running.

CG-NMS Log File Location

The CG-NMS log file (server.log) is located in the /opt/cgms/server/cgms/log directory.

CG-NMS Helper Scripts

Table 4 describes the helper CG-NMS scripts in the /opt/cgms/bin/ directory.

Table 4   CG-NMS Helper Scripts

Script	Description
cgms_jmx_client.sh	Java Management Extensions (JMX) client script.
deinstall_cgms_watchdog.sh	Uninstalls the watchdog script.
install_cgms_watchdog.sh	Installs the watchdog script.

Table 4   CG-NMS Helper Scripts (continued)

Script	Description
mcast_test.sh	Tests the communication between cluster members.
password_admin.sh	Changes or resets the user password used to access CG-NMS.
print_cluster_view.sh	Prints cluster members.

Upgrading CG-NMS

Caution: It is important to run the following steps sequentially.

Note: It is not necessary to stop the database during normal upgrades. All upgrades are in-place.

To upgrade the CG-NMS application:

1. Obtain the new CG-NMS RPM.

2. Stop CG-NMS:

   ```
   service cgms stop
   ```

   Note: The application typically takes approximately 10 seconds to stop. Run **ps | grep java** to verify that no Java processes are running.

3. Upgrade the CG-NMS RPM:

   ```
   rpm -Uvh new_cgms_rpm_filename
   ```

   Note: These files overwrite the files in /opt/cgms.

4. Run the database migrations to upgrade the database from the /opt/cgms directory:

   ```
   cd /opt/cgms
   bin/db-migrate
   ```

   Note: You must run the db-migrate script after each upgrade.

5. When prompted, enter the database password. The default password is **cgms123**.

6. Start CG-NMS:

   ```
   # service cgms start
   ```

   You can also use the RHEL GUI to start the CG-NMS service (**Admin > Server Settings > Services**). For information, see the RHEL documentation.

Uninstalling CG-NMS

Note: This deletes all CG-NMS local installation configuration settings and installation files (for example, the keystore with your certificates).

Tip: If you plan to reinstall CG-NMS, copy your current keystore and certificate files to use to overwrite the keystore and certificate files included with the install package.

To remove the CG-NMS application, run these commands:

```
# rpm -e cgms
# rm -rf /opt/cgms
```

Cleaning up the CG-NMS Database

To clean up the CG-NMS database:

1. (HA database configurations) Stop the Observer server.

2. (HA database configurations) Run the $ORACLE_BASE/cgms/scripts/ha/deleteStandbyDb.sh script to delete the standby database.

3. (HA database configurations) Run the $ORACLE_BASE/cgms/scripts/ha/deletePrimaryDbHa.sh script to delete the HA configuration from primary database.

4. Run the $ORACLE_BASE/cgms/scripts/deleteCgmsDb.sh script to delete primary database.

Installing and Configuring the CG-NMS TPS Proxy

The first use of the optional TPS proxy is typically when a CGR sends an inbound request to initialize the portion of ZTD handled by CG-NMS. CG-NMS operates behind a firewall and does not have a publicly reachable IP address. When FARs (CGRs and ISRs) contact CG-NMS for the first time, CG-NMS requires that they use the TPS proxy. This server lets FARs contact the CG-NMS application server to request tunnel provisioning (see Managing Tunnel Provisioning).

The TPS proxy does not have its own GUI. You must edit the properties in the **cgnms.properties** and **tpsproxy.properties-template** files for HTTPS outbound tunnel provisioning requests so that CG-NMS recognizes them as requests from the TPS proxy.

After provisioning the tunnel(s), the FARs can contact CG-NMS directly without using the TPS proxy. CG-NMS is notified of the exact certificate subject from the proxy certificate, and then authenticates that the HTTPS inbound requests are coming from the TPS proxy.

Setting Up the TPS Proxy

Install the cgms-tpsproxy RPM package Java application on a separate (TPS proxy) server to act as a stateless extension of CG-NMS outside the firewall. The TPS proxy can be a Red Hat Enterprise Linux (RHEL) server (see TPS proxy system requirements in Table 1). The cgnms-tpsproxy application runs as a daemon on the server and requires the following configuration parameters:

- URL of the CG-NMS server (to forward inbound requests).

- IP address of the CG-NMS server, as part of a whitelist (approved list) for forwarding outbound requests.

Before you install the TPS proxy, obtain the TPS proxy installation package:

```
cgms-tpsproxy-version_number.x86_64.rpm
```

To configure the proxy-server settings:

1. Configure a RHEL server to use as the TPS proxy.

2. Connect this RHEL server so that it can be reached while outside the firewall.

3. Configure the TPS proxy using the template file:

   ```
   ssh root@tps_proxy_server
   cd /opt/cgms-tpsproxy/conf
   cp tpsproxy.properties-template tpsproxy.properties
   ```

   Note: Edit the cgnms.properties and tpsproxy.properties files after running the encryption_util.sh script during CG-NMS TPS Proxy Enrollment.

4. Edit the tpsproxy.properties file to add the following lines defining the inbound and outbound addresses for the CG-NMS application server:

```
[root@cgr-centos57 conf]# cat tpsproxy.properties-template
inbound-proxy-destination=https://nms_domain_name:9120
outbound-proxy-allowed-addresses=nms_ip_address
cgms-keystore-password-hidden=<obfuscated password>
```

Note: You must edit the properties in the cgnms.properties and tpsproxy.properties-template files for HTTPS outbound tunnel provisioning requests so that CG-NMS recognizes them as requests from the TPS proxy.

Configuring the TPS Proxy Firewall

To configure the TPS proxy firewall:

■ Set up a firewall rule to allow HTTPS connections from the TPS proxy to the CG-NMS server on port 9120 (for HTTPS inbound requests).

■ Set up a firewall rule to allow HTTPS connections from the CG-NMS server to the TPS proxy on port 9122 (for HTTPS outbound requests).

CG-NMS TPS Proxy Enrollment

The enrollment process for the TPS proxy is the same as the CG-NMS enrollment process. The certification authority (CA) that signs the certificate of the CG-NMS application server must also sign the certificate of the TPS proxy. The certificate of the TPS proxy is stored in a Java keystore and is similar to the CG-NMS certificate.

For the enrollment process, consider these scenarios:

■ Fresh installation

– If the keystore password is the same as the default password, change the default password.

Note: We strongly recommend that you change all default passwords. Do not use special characters such as, @, #, !, or + as the encryption_util.sh script cannot encrypt special characters.

– If the keystore password is different from default password, run the encryption_util.sh script and copy the encrypted password to the properties file.

Note: Edit the cgnms.properties and tpsproxy.properties files after running the encryption_util.sh script.

■ Upgrade

Regardless of whether you are using the default password or a custom one, the upgrade process encrypts the password in the /opt/cgms-tpsproxy/conf/tpsproxy.properties file.

For information on CG-NMS enrollment, see: *Generating and Exporting Certificates*.

To enroll the terminal TPS proxy:

1. Create a **cgms_keystore** file.

2. Add your certifications to this file.

3. Copy the file to the **/opt/cgms-tpsproxy/conf** directory.

Configuring CG-NMS to Use the TPS Proxy

You must edit the properties in the cgnms.properties and tpsproxy.properties-template files for HTTPS outbound tunnel provisioning requests so that CG-NMS recognizes them as requests from the TPS proxy. The TPS proxy logs all inbound and outbound requests.

Note: If the properties in the cgnms.properties and tpsproxy.properties-template files are not set, CG-NMS does not recognize the TPS proxy, drops the forwarded request, and considers it from an unknown device.

Note: The following examples employ variable not mandatory values, and are provided as examples only.

To configure CG-NMS to use the TPS proxy:

1. Open an SSH connection to the CG-NMS server:

   ```
   ssh root@nms_machine
   cd /opt/cgms/server/cgms/conf/
   ```

   Note: Edit the cgnms.properties and tpsproxy.properties files after running the encryption_util.sh script during CG-NMS TPS Proxy Enrollment.

2. Edit the **cgms.properties** file to add lines identifying the TPS proxy IP address, domain name, and user subjects in the cgdm-tpsproxy-subject property:

   Note: The cgdm-tpsproxy-subject property must match the installed TPS proxy certificate.

   ```
   cgdm-tpsproxy-addr=proxy_server_IP_address
   cgdm-tpsproxy-subject=CN="common_name", OU="organizational_unit", O="organization", L="location",
   ST="state", C="country"
   ```

   Note: Use quotes around comma-separated strings.

Starting the CG-NMS TPS Proxy

Start the TPS proxy after it is installed, configured, and enrolled.

To start the TPS proxy, run the start script:

```
service tpsproxy start
```

The TPS proxy log file is located at:

```
/opt/cgms-tpsproxy/log/tpsproxy.log
```

Note: For information, see TPS Proxy Validation.

TPS Proxy Validation

The TPS proxy logs all HTTPS inbound and outbound requests in the TPS proxy log file located at /opt/cgms-tpsproxy/log/tpsproxy.log

The following entry in the TPS proxy tpsproxy.log file defines inbound requests for a CGR:

```
73: cgr-centos57: May 21 2014 01:05:20.513 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][eid=CGR1240/K9+JAF1732ARCJ][ip=192.168.201.5][sev=INFO][tid=qtp46675819-29]:
Inbound proxy request from [192.168.201.5] with client certificate subject [CN=CGRJAF1732ARCJ.example.com,
SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

This message entry in the TPS proxy tpsproxy.log file indicates that the TPS successfully forwarded the message to CG-NMS:

```
74: cgr-centos57: May 21 2014 01:05:20.564 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][sev=INFO][tid=com.cisco.cgms.tpsproxy.TpsProxyServlet-49dc423f-22]: Completed
inbound proxy request from [192.168.201.5] with client certificate subject [CN=CGRJAF1732ARCJ.example.com,
SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

The following entry in the CG-NMS server log file identifies the TPS proxy:

```
Request came from proxy
Using forwarded client subject (CN=cg-cgr-1, SERIALNUMBER=PID:CGR1240/K9 SN:JSJ15220047) for authentication
```

The following entry in the TPS proxy tpsproxy.log file defines outbound requests:

```
%CGMS-6-UNSPECIFIED: %[ch=TpsProxyOutboundHandler][ip=192.168.205.5][sev=INFO][tid=qtp257798932-15]: Outbound
proxy request from [192.168.205.5] to [192.168.201.5:8443]
```

The following entry in the CG-NMS server log file identifies the HTTPS connection:

```
Using proxy at 192.168.201.6:9122 to send to https://192.168.201.4:8443/cgdm/mgmt commands:
```

Configuring CG-NMS for Dual-PHY

For Dual-PHY CGRs, you must configure all Dual-PHY WPAN modules–master and slaves–by setting the Dual-PHY parameters (see Table 12) in the device addition file. The parameters to set in the appropriate device addition file are **masterWpanInterface** and **slaveWpanInterface**. For slave Dual-PHY WPAN devices, you must also set the **slave-mode** parameter.

Note: See the *Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)* for Dual-PHY CGR configuration information.

EXAMPLE

The following instructs CG-NMS which WPAN devices to allocate as the master interface and slave interface during the configuration push:

```
deviceType,eid,ip,meshPrefixConfig,meshPrefixLengthConfig,meshPanidConfig,meshAddressConfig,dhcpV4LoopbackLin
k,dhcpV4TunnelLink,dhcpV6LoopbackLink,dhcpV6TunnelLink,tunnelSrcInterface1,tunnelHerEid,adminUsername,adminPa
ssword,certIssuerCommonName,ipsecTunnelDestAddr1,masterWpanInterface,slaveWpanInterface,lat,lng
cgr1000,CGR1240/K9+JAF1741BFQS,2.2.56.253,2319:DEAD:BEEF:CAFE::,64,1233,2319:DEAD:BEEF:CAFE::,20.211.0.1,20.2
11.0.1,2001:420:7bf:7e8::1,2001:420:7bf:7e8::1,GigabitEthernet2/1,cg-isr900,cg-nms-administrator,0ERIF+cKsLwy
T0YTFd0k+NpVAAPxcIvFfoX1sogAXVkSOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+pEQ1aIQvIGuIas9wp9MKUARYpNErXRiHEnpeH
044Rfa4uSgsWXEyrVNxHyuvSefB5j6H0uA7tIQwEHDXOiq/d0yxvfd4IYos7NzPXlJNiR+Cp6bwx7dG+d9Jo+JuNxLXpi8Fo5n88usjMoXPNb
yrqvgn7SS4f+VYgXx1iyDNP0k+7OEE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMijPstDBXpFv8dqtA0xDGKu
aRg==,cenbursaca-cenbu-sub-ca,2.2.55.198,Wpan3/1,Wpan5/1,41.413324,-120.920315
```

The following is a typical template for configuring the master/slave interface on CGR WPAN modules:

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154  panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
ieee154 ssid cisco_muruga_dual
ieee154 txpower 21
slave-mode 3
rpl dag-lifetime 240
rpl dio-min 21
rpl version-incr-time 240
authentication host-mode multi-auth
authentication port-control auto
ipv6 dhcp relay destination global  2001:420:7BF:5F::705
```

Configuring CG-NMS for Dual-PHY

```
dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
end
```

Mesh Security Keys for Dual-PHY Devices

Note: Do not configure mesh security keys on slave WPAN devices.

With master/slave mode configured correctly in CG-NMS, CG-NMS automatically detects the master WPAN and sets its the mesh security keys. When configuring an existing CGR and adding another WPAN interface, remove all mesh security keys from both interfaces, and then configure master/slave mode through CG-NMS. If CGRs are connected, all meters go through re-authentication.

You can remove mesh keys using the command:

```
mesh-security expire mesh-key interface wpan <slot>/<slot number>
```

Configuration Example

The following examples retrieve the current Dual-PHY WPAN device RPL slot tree, RPL slot table, RPL IP route info table, and configuration information for slots 4/1 and 3/1.

```
cisco-NXT-FAR5#show wpan 4/1 rpl stree

--------------------------- WPAN RPL SLOT TREE [4] ---------------------------

  [2001:RTE:RTE:64::4]
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800     // SY RF nodes
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
                 \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
                  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
                          \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
```

```
                              \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
                              \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00     // CY PLC nodes
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
          \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07


RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)



cisco-NXT-FAR5#ping 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms

cisco-NXT-FAR5#ping 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-NXT-FAR5#

cisco-NXT-FAR5#show wpan 4/1 rpl stable

----------------------------- WPAN RPL ROUTE SLOT TABLE [4] -----------------------------
NODE_IPADDR                    NEXTHOP_IP                     SSLOT LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800    2001:RTE:RTE:64::4                     3      17:49:12
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801    2001:RTE:RTE:64::4                     3      18:14:05
2001:RTE:RTE:64:207:8108:3C:1802    2001:RTE:RTE:64::4                     3      18:14:37
2001:RTE:RTE:64:207:8108:3C:1803    2001:RTE:RTE:64::4                     3      17:56:56
2001:RTE:RTE:64:207:8108:3C:1804    2001:RTE:RTE:64::4                     3      17:48:53
2001:RTE:RTE:64:207:8108:3C:1805    2001:RTE:RTE:64::4                     3      17:47:52
2001:RTE:RTE:64:207:8108:3C:1806    2001:RTE:RTE:64::4                     3      17:49:54
2001:RTE:RTE:64:207:8108:3C:1807    2001:RTE:RTE:64::4                     3      17:46:38
2001:RTE:RTE:64:207:8108:3C:1808    2001:RTE:RTE:64::4                     3      18:22:01
2001:RTE:RTE:64:207:8108:3C:1809    2001:RTE:RTE:64::4                     3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180A    2001:RTE:RTE:64::4                     3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180B    2001:RTE:RTE:64::4                     3      18:24:00
2001:RTE:RTE:64:207:8108:3C:1A00    2001:RTE:RTE:64:207:8108:3C:1801       3      17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01    2001:RTE:RTE:64:207:8108:3C:180B       3      18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02    2001:RTE:RTE:64:207:8108:3C:180B       3      18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03    2001:RTE:RTE:64:207:8108:3C:1805       3      18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04    2001:RTE:RTE:64:207:8108:3C:180B       3      17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05    2001:RTE:RTE:64:207:8108:3C:180B       3      18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06    2001:RTE:RTE:64:207:8108:3C:180B       3      18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07    2001:RTE:RTE:64:207:8108:3C:1805       3      17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08    2001:RTE:RTE:64:207:8108:3C:180B       3      18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09    2001:RTE:RTE:64:207:8108:3C:180B       3      18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A    2001:RTE:RTE:64:207:8108:3C:180B       3      18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B    2001:RTE:RTE:64:207:8108:3C:180B       3      18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00    2001:RTE:RTE:64:207:8108:3C:1A0A       3      18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01    2001:RTE:RTE:64:207:8108:3C:1A0A       3      18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02    2001:RTE:RTE:64:207:8108:3C:1A06       3      18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03    2001:RTE:RTE:64:207:8108:3C:1A05       3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04    2001:RTE:RTE:64:207:8108:3C:1A06       3      18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05    2001:RTE:RTE:64:207:8108:3C:1A01       3      18:10:02
```

Configuring CG-NMS for Dual-PHY

```
2001:RTE:RTE:64:207:8108:3C:1C06      2001:RTE:RTE:64:207:8108:3C:1A01      3       18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07      2001:RTE:RTE:64:207:8108:3C:1A01      3       18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08      2001:RTE:RTE:64:207:8108:3C:1A05      3       18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09      2001:RTE:RTE:64:207:8108:3C:1A05      3       18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A      2001:RTE:RTE:64:207:8108:3C:1A05      3       18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B      2001:RTE:RTE:64:207:8108:3C:1A0A      3       18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00      2001:RTE:RTE:64::4                    4       18:21:40
// CY PLC nodes
2001:RTE:RTE:64:217:3BCD:26:4E01      2001:RTE:RTE:64::4                    4       17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02      2001:RTE:RTE:64::4                    4       18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03      2001:RTE:RTE:64::4                    4       17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04      2001:RTE:RTE:64::4                    4       18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05      2001:RTE:RTE:64::4                    4       18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06      2001:RTE:RTE:64::4                    4       18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07      2001:RTE:RTE:64::4                    4       18:24:04


Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)

cisco-NXT-FAR5#show wpan 4/1 rpl itable


--------------------------- WPAN RPL IPROUTE INFO TABLE [4] ---------------------------
NODE_IPADDR            RANK  VERSION   NEXTHOP_IP                     ETX_P     ETX_LRSSIR  RSSIF HOPS  PARENTS    SSLOT
2001:RTE:RTE:64:207:8108:3C:1800    835   1    2001:RTE:RTE:64::4                       0       762   -67   -71   1    1    3
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801    692   2    2001:RTE:RTE:64::4                       0       547   -68   -67   1    1    3
2001:RTE:RTE:64:207:8108:3C:1802    776   2    2001:RTE:RTE:64::4                       0       711   -82   -83   1    1    3
2001:RTE:RTE:64:207:8108:3C:1803    968   2    2001:RTE:RTE:64::4                       0       968   -72   -63   1    1    3
2001:RTE:RTE:64:207:8108:3C:1804    699   1    2001:RTE:RTE:64::4                       0       643   -71   -66   1    1    3
2001:RTE:RTE:64:207:8108:3C:1805    681   1    2001:RTE:RTE:64::4                       0       627   -70   -64   1    1    3
2001:RTE:RTE:64:207:8108:3C:1806    744   1    2001:RTE:RTE:64::4                       0       683   -69   -68   1    1    3
2001:RTE:RTE:64:207:8108:3C:1807    705   1    2001:RTE:RTE:64::4                       0       648   -76   -63   1    1    3
2001:RTE:RTE:64:207:8108:3C:1808    811   2    2001:RTE:RTE:64::4                       0       811   -68   -69   1    2    3
2001:RTE:RTE:64:207:8108:3C:1809    730   1    2001:RTE:RTE:64::4                       0       692   -68   -70   1    1    3
2001:RTE:RTE:64:207:8108:3C:180A    926   1    2001:RTE:RTE:64::4                       0       926   -66   -68   1    1    3
2001:RTE:RTE:64:207:8108:3C:180B    602   1    2001:RTE:RTE:64::4                       0       314   -74   -69   1    1    3
2001:RTE:RTE:64:207:8108:3C:1A00    948   1    2001:RTE:RTE:64:207:8108:3C:1801        692     256   -73   -75   2    1    3
2001:RTE:RTE:64:207:8108:3C:1A01    646   2    2001:RTE:RTE:64:207:8108:3C:180B        323     256   -73   -75   2    3    3
2001:RTE:RTE:64:207:8108:3C:1A02    948   1    2001:RTE:RTE:64:207:8108:3C:180B        602     256   -73   -75   2    2    3
2001:RTE:RTE:64:207:8108:3C:1A03    803   2    2001:RTE:RTE:64:207:8108:3C:1805        503     256   -68   -78   2    3    3
2001:RTE:RTE:64:207:8108:3C:1A04    858   1    2001:RTE:RTE:64:207:8108:3C:180B        602     256   -65   -69   2    1    3
2001:RTE:RTE:64:207:8108:3C:1A05    646   2    2001:RTE:RTE:64:207:8108:3C:180B        323     256   -71   -69   2    2    3
2001:RTE:RTE:64:207:8108:3C:1A06    858   1    2001:RTE:RTE:64:207:8108:3C:180B        602     256   -73   -75   2    2    3
2001:RTE:RTE:64:207:8108:3C:1A07    979   1    2001:RTE:RTE:64:207:8108:3C:1805        627     352   -71   -73   2    1    3
2001:RTE:RTE:64:207:8108:3C:1A08    646   2    2001:RTE:RTE:64:207:8108:3C:180B        390     256   -75   -70   2    3    3
2001:RTE:RTE:64:207:8108:3C:1A09    948   1    2001:RTE:RTE:64:207:8108:3C:180B        602     256   -70   -69   2    3    3
2001:RTE:RTE:64:207:8108:3C:1A0A    646   2    2001:RTE:RTE:64:207:8108:3C:180B        390     256   -75   -71   2    2    3
2001:RTE:RTE:64:207:8108:3C:1A0B    858   1    2001:RTE:RTE:64:207:8108:3C:180B        602     256   -68   -68   2    2    3
2001:RTE:RTE:64:207:8108:3C:1C00    902   2    2001:RTE:RTE:64:207:8108:3C:1A0A        646     256   -70   -74   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C01    902   2    2001:RTE:RTE:64:207:8108:3C:1A0A        646     256   -71   -72   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C02    1114  1    2001:RTE:RTE:64:207:8108:3C:1A06        858     256   -74   -73   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C03    1114  1    2001:RTE:RTE:64:207:8108:3C:1A05        858     256   -76   -77   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C04    902   2    2001:RTE:RTE:64:207:8108:3C:1A06        646     256   -75   -68   3    2    3
2001:RTE:RTE:64:207:8108:3C:1C05    1114  1    2001:RTE:RTE:64:207:8108:3C:1A01        858     256   -66   -74   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C06    1114  1    2001:RTE:RTE:64:207:8108:3C:1A01        858     256   -74   -72   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C07    1114  1    2001:RTE:RTE:64:207:8108:3C:1A01        858     256   -70   -75   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C08    1114  1    2001:RTE:RTE:64:207:8108:3C:1A05        858     256   -74   -70   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C09    1114  1    2001:RTE:RTE:64:207:8108:3C:1A05        858     256   -70   -74   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C0A    1114  1    2001:RTE:RTE:64:207:8108:3C:1A05        858     256   -70   -69   3    1    3
2001:RTE:RTE:64:207:8108:3C:1C0B    902   2    2001:RTE:RTE:64:207:8108:3C:1A0A        646     256   -76   -74   3    1    3
2001:RTE:RTE:64:217:3BCD:26:4E00    616   2    2001:RTE:RTE:64::4                       0       616   118   118   1    1    4    // CY PLC
nodes
2001:RTE:RTE:64:217:3BCD:26:4E01    702   1    2001:RTE:RTE:64::4                       0       646   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E02    557   2    2001:RTE:RTE:64::4                       0       557   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E03    626   1    2001:RTE:RTE:64::4                       0       579   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E04    609   2    2001:RTE:RTE:64::4                       0       609   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E05    602   2    2001:RTE:RTE:64::4                       0       602   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E06    594   2    2001:RTE:RTE:64::4                       0       594   118   118   1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E07    584   2    2001:RTE:RTE:64::4                       0       584   118   118   1    1    4


Number of Entries in WPAN RPL IPROUTE INFO TABLE: 44


cisco-NXT-FAR5#


cisco-NXT-FAR5#show run int wpan 4/1
Building configuration...
Current configuration : 320 bytes
!
interface Wpan4/1
 no ip address
```

```
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
 ieee154 panid 5552
 ieee154 ssid ios_far5_plc
 ipv6 address 2001:RTE:RTE:64::4/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end

cisco-NXT-FAR5#show run int wpan 3/1
Building configuration...
Current configuration : 333 bytes
!
interface Wpan3/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
 ieee154 panid 5551
 ieee154 ssid ios_far5_rf
 slave-mode 4
 ipv6 address 2001:RTE:RTE:65::5/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end
```

Backing Up and Restoring the CG-NMS Database

The following topics demonstrate how CG-NMS supports both full and incremental database backups:

- Before You Begin

- Creating a Full Backup of the CG-NMS Database

- Scheduling a Full CG-NMS Backup

- Restoring a CG-NMS Backup

Before You Begin

Before backing up your CG-NMS database:

1. Download and install the latest cgms-oracle-*version_number*.x86_64.rpm package.

2. Copy the scripts, templates, and tools folders from the /opt/cgms-oracle folder to the $ORACLE_BASE/cgms folder.

3. Set the ownership of the files and folders you copied to oracle:dba.

Creating a Full Backup of the CG-NMS Database

Full backups back up all the blocks from the data file. Full backups are time consuming and consume more disk space and system resources than partial backups.

CG-NMS lets you perform full hot backups of CG-NMS database. In a hot backup, CG-NMS and the CG-NMS database are running during the backup.

Note: The destination backup directory must be writable by the oracle user and have enough space for the CG-NMS data.

To create a backup file of the CG-NMS software:

1. On the CG-NMS database server, open a CLI window.

2. Switch to the user oracle:

   ```
   su - oracle
   ```

3. Change directory to the location of the CG-NMS backup script (backupCgmsDb.sh):

   ```
   cd /home/oracle/app/oracle/cgms/scripts
   ```

4. Run the backup script and specify the destination folder. For example, to store the backup data in the /home/oracle/bkp folder, enter this command:

   ```
   ./backupCgmsDb.sh full /home/oracle/bkp
   08-03-2012 15:54:10 PST: INFO: ========== CGMS Database Backup Started ==========
   08-03-2012 15:54:10 PST: INFO: Log file: /tmp/cgms_backup_restore.log
   Are you sure you want to backup CG-NMS database (y/n)? y
   ```

5. Enter y to begin the backup process.

Scheduling a Full CG-NMS Backup

To schedule a full CG-NMS backup to run daily at 1:00 AM (default setting):

Note: The destination backup directory must be writable by the oracle user and have enough space for the CG-NMS data.

1. On the CG-NMS database server, open a CLI window.

2. Switch to the user *oracle*:

   ```
   su - oracle
   ```

3. Change directory to the location of the CG-NMS backup script (backupCgmsDb.sh):

   ```
   cd /home/oracle/app/oracle/cgms/scripts
   ```

4. Run the backup script and specify the destination folder.

To change the backup scheduling interval, edit the installCgmsBackupJob.sh script before running it.
For example, to store the backup data in /home/oracle/bkp, enter this command:

```
./installCgmsBackupJob.sh /home/oracle/bkp
```

To delete the backup job, enter these commands:

```
cd /home/oracle/app/oracle/cgms/scripts
./deinstallCgmsBackupJob.sh
```

Backing Up the CG-NMS Database Incrementally

Incremental backups only back up data file blocks that changed since the previous specified backup. CG-NMS supports two incremental backup levels, and an hourly log backup:

- incr0–Base backup for subsequent incremental backups. This is similar to a full backup. For large deployments (millions of mesh endpoints and several thousand FARs). Run incr0 backups twice a week.

- incr1–Differential backup of all blocks changed since the last incremental backup. For large deployments (millions of mesh endpoints and several thousand FARs), run incr1 backups once a day.

Note: An incr0 backup must run before an incr1 backup to establish a base for the incr1 differential backup.

■ Hourly archivelog backup–The Oracle Database uses archived logs to record all changes made to the database. These files grow over time and can consume a large amount of disk space. Schedule the backup_archive_log.sh script to run every hour. This script backs up the database archive (.arc) log files, stores them on a different server, and deletes the source archivelog files to free space on the database server.

Tip: Before performing any significant operation that causes many changes in the CG-NMS database (for example, importing a million mesh endpoints or uploading firmware images to mesh endpoints), perform am incr0 backup. After the operation completes, perform another incr0 backup, and then resume the scheduled incremental backups.

Performing an Incremental Backup

Note: The destination backup directory must be writable by the oracle user and have enough space for the CG-NMS data.

To perform an incremental backup:

1. On the CG-NMS database server, open a CLI window.

2. Switch to the user *oracle* and change directory to the location of the CG-NMS backup script:

```
su - oracle
cd /home/oracle/app/oracle/cgms/scripts
```

3. Run the backup script and specify the incremental backup level and the destination folder where the backup data is stored (for example, /home/oracle/bkp). For example, to perform an incr0 backup to/home/oracle/bkp, enter the command:

```
./backupCgmsDb.sh incr0 /home/oracle/bkp
```

To perform an incr1 backup, enter the command:

```
./backupCgmsDb.sh incr1 /home/oracle/bkp
```

Restoring a CG-NMS Backup

Perform database backups and restores using the scripts provided in the cgms-oracle.rpm package. If using the supplied scripts, backups and restores only work if performed on the same Oracle database version.

Note: Backups from Oracle version 11.2.0.1 can only be restored on v11.2.0.1 if using the supplied scripts. Backups do not work across different versions of Oracle, for example, a backup taken on 11.2.0.1 cannot be restored on 11.2.0.3 using the supplied scripts. If a database upgrade from 11.2.0.1 to 11.2.0.3 is required, follow the Oracle upgrade procedure. Refer to the Oracle upgrade document and Web site.

CG-NMS supports restoring CG-NMS backups on the same host or different host. If you choose to restore CG-NMS backups on a different host, ensure that the host runs the same or a higher version of the Oracle database software and that CG-NMS database on the destination host was created using the setupCgmsDb.sh script.

Note: CG-NMS does not support cross-platform backups.

To restore a CG-NMS backup:

1. Stop CG-NMS.

```
service cgms stop
```
2. Switch to the user oracle, change directories to the script location, and stop Oracle:

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./stopOracle.sh
```

3. To restore the CG-NMS database, run the command:

```
./restoreCgmsDb.sh full-backup-file
```

Tip: Performing a restore from a full backup can be time consuming. For large deployments, we recommend restoring the database from incremental backups.

To restore CG-NMS database from an incremental backup, run these commands and specify the path to last incremental backup file:

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./restoreCgmsDb.sh last-incr1-backup-file
```

The restore script might display these errors:

```
06-08-2012 13:12:56 PDT: INFO: Import completed successfully
06-08-2012 13:12:56 PDT: INFO: Shared memory file system. Required (1K-blocks): 6084456, Available
(1K-blocks): 4083180
06-08-2012 13:12:56 PDT: ERROR: Insufficient shared memory file system. Increase your shared memory file
system before restoring this database.
06-08-2012 13:12:56 PDT: ERROR: ========== CGMS Database Restore Failed ==========
06-08-2012 13:12:56 PDT: ERROR: Check log file for more information.
```

To avoid these errors, increase the size of the shared memory file system:

```
###### as "root" user
###### Following command allocates 6G to shm. Adjust size as needed.
# umount tmpfs
# mount -t tmpfs tmpfs -o size=6G /dev/shm

###### Edit /etc/fstab and replace defaults as shown below
tmpfs                   /dev/shm                tmpfs   size=6G       0 0
```

4. Start Oracle:

```
./startOracle.sh
```

5. Change directories to /opt/cgms and run the db-migrate script:

```
$ cd /opt/cgms
$ bin/db-migrate
```

When you restore a CG-NMS database, the restore script restores the database to the CG-NMS version the database was using. An error returns if you restore an old database to a newer version of CG-NMS. Run the migrate script to ensure that the database runs with the current version of CG-NMS.

6. Start CG-NMS:

```
service cgms start
```

For disaster recovery, perform a clean restore. The script starts by deleting the current CG-NMS database:

```
$ su -oracle
$ cd /home/oracle/app/oracle/cgms/scripts
$ ./deleteCgmsDb.sh
INFO: ======== CGMS Database Deletion Started - 2011-10-16-07-24-09 =========
INFO: Log file: /tmp/cgmsdb_setup.log
INFO: Deleting database. This may take a while. Please be patient ...
INFO: Delete database completed successfully
INFO: ========== CGMS Database Deletion Completed Successfully - 2011-10-16-07-25-01 ==========
```

If a clean restore is not required, use the Oracle tool to restore the database.

Generating and Installing Certificates

This chapter describes how to generate and install certificates, and includes the following topics:

- Information About Certificates
- Generating and Exporting Certificates
- Installing the Certificates
- Configuring CG-NMS to Access the Keystore
- Configuring the TPS Proxy to Access the Keystore
- Setting Up an HSM Client
- Configuring the HSM Group Name and Password

Information About Certificates

The following topics provide information on certificates:

- Role of Certificates
- Keystore

Role of Certificates

All communications between the Cisco 1000 Series Connected Grid Router (CGR 1000 or CGR) and the Cisco Connected Grid Network Management System (CG-NMS) must be authenticated in both directions through mutual authentication. Before mutual authentication can occur, the Cisco CG-NMS and the CGR must each have a certificate signed by the same Certificate Authority (CA). You can employ either a root CA or subordinate CA (subCA).

For details on generating certificates for CGRs, refer to the Certificate Enrollment Guide for the Cisco 1000 Series Connected Grid Routers.

Generating certificates for CG-NMS also involves generating and loading certificates on the CG-NMS TPS Proxy (tpsproxy). After generating the certificates, import them into the storage location on the TPS proxy and CG-NMS known as the Keystore.

Keystore

The Keystore provides details for a specific system (such as CG-NMS or the TPS proxy) and includes the following items:

- The certificate for that system (such as the CG-NMS certificate or TPS proxy certificate)
- The private key for the system
- The certificate chain (path to the CA or subCA)

The CG-NMS key and certificates are stored in the cgms_keystore file on the CG-NMS server in the /opt/cgms/server/cgms/conf directory.

Generating and Exporting Certificates

Note: The CG-NMS certificate encrypts data in the database. **Do not lose this certificate!** Loss of this certificate results in some database data that will not be able to be decrypted.

Complete the following procedures to generate and export certificates:

- Configuring a Certificate Template for CG-NMS and the CG-NMS TPS Proxy

- Enabling a Certificate Template

- Generating Certificates for CG-NMS and the CG-NMS TPS Proxy

- Command Authorization Support

- Exporting the CA Certificate

Configuring a Certificate Template for CG-NMS and the CG-NMS TPS Proxy

On the CA (or subCA) you must create certificate templates to generate certificates for the CG-NMS and TPS proxy.

To create a certificate template:

1. Open the Certificate Authority application on a Windows Server 2008 R2 system operating with the Enterprise edition.

The Certificate Authority application is standard on the above noted Windows Server version.

2. Expand the menu to view the Certificate Templates folder.

3. Right-click **Certificate Templates** and choose **Manage** from the context menu.

4. In the right-pane, right-click **Computer**, choose **Duplicate Template** from the context menu, and enter **NMS**.

5. In the Duplicate Template pane, select **Windows Server 2008 Enterprise**.

6. Click **OK**.

7. Click the **NMS Properties > General** tab, and do the following:

    a. Enter **NMS** in the **Template display name** and **Template name** fields.

    b. Enter an appropriate **Validity** period, which defines the lifetime of the certificate.

    c. Check the **Publish certificate in Active Directory** check box.

    d. Click **OK**.

8. Click the **NMS Properties > Extensions** tab, and do the following:

    a. Select **Application Policies** in the Extensions pane.

    b. In the Application Policies pane, verify that Client Authentication and Server Authentication appear in the bottom pane.

    c. Select **Key Usage** in the Extensions top pane and click **Edit**.

    d. In the **Edit Key Usage Extension** pane, clear the **Make this extension critical** check box.

    e. Click **OK**.

9. Click the **NMS Properties > Request Handling** tab, and do the following:

   a. Choose **Signature and encryption** from the Purpose drop-down menu.

   b. Check the **Allow private key to be exported** check box.

   c. Click **OK**.

10. Click the **NMS Properties > Security** tab, and do the following:

    a. Select **Administrator** within the Group or user names pane.

    b. For each group or user names item listed (such as authenticated users, administrator, domain administrators, enterprise administrators) check the **Allow** check box for all permissions (full control, read, write, enroll, autoenroll).

    c. Click **OK**.

11. Click the **NMS Properties > Cryptography** tab, and retain the following default settings:

   ■ Algorithm name: RSA

   ■ Minimum key site: 2048

   ■ Cryptographic provider: Requests can use any provider available on the subject computer

   ■ Request hash: SHA256

12. Click **OK**.

13. Click the **NMS Properties > Subject Name** tab, and retain the following default settings:

   ■ Radio button for **Supply in the request radio button** selected

   ■ Check box checked for **Use subject information from existing certificates for autoenrollment renewal requests**

14. Click **OK**.

Note: Retain the default settings for the remaining tabs: Superseded Templates, Server, and Issuance Requirements.

Enabling a Certificate Template

Before you can create a certificate, you must enable the certificate template.

To enable the certificate template:

1. Configure a certificate template (see Generating and Exporting Certificates).

2. Open the Certificate Authority application on the Windows Server.

3. Expand the menu to view the Certificate Templates folder.

4. Right-click **Certificate Templates** and choose **New > Certificate Template to Issue** from the context menu.

5. In the Enable Certificate Templates window, highlight the new **NMS** template.

6. Click **OK**.

Generating Certificates for CG-NMS and the CG-NMS TPS Proxy

Follow the same steps for generating a certificate for CG-NMS and for the TPS proxy by using the configuration template that you previously created.

Go through the steps in this section twice: once to generate the CG-NMS certificate, and once to generate the TPS proxy certificate.

Tip: In 9.b the value you enter is dependent on whether you are creating a certificate for the CG-NMS or the TPS proxy.

After creating these two certificates, securely transfer the CG-NMS certificate to the CG-NMS application server, and securely copy the TPS proxy certificate to the TPS proxy server.

To generate a certificate:

1. Configure a certificate template (see Generating and Exporting Certificates).

2. Enable the certificate template (see Enabling a Certificate Template).

3. From a server running Windows Server 2008, choose **Start > Run** and enter **mmc** to open the MMC console.

4. In the Console 1 window, expand the **Certificates > Personal** folders.

5. Right-click **Certificates** and choose **All Tasks > Request New Certificate** from the context menu.

6. In the Before You Begin window, click **Next**.

7. In the Select Certificate Enrollment Policy window, choose **Active Directory Enrollment Policy**.
   Click **Next**.

8. In the Request Certificates window, do the following:

   a. Check the **NMS** check box.

   b. Click the **More information**... link.

9. In the Certificate Properties window, click the **Subject** tab, and do the following:

   a. From the Type drop-down menu, choose **Common name (CN)**.

   b. In the **Value** field, add the fully-qualified domain name (FQDN):

   ■ For CG-NMS certificates, enter the FQDN of the CG-NMS server for your deployment, for example: CN=nms.sgbu.cisco.com.

   ■ For TPS proxy certificates, enter the FQDN for the TPS proxy for your deployment, for example: CN= tps.sgbu.cisco.com.

   c. Click **Add** and the Common Name appears in the right-pane.

   d. From the Type drop-down menu, choose **Organization (O)**.

   e. In the **Value** field, add the company name or organization for the CG-NMS or TPS proxy.

   f. Click **Add** and the organization appears in the right-pane.

Figure 1   Defining a Common Name and Organization for CG-NMS
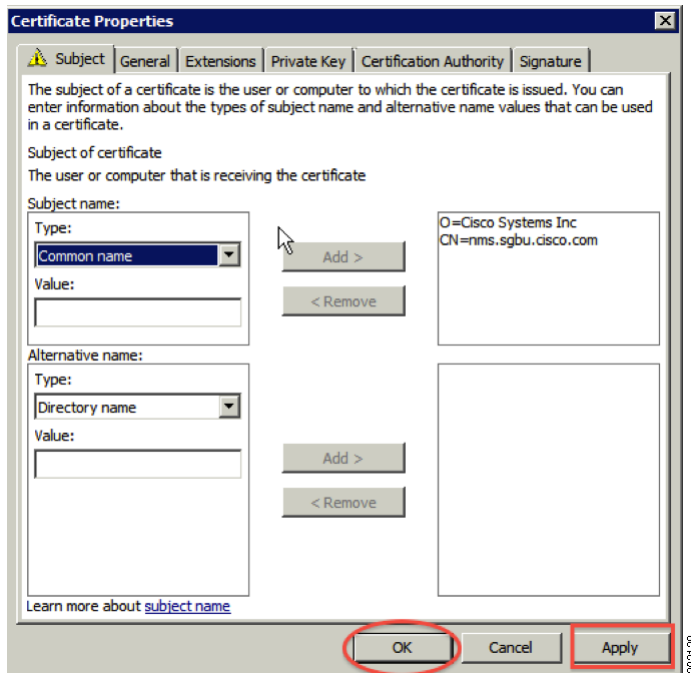
10. Click **Apply**. Click **OK**.

11. In the Certificate Enrollment window, check the **NMS** check box and click **Enroll**.

12. After enrollment completes, click **Finish**.

13. In the MMC console (Console 1), expand the **Certificates** folder.

14. Choose **Personal > Certificates**.

15. In the Issued To pane, right-click the new certificate and choose **All Tasks > Export** from the context menu.

The Export Wizard window displays.

Figure 2   Issued To Pane Showing Supported Certificates
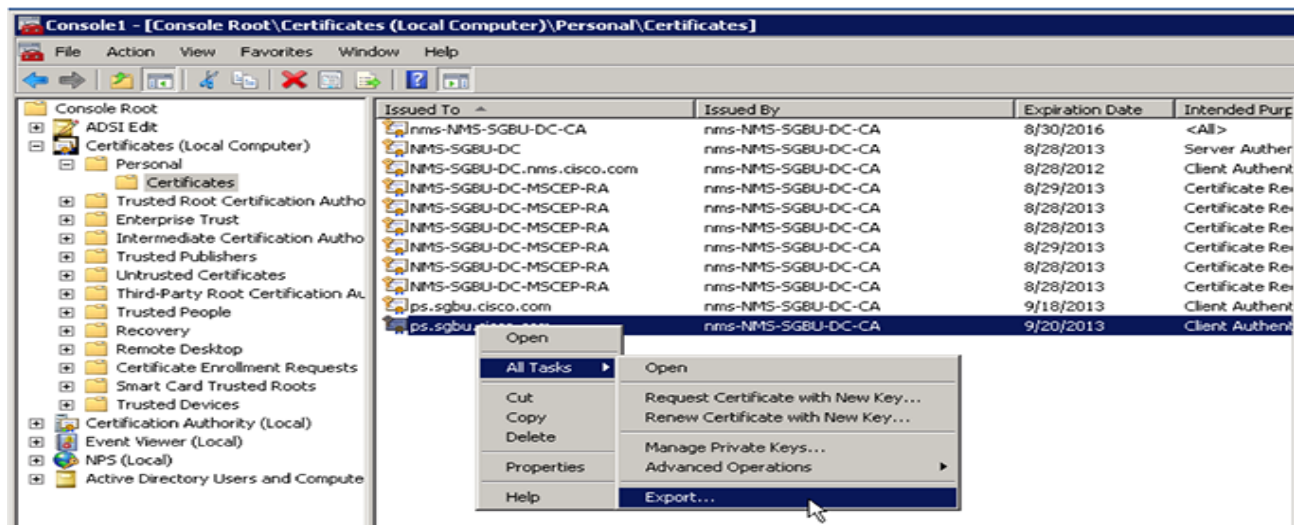
16. Initiate the Export Wizard.

17. At the Export Private Key window, select the **Yes, export the private key** radio button. Click **Next**.

18. At the Export File Format window, do the following:

   a. Click the **Personal Information Exchange** radio button.

   b. Check the **Include all certificates in the certification path if possible** check box.

   This option includes the full certificate chain within the certificate.

   c. Click **Next**.

19. In the password window, enter **keystore** and re-enter to confirm.

The password is the default password that the CG-NMS and the TPS proxy use to read this file.

20. Click **Next**.

21. In the File to Export window, enter the file name (such as *nms_cert* or *tps_cert*) and click **Next**.

22. In the Completing the Certificate Export Wizard, click **Finish**.

Files with a *.pfx extension are automatically saved to the Desktop. PFX refers to the Personal Information Exchange format, which is also known as PKCS_#12 format. PFX is an industry-standard format that allows certificates and their private keys to be transferred (exported) from one computer to another.

23. Securely transfer the two certificate files (such as *nms_cert.pfx* and *tps_cert.pfx*) from the Windows Desktop to the CG-NMS (*nms_cert.pfx*) and TPS proxy *(tps_cert.pfx)*, respectively.

Note: For heightened security, after a successful transfer delete the *.pfx files from the Windows Desktop and empty the Recycle bin.

Command Authorization Support

The Cisco Connected Grid Routers (CGRs) are managed by CG-NMS over a WAN backhaul connection such as 3G or WiMAX. For CG-OS CGRs, you define an OID value to enable administrative privileges fro CG-NMS.

The OID for this policy is 1.3.6.1.4.1.9.21.3.3.1. This element appears in the certificate if CG-NMS is authorized to issue management commands to the CGR with administrative privileges. CG-NMS communicates with the CGR over a secured session, such as TLS, the CGR can execute these commands as if they were issued by the network administrator.

This section discusses the following topics:

- Enabling Command Authorization Using NMS/TPS Certificates

- Adding an OID Value to the CA Certificate

- Renewing Certificates

Enabling Command Authorization Using NMS/TPS Certificates

Follow this procedure to authorize the command authorization (CA) feature of the router, and complete registration with CG-NMS.

1. Generate new NMS/TPS certificates (see Generating Certificates for CG-NMS and the CG-NMS TPS Proxy) or renew the existing NMS/TPS certificate (see Renewing Certificates).

2. Add an OID value to the CA certificate (see Adding an OID Value to the CA Certificate).

3. Generate a new .pfx file for the NMS/TPS certificate (see Generating Certificates for CG-NMS and the CG-NMS TPS Proxy).

4. Stop CG-NMS (see Stopping CG-NMS).

5. Rename the existing cgms_keystore file (for example, cgms_keystore_no_oid).

6. Export the .pfx file to CG-NMS and create a new cgms_keystore file (see Using Keytool to Create the cgms_keystore File).

7. Install the new certificates (see Installing the Certificates).

8. Add the new cgms_keystore file to CG-NMS (see Copying the cgms_keystore File to CG-NMS).

9. Start CG-NMS (see Starting CG-NMS).

10. Register the routers with CG-NMS.

Adding an OID Value to the CA Certificate

You must add an OID value to the CA certificate to allow CG-NMS to use the admin role for command authorization on the router.

To add an OID value to the CA certificate:

1. On the CA server, open a cmd console and type:

```
certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
```

2. Restart the CA.

3. In the Select Certificate Enrollment Policy window, choose **Active Directory Enrollment Policy** and click **Next**.

4. In the Request Certificates window, do the following:

   a. Check the **NMS** check box.

   b. Click the **More information**... link.

67

Generating and Exporting Certificates

5. In the Certificate Properties window, click the **Subject** tab complete the fields.

6. In the Certificate Properties window, click the **Extensions** tab and click the **Custom extension definition** button to expand the section.
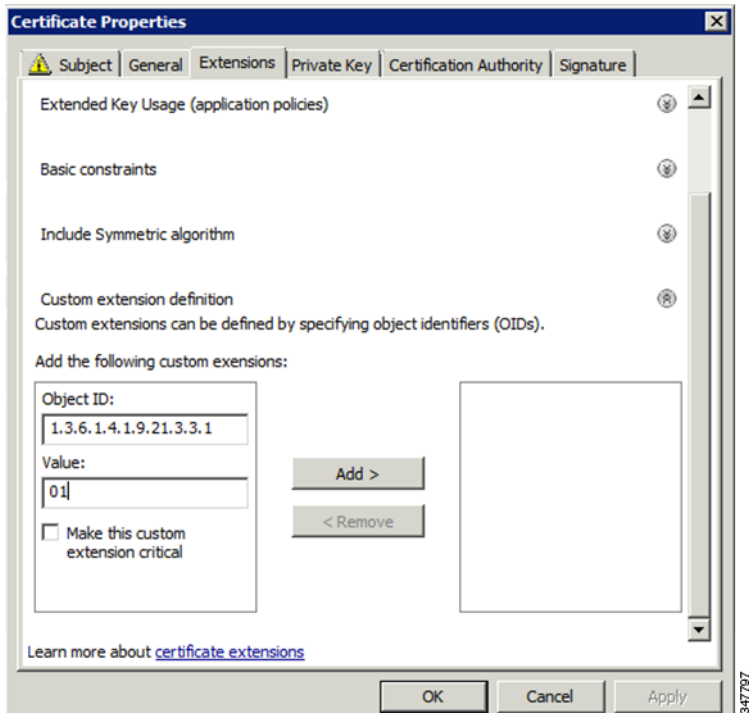
7. Type the following in the **Object ID** field:

`1.3.6.1.4.1.9.21.3.3.1`

8. In the **Value** field, type:

`01`

9. Click **Add**.
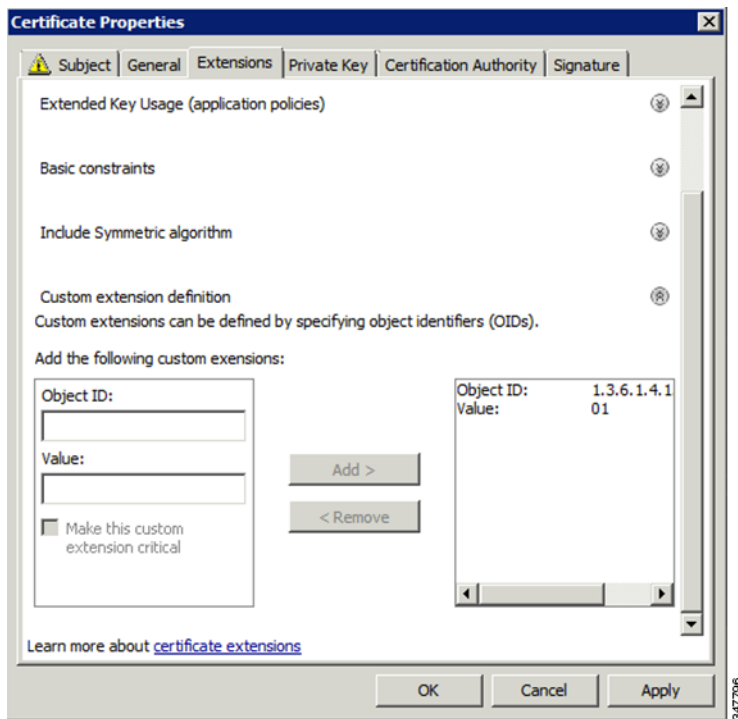
The OID and Value are added to the field at the right as custom extensions.

10. Ensure that these values are correct, and then click **Apply**.

Renewing Certificates

To renew certificates and add the OID value:

1. From the RSA CA server with the original NMS/TPS certificate, type the following open command at the command prompt:

```
certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
```

2. Restart the CA server.

3. Open the certificate console in the MMC.

4. Locate the issued NMS/TPS certificate in the Personal folder on the CA server.

5. Right-click on the server icon, and select **All Tasks > Advanced Operations > Renew This Certificate with the Same Key** option from the context menu.

69
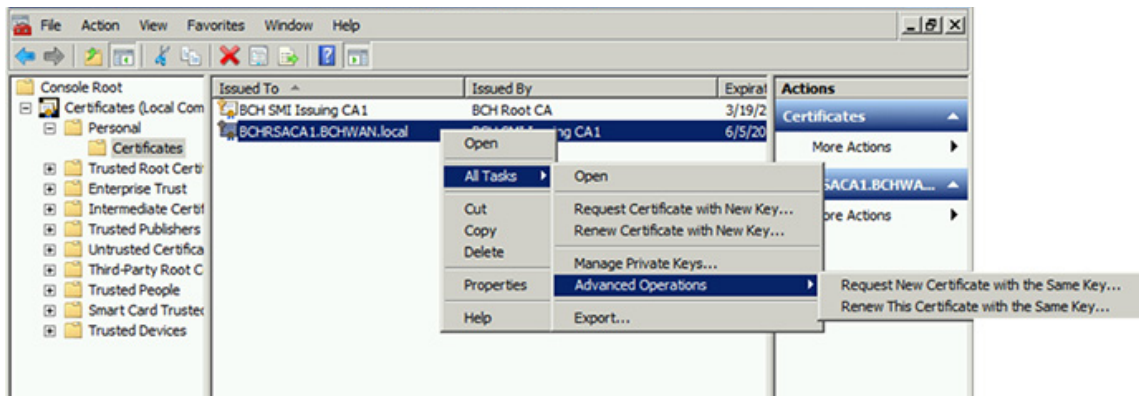
6. In the Certificate Enrollment window, click **Next**.

7. Click **Details**.
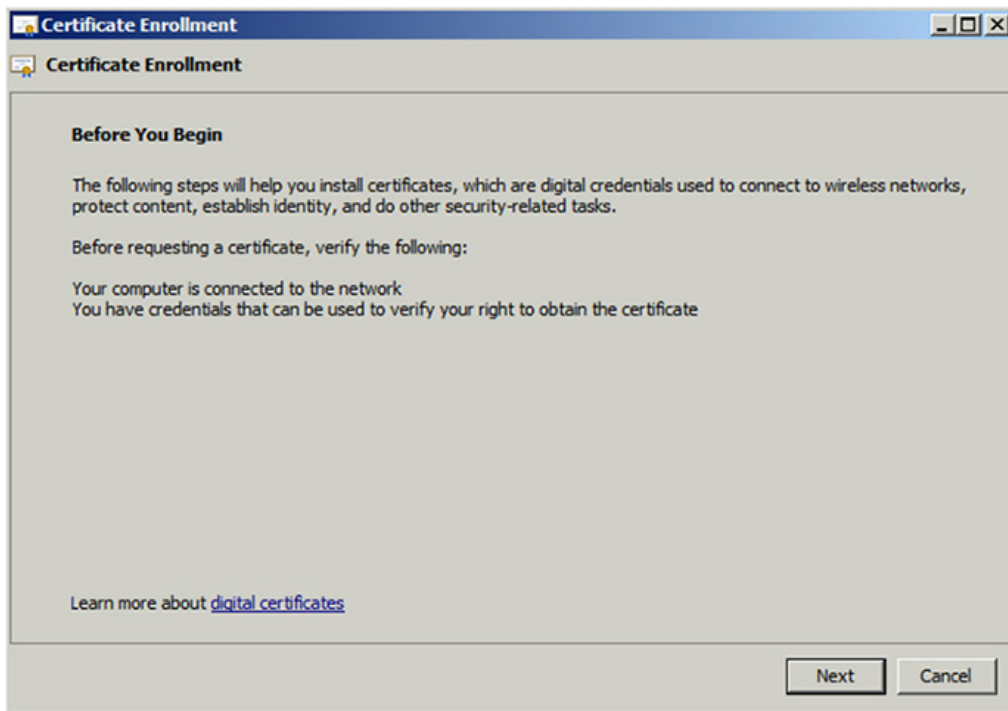
Generating and Exporting Certificates
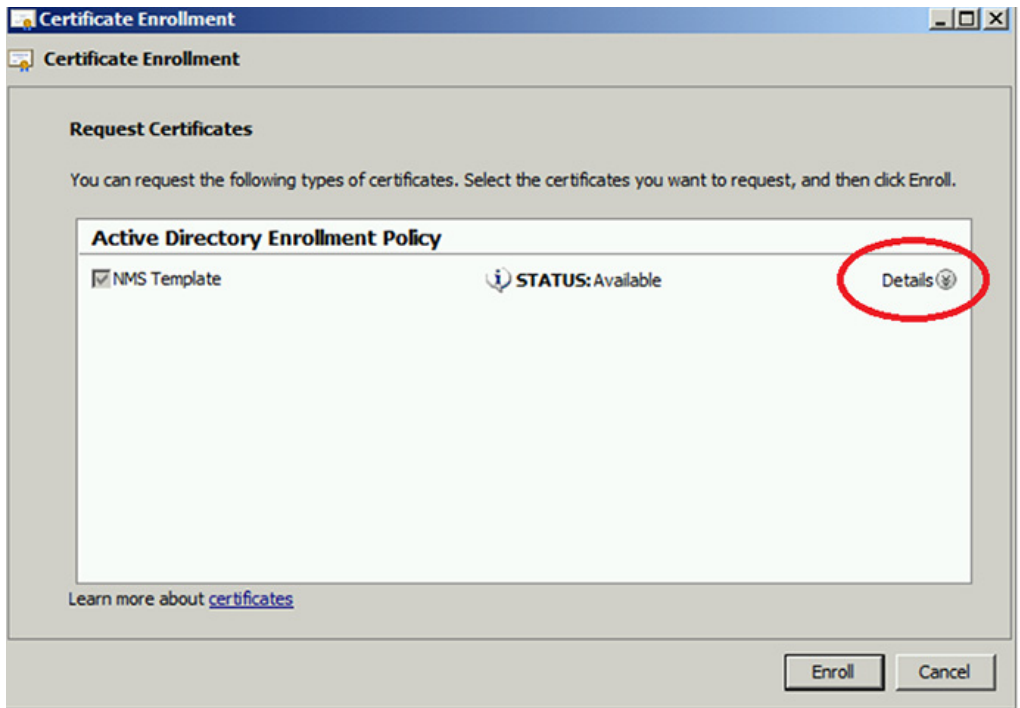
8. Click **Properties**.
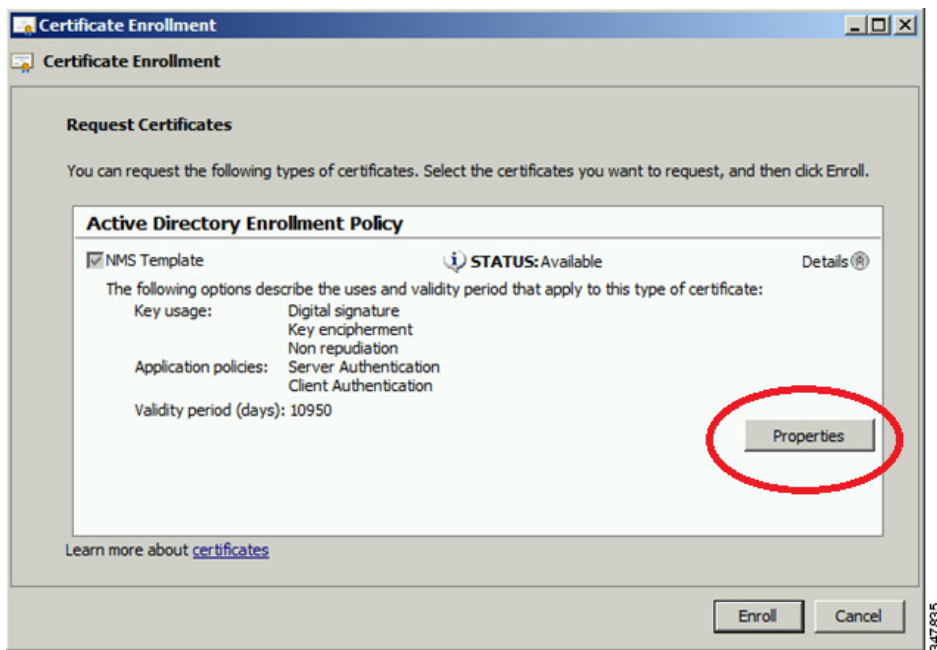
9. Enter the OID and its value, and click **OK**.
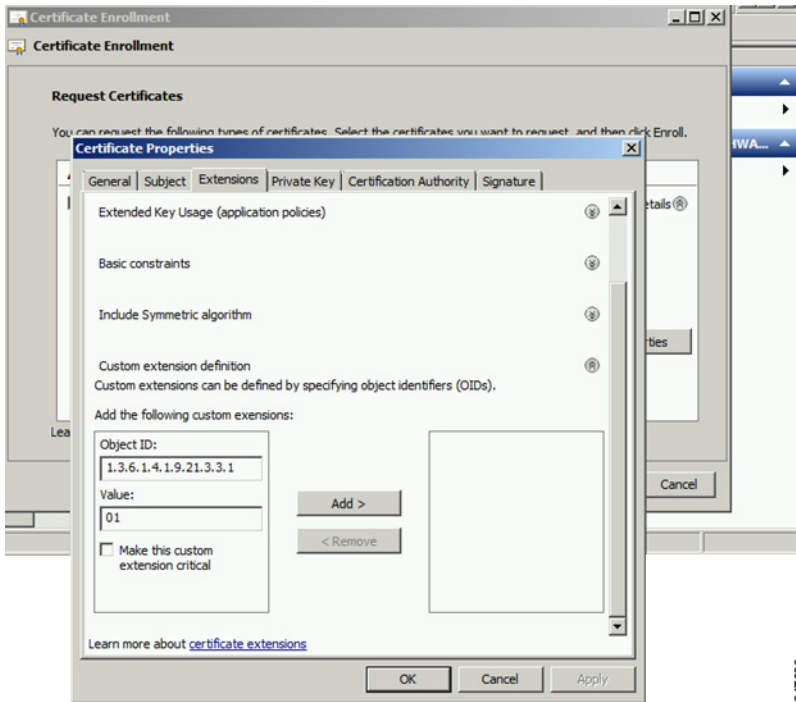
10. Click **Add >**, and then click **OK**.
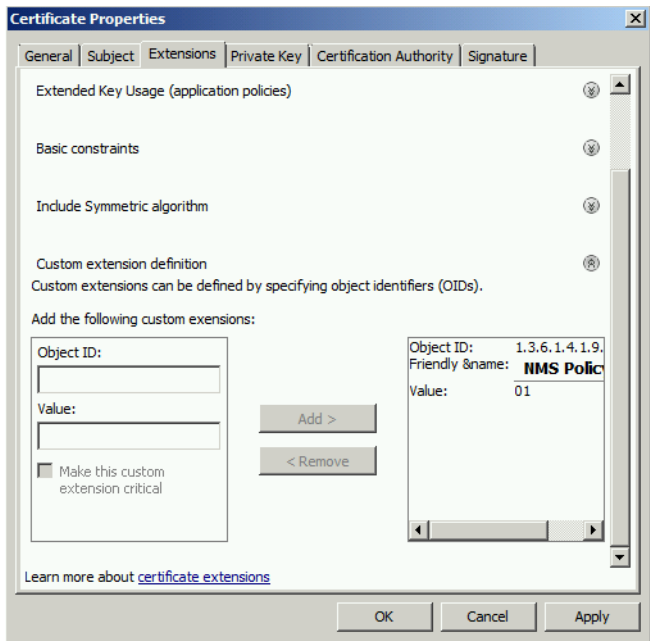
11. Click **Enroll**.
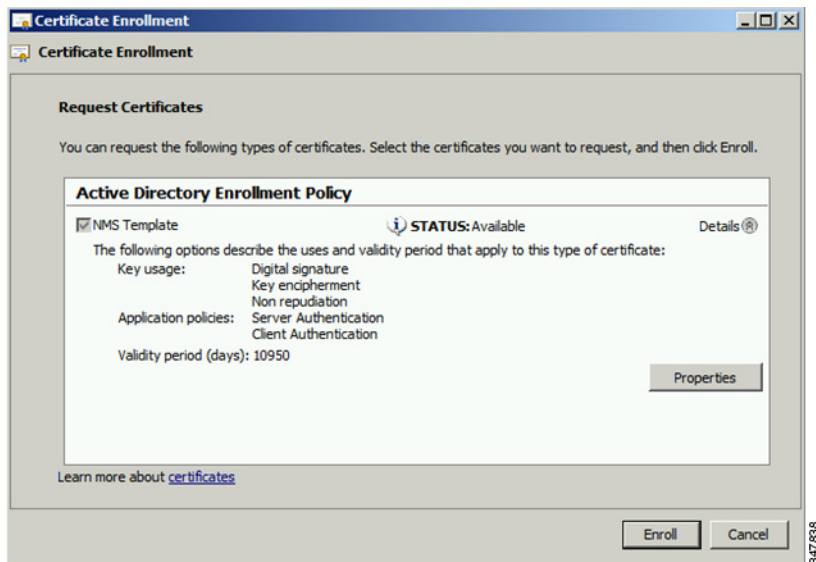
12. Click **Finish**.
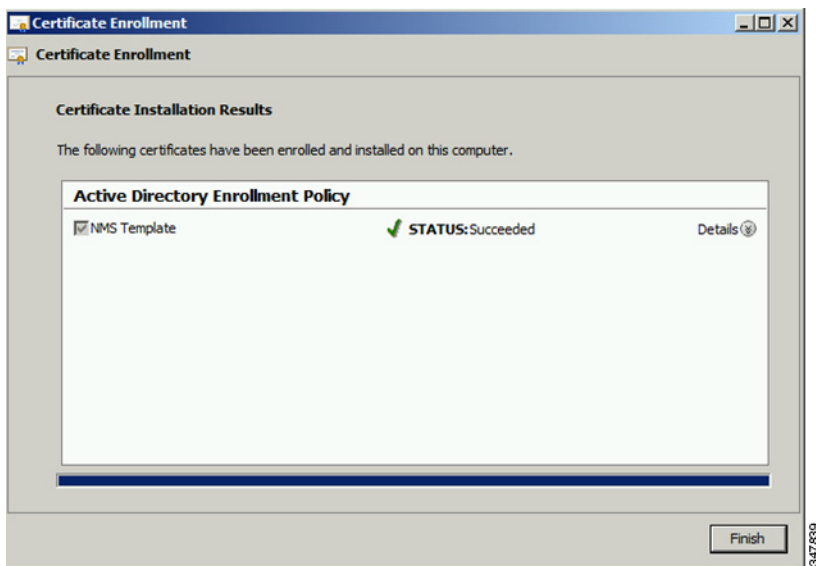
13. Verify that the certificate contains the OID value.

Exporting the CA Certificate

To export the certificate from the Certificate Authority or subordinate CA to the CG-NMS:

1. Open the Certificate Authority application on a Windows Server 2008 R2 system operating with the Enterprise Edition.

2. Expand the menu to view the **Certificates (Local Computer) > Personal > Certificates** folder.

3. Locate the certificate whose fingerprint matches that in use by the Cisco CGR 1000 and Cisco ASR.

4. Right-click the certificate and choose **All Tasks > Export** from the context menu.

5. In the Certificate Export Wizard window, click **Next**.

6. In the Export Private Key window, select the **No, do not export the private key** radio button. Click **Next**.

7. In the Export File Format window, select the **Base-64 encoded X.509 (.CER)** radio button. Click **Next**.

8. In the File to Export window, assign a name for the file that you want to export. Click **Next**.

9. In the File to Export window, enter the file name (such as *ca_cert* or *subca_cert*) and click **Next**.

10. In the Completing the Certificate Export Wizard, click **Finish**.

Files with a *.cer extension are automatically saved to the Desktop.

11. Securely transfer the certificate file (such as *ca_cert.cer*) from the Windows Desktop to CG-NMS.

Note: For heightened security, after a successful transfer delete the *.cer file from the Windows Desktop and empty the Recycle bin.

Installing the Certificates

You must create a cgms_keystore file on both the servers running CG-NMS and CG-NMS TPS Proxy.

- **CG-NMS**—When creating the cgms_keystore file, you import the CG-NMS certificate, its private key, and the certificate chain. After creating the cgms_keystore file, you copy it into a specific directory on the server.

- **CG-NMS TPS Proxy**—When you create the cgms_keystore file, you import the CG-NMS TPS Proxy certificate, its private key, and the certificate chain. After you create the cgms_keystore file, you copy it into a specific directory on the TPS proxy.

To create the cgms_keystore file for the TPS proxy and CG-NMS, use Keytool and complete the following procedures:

- Before You Begin

- Using Keytool to Create the cgms_keystore File

- Copying the cgms_keystore File to CG-NMS

Before You Begin

Before using Keytool to create the cgms_keystore file, determine the password to use for the keystore. In examples, this chapter refers to this password as *keystore_password*.

Using Keytool to Create the cgms_keystore File

To create the cgms_keystore file for both CG-NMS and the TPS proxy:

1. As root, view the contents of the .pfx file by entering the following command on the server (CG-NMS and TPS proxy):

[root@*tps_server* **~]# keytool**

Note: Viewing the .pfx provides the Alias Name required during the import.

2. Enter the keystore password when prompted.

This is the same password entered when creating the .pfx file.

The information that displays (see the following Example) includes the alias_name needed for 3..

3. Enter the following command to import the certificates into the cgms_keystore file:

keytool -importkeystore -v -srckeystore *filename.pfx* **-srcstoretype pkcs12 -destkeystore cgms_keystore -deststoretype jks -srcalias** *alias_name* **-destalias cgms -destkeypass** *keystore_password*

4. Enter the destination keystore password when prompted.

5. Re-enter the keystore password when prompted.

6. Enter the password used when creating the .pfx file (either *nms_cert.pfx* or *tps_cert.pfx*) when prompted for the source keystore password.

Note: In this example, **keystore** was the password when we created the *.pfx* file.

Example

To view the *nms_cert.pfx* file and access the Alias name, enter the following commands as root:

Note: This example shows the steps for the *nms_cert.pfx*. To view the details on the *tps_cert.pfx* and import the certificates to the TPS proxy, use the same commands but replace the references to *nms_cert.pfx* with *tps_cert.pfx*, and use the Alias name from the *tps_cert.pfx* file.

```
# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12
Enter keystore password: keystore
Keystore type: PKCS12
Keystone provider: SunJSSE
Your keystore contains 1 entry
Alias name: le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b
Creation date: March 29.2012
Entry type: PrivateKey Entry
Certificate chain length: 3
Certificate[1]:
Owner: CN=nms.sgbu.cisco.com
Issuer: CN=cisco-RSA-SUBCA-CA, DC=cisco, DC=com
...
```

To import the certificates to the **cgms_keystore** file on the CG-NMS, enter the following commands as root:

```
# keytool -importkeystore -v -srckeystore nms_cert.pfx -srcstoretype pkcs12 -destkeystore cgms_keystore
-deststoretype jks -srcalias le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b -destalias cgms -destkeypass
keystore_password

Enter destination keystore password: keystore_password
Re-enter new password: keystore_password
Enter source keystore password: keystore
...Storing cgms_keystore
```

Note: The **storing** *cgms*_**keystore** text indicates successful completion.

Copying the cgms_keystore File to CG-NMS

To copy the **cgms_keystore** file into the following CG-NMS and TPS proxy directories:

1. For CG-NMS, copy the cgms_keystore file to this directory: **/opt/cgms/server/cgms/conf/**

2. For the TPS proxy, copy the cgms_keystore file to this directory: **/opt/cgms-tpsproxy/conf/**

Note: For these certificates to be active and enforceable, they must be in the correct directory.

Importing the CA Certificate

In addition to importing the NMS certificate, you must import the CA or (subCA) certificate to the cgms_keystore.

To import the CA certificate into the cgms_keystore:

1. On the CG-NMS application server, log in as root.

2. Change directory to /opt/cgms/server/cgms/conf, where you have placed the cgms_keystore file:

cd /opt/cgms/server/cgms/conf

3. Import the CA certificate:

keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer

A script displays on the screen.

4. Enter the keystore password when prompted.

5. Re-enter the password.

6. Enter **yes** when prompted to trust the certificate.

The certificate is added to the Keystore.

Example

To import the CA certificate, enter the following commands as root:

```
# keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer
Enter keystore password: keystore_password
Owner:  CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Issuer: CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Serial number:50adbd57e6b136984f9c1512a0eb7174
Valid from: Wed Jan 11 10:58:09 PDT 2012 until: Wed Jan 11:08:59 PDT 2016
Certificate _fingerprints:
    MD5: AE:5D:F4:0A:2B:E5:C8:D8:4A:F4:18:56:FD:A7:8D:7D
    SHA1: 83:22:12:8C:6A:23:D3:08:2B:00:55:EF:BD:FF:BA:47:97:99:7E:41
    Signature algorithm name: SHA1withRSA
    Version:3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
#2:ObjectId: 2.5.29.15 Criticality=false
KeyUsage[
DigitalSignature
Key_CertSign
Crl_Sign
]
#3:ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000:C6 AB 38 CC EE 79 B0 51 3B 4D 13 c8 9A 56 F6 73 ..8..y.Q;M...V.s
0010:B9 19 FF 7B                                ....
]
]
#4: ObjectId:1.3.6.1.4.1.311.21.1 Criticality=false
Trust this certificate [no] yes
Certificate was added to the keystore.
```

Importing the CA Certificate into the CG-NMS TPS Proxy Keystore

Follow the same steps as in Importing the CA Certificate to import the CA certificate into cgms_keystore on the CG-NMS TPS proxy.

Configuring CG-NMS to Access the Keystore

After you create cgms_keystore and import the NMS and CA certificates to it, configure CG-NMS to access the cgms_keystore file.

To set the keystore password:

1. Stop CG-NMS.

2. Run the setupCgms.sh script:

```
pwd
/opt/cgms/bin
./setupCgms.sh
06-12-2012 10:21:39 PDT: INFO: ========== CG-NMS Setup Started - 2012-06-12-10-21-39 =====
06-12-2012 10:21:39 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log
Are you sure you want to setup CG-NMS (y/n)? y
06-12-2012 10:21:39 PDT: INFO: User response: y
...
Do you want to change the keystore password (y/n)? y
06-12-2012 10:21:52 PDT: INFO: User response: y
Enter keystore password: keystore_password
Re-enter keystore password: keystore_password
06-12-2012 10:21:59 PDT: INFO: Configuring keystore password. This may take a while. Please wait ...
06-12-2012 10:22:00 PDT: INFO: Keystore password configured.
...
```
This script saves the password set in the cgms.properties file.

3. Start CG-NMS.

Tip: To protect the cgms_keystore and cgms.properties files, set their permissions to root read only.

Caution: Protect your system! Ensure that only root has access to the CG-NMS server. Your firewall should only allow SSH access from internal hosts.

Configuring the TPS Proxy to Access the Keystore

To configure the TPS proxy to access the keystore:

1. Change to the tpsproxy bin directory:

```
cd /opt/cgms-tpsproxy/bin
```

2. Convert your chosen password into encrypted form:

```
./encryptionUtil.sh {your chosen password for cgms_keystore}
7jlXPniVpMvat+TrDWqh1w==
```

3. Copy the encrypted password into the tpsproxy.properties file:

   a. Open the file for editing.

   ```
   cd /opt/cgms-tpsproxy/conf
   emacs tpsproxy.properties
   ```

    b. Add this line to the file:

```
cgms-keystore-password-hidden=keystore_password
```

    In this example, the encrypted *keystore_password* is "7jlXPniVpMvat+TrDWqh1w==".

  4. Restart TPS proxy:

```
service tpsproxy restart
```

Setting Up an HSM Client

Complete the following procedures to set up the HSM client:

- Installing an HSM Client on the CG-NMS Server

- Configuring an HSM HA Client

Note: If your installation uses SSM for CSMP-based messaging, see Installing and Setting Up the SSM.

Installing an HSM Client on the CG-NMS Server

The Hardware Security Module (HSM) works as a security server listening at port 1792. For CG-NMS to communicate with HSM:

  1. Install an HSM client on the CG-NMS server.

  2. Configure the HSM client to have the certificate for HSM.

  3. Upload the certificate to HSM.

This section describes how to install and configure an HSM client, assuming that HSM is at 172.16.0.1 and the client at 172.31.255.254.

To install and set up an HSM client:

  1. Get the HSM client package, unpack it, and run the installation script:

sh install.sh

  2. Change to the /usr/lunasa/bin directory:

```
cd /usr/lunasa/bin
```

  3. Create the client certificate:

```
./vtl createCert -n ip_address_of_hsm_client
```

  4. Download the HSM certificate from the HSM server:

scp admin@*ip_address_of_hsm_server***:server.pem .**

  5. Upload the client certificate to the HSM server:

```
scp ../cert/client/ip_address_of_hsm_client.pem admin@ip_address_of_hsm_server: .
```

  6. Load the HSM certificate:

```
vtl addServer -n ip_address_of_hsm_server -c server.pem .
```

  7. Ensure that the HSM server is added:

78

```
vtl listServer
```

8. From the HSM client, use SSH to log in to the HSM server:

```
ssh admin@ip_address_of_hsm_server
Last login: Mon Aug 15 15:36:43 2012 from 10.27.164.171
Luna SA 5.0.1-2 Command Line Shell - Copyright (c) 2001-2010 SafeNet, Inc. All rights reserved.
[TestLunaSA1] lunash:>
```

9. Use SSH to perform these steps on the HSM server:

   a. Add the client to the HSM server:

```
[TestLunaSA1] lunash:>client register -c hsm_client_name -i ip_address_of_hsm_client
'client register' successful.    Command Result : 0 (Success)
```

   b. List the clients defined on the server and ensure that the client was added:

```
[TestLunaSA1] lunash:>client list
registered client 1: cg-nms
registered client 2: hsm_client_name
Command Result : 0 (Success)
```

   c. Assign the client to a partition:

```
[TestLunaSA1] lunash:>client assignPartition -c hsm_client_name -p partition_name
'client assignPartition' successful.
Command Result : 0 (Success)
```

   d. Log out of HSM.

10. On the server running the HSM client, verify the HSM client installation:

```
vtl verify
The following Luna SA Slots/Partitions were found:
Slot    Serial #    Label
====    ========    =====
1    151285008    TestPart1
```

11. After the HSM client installation completes, run the test suite ckdemo.

ckdemo
```
Ckdemo is the property of SafeNet Inc and is provided to our customers for
diagnostic and development purposes only.  It is not intended for use in
production installations.  Any re-distribution of this program in whole or
in part is a violation of the license agreement.

CrystokiConnect()           (modified on Oct 18 2012 at 20:57:53)

*** CHRYSTOKI DEMO - SIMULATION LAB ***


Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
     ( 1) Open Session  ( 2) Close Session  ( 3) Login
     ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
     ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
     (10) Get Info      (11) Slot Info      (12) Token Info
     (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                        (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
     (20) Create object (21) Copy object    (22) Destroy object
```

```
         (23) Object size    (24) Get attribute  (25) Set attribute
                             (26) Find object     (27) Display Object
SECURITY FUNCTIONS
     (40)   Encrypt file (41) Decrypt file   (42)  Sign
     (43)   Verify       (44) Hash file       (45)  Simple Generate Key
                                              (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
     (50) HA Init        (51) HA Login
KEY FUNCTIONS
     (60) Wrap key       (61) Unwrap key      (62) Generate random number
     (63) Derive Key     (64) PBE Key Gen     (65) Create known keys
     (66) Seed RNG       (67) EC User Defined Curves
CA FUNCTIONS
     (70) Set Domain     (71) Clone Key       (72) Set MofN
     (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
     (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
     (79) Modify MofN    (86) Dup. MofN Keys (87) Deactivate MofN
     (88) Get Token Certificates      (112) Set Legacy Cloning Domain
OTHERS
     (90) Self Test
     (94) Open Access    (95) Close Access
     (97) Set App ID     (98) Options        (100) LKM Commands
OFFBOARD KEY STORAGE:
     (101) Extract Masked Object          (102) Insert Masked Object
     (103) Multisign With Value           (104) Clone Object
     (105) SIMExtract                     (106) SIMInsert
     (107) SimMultiSign                   (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
     (108) Execute Script                 (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
     (111) Get Cluster State
SRK FUNCTIONS:
     (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
     (203) SRK Zeroize    (204) SRK Enable/Disable


     (  0) Quit demo

Enter your choice : 1

Slots available:
     slot#1 - LunaNet Slot
     slot#2 - Luna UHD Slot
     slot#3 - Luna UHD Slot
     slot#4 - Luna UHD Slot
Select a slot: 1

SO[0] or normal user[1]?

You must enter a number between 0 and 1: 1

Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
     ( 1) Open Session  ( 2) Close Session  ( 3) Login
     ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
     ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
     (10) Get Info      (11) Slot Info      (12) Token Info
     (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                        (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
     (20) Create object (21) Copy object    (22) Destroy object
     (23) Object size   (24) Get attribute  (25) Set attribute
                        (26) Find object    (27) Display Object
```

```
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options       (100) LKM Commands
OFFBOARD KEY STORAGE:
    (101) Extract Masked Object            (102) Insert Masked Object
    (103) Multisign With Value             (104) Clone Object
    (105) SIMExtract                       (106) SIMInsert
    (107) SimMultiSign                     (118) Extract Object
                                           (119) Insert Object

SCRIPT EXECUTION:
    (108) Execute Script                   (109) Execute Asynchronous Script
                                           (110) Execute Single Part Script

CLUSTER EXECUTION:
    (111) Get Cluster State
SRK FUNCTIONS:
    (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
    (203) SRK Zeroize    (204) SRK Enable/Disable

    (  0) Quit demo

Enter your choice : 3
Security Officer[0]
Crypto-Officer  [1]
Crypto-User     [2]: 1
Enter PIN           : 9JT5-WMYG-E5FE-TExs

Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
```

```
    (60) Wrap key       (61) Unwrap key      (62) Generate random number
    (63) Derive Key     (64) PBE Key Gen     (65) Create known keys
    (66) Seed RNG       (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain     (71) Clone Key       (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN    (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options       (100) LKM Commands
OFFBOARD KEY STORAGE:
    (101) Extract Masked Object        (102) Insert Masked Object
    (103) Multisign With Value         (104) Clone Object
    (105) SIMExtract                   (106) SIMInsert
    (107) SimMultiSign                 (118) Extract Object
                                       (119) Insert Object
SCRIPT EXECUTION:
    (108) Execute Script               (109) Execute Asynchronous Script
                                       (110) Execute Single Part Script
CLUSTER EXECUTION:
    (111) Get Cluster State
SRK FUNCTIONS:
    (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
    (203) SRK Zeroize    (204) SRK Enable/Disable

    (  0) Quit demo

Enter your choice : 27

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000: -1

No objects found

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000: 0
ERROR: Can not find object with handle 0

Status: C_GetObjectSize returned error. (CKR_OBJECT_HANDLE_INVALID)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
```

```
    (50) HA Init        (51) HA Login
KEY FUNCTIONS
    (60) Wrap key       (61) Unwrap key     (62) Generate random number
    (63) Derive Key     (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG       (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain     (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN    (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options       (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object          (102) Insert Masked Object
   (103) Multisign With Value           (104) Clone Object
   (105) SIMExtract                     (106) SIMInsert
   (107) SimMultiSign                   (118) Extract Object
                                        (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                 (109) Execute Asynchronous Script
                                        (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 0

Exiting GESC SIMULATION LAB
```

Configuring an HSM HA Client

Note: You must perform the steps in this section even if you only have one HSM server. You must also create a group that contains the HSM server.

To configure an HSM HA client:

1. Configure the HSM client so that it connects with both HSM servers, as described in Installing an HSM Client on the CG-NMS Server.

2. Change to the /usr/lunasa/bin directory:

```
cd /usr/lunasa/bin
```

3. Create a group that contains only the partition of the first HSM server by running this command and providing the serial number (*serial_num*) of the HSM server obtained by running the **./vtl verify** command (10.), the name of the group (*group_name*), and the password (*prtn_password*) for accessing the partition:

./vtl haAdmin -newGroup -serialNum *serial_num* **-label** *group_name* **-password** *prtn_password*

For example:

```
./vtl haAdmin -newGroup -serialNum 151285008 -label testGroup1 -password TestPart1

Warning:  There are 2 objects currently on the new member.
```

```
            Do you wish to propagate these objects within the HA
            group, or remove them?

            Type 'copy' to keep and propagate the existing
            objects, 'remove' to remove them before continuing,
            or 'quit' to stop adding this new group member.
            > copy


New group with label "testGroup1" created at group number 1151285008.
Group configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008
                    Needs sync:  no
```

4. Add the partition of the second HSM to the group.

For example:

```
./vtl haAdmin -addMember -group testGroup1 -serialNum 151268008 -password TestPart1
Member 151268008 successfully added to group testGroup1. New group
configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008, 151268008
                    Needs sync:  yes


Please use the command 'vtl haAdmin -synchronize' when
you are ready to replicate data between all members of the
HA group. (If you have additional members to add, you may
wish to wait until you have added them before synchronizing
to save time by avoiding multiple synchronizations.)
```

5. Verify that both partitions can be listed:

```
./vtl haAdmin -listGroups


If you would like to see synchronization data for group testGroup1,
please enter the password for the group members. (Press enter to
skip the synchronization check):
> *********

                  HA Group Label:  testGroup1
                 HA Group Number:  1151285008
                 Synchronization:  enabled
                   Group Members:  151285008, 151268008
                      Needs sync:  yes

              HA auto recovery:  disabled
                    HA logging:  disabled
```

6. Enable HA auto recovery:

```
[root@localhost bin]# ./vtl haAdmin -autoRecovery

vtl haAdmin -autoRecovery [ -retry <count> | -interval <seconds> ] -retry <retry count> -interval
<seconds>
```

- Set the **retry** value between -1 and 500 where, -1 is an infinite number of retries and 0 disables auto recovery.

- Specify the auto recovery poll **interval** in seconds.

   7. Enable HA.

```
./vtl haAdmin -HAOnly -enable
```

Configuring the HSM Group Name and Password

The HSM Group name and password is provided by Cisco at manufacture.

To allow the HSM Group name and password to be configured by the user:

   1. Edit the **cgms.properties** file to add the following properties:

- hsm-keystore-name *<name>*

- hsm-keystore-password *<encrypted password>*

Tip: You can use the same HSM server for multiple CG-NMS installations by creating multiple partitions on the HSM server, configuring the HSM client, and specifying the partition name and partition password in the cgms.properties file.

   2. Save the cgms.properties file.

   3. To apply these changes, restart CG-NMS:

```
service cgms start
```

Configuring the HSM Group Name and Password

Managing User Access

This chapter has the following topics for managing users and roles in CG-NMS:

- Managing the Password Policy

- Configuring Remote Authentication

- Managing Roles

- Managing Users

All user management actions are accessed through the **Admin > Access Management** menu (Figure 1).

Figure 1   Admin Menu

Managing the Password Policy

CG-NMS provides default password policy values that you can enforce among CG-NMS users.

Note: To modify these values, you must be logged in either as root or as a user with Administrative Operations permissions.

Caution: In some cases, changing password policies immediately terminates all user sessions and resets all passwords.

Note: The "Password history size" and "Max unsuccessful login attempts" policies do not apply to CG-NMS North Bound API users.

These changes *invalidate* all user sessions and expire their passwords (including the root user):

- When you increase the minimum length of passwords

- When you decrease the password expiry interval

- When you enable "**Password cannot contain username or reverse of username**"

87

- When you enable **"Password cannot be cisco or ocsic (cisco reversed)"**

- When you enable **"No character can be repeated more than three times consecutively in the password"**

- When you enable **"Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)"**

To edit password policies:

1. Choose **Admin > Access Management > Password Policy**.

2. To enable or disable a policy, choose the appropriate option (**Enabled** or **Disabled**) from the Status drop-down menu.

3. To modify the value of a policy, if applicable, enter the new value in the Value field.

   Note: CG-NMS supports a maximum password length of 32 characters.

4. Click **Save** to start enforcing the new policies.

   Note: The password policy you configure in CG-NMS applies only to local users and not to remote Active Directory (AD) users. The password policy for AD users is determined and enforced by the AD admin.

Configuring Remote Authentication

To configure remote authentication for CG-NMS, you need to perform configurations steps in Active Directory (AD) and CG-NMS.

- Support for Remote Authentication

- Configuring Remote Authentication in AD

- Configuring Security Policies on the RADIUS Server

- Configuring Remote Authentication in CG-NMS

- Enabling and Disabling Remote User Accounts

- Deleting Remote User Accounts

- Logging In to CG-NMS Using a Remote User Account

Support for Remote Authentication

With Remote Authentication, it is easier to integrate CG-NMS into an existing AD and Network Policy Server (NPS) infrastructure. This allows administrators to configure CG-NMS access for users in AD.

When you configure remote authentication in CG-NMS, it hands over the authentication and authorization responsibility to AD and NPS. AD performs user authentication to check the validity of user credentials. The RADIUS server performs user authorization to check whether a user belongs to a group that defines the user role. If so, the server returns the role name to CG-NMS.

CG-NMS   RADIUS   Active
Server   Server   Directory
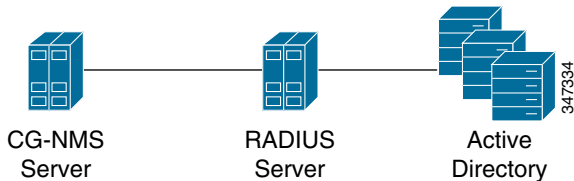
The following is the flow of user authentication and authorization by AD and NPS:

1. The user enters their credentials.

   ■ If user was created locally on the NMS server, authentication and authorization occurs locally.

   ■ If CG-NMS determines that the user is a remote user, authentication and authorization occurs on the configured RADIUS server.

   ■ If remote authentication is not configured, authentication fails and user is denied access.

2. For remote users, if authentication and authorization are successful, the assigned user role returns to the NMS server from the RADIUS server.

3. If the role that returns is valid, the user is granted access.

   Note: When remote authentication is enabled, user management is done in AD. If an AD user logs in who was deleted from CG-NMS, their profile is added back to CG-NMS. To prevent access to CG-NMS, their AD user profiles must first be deleted from AD.

Configuring Remote Authentication in AD

To configure AD to allow CG-NMS to remotely authenticate users:

1. Log in to NPS.

2. Add CG-NMS as a radius client on the RADIUS server.

   Provide a friendly name, and IP address or DNS name of the CG-NMS server and configure the shared secret that CG-NMS uses to connect to the RADIUS server.

Configuring Remote Authentication
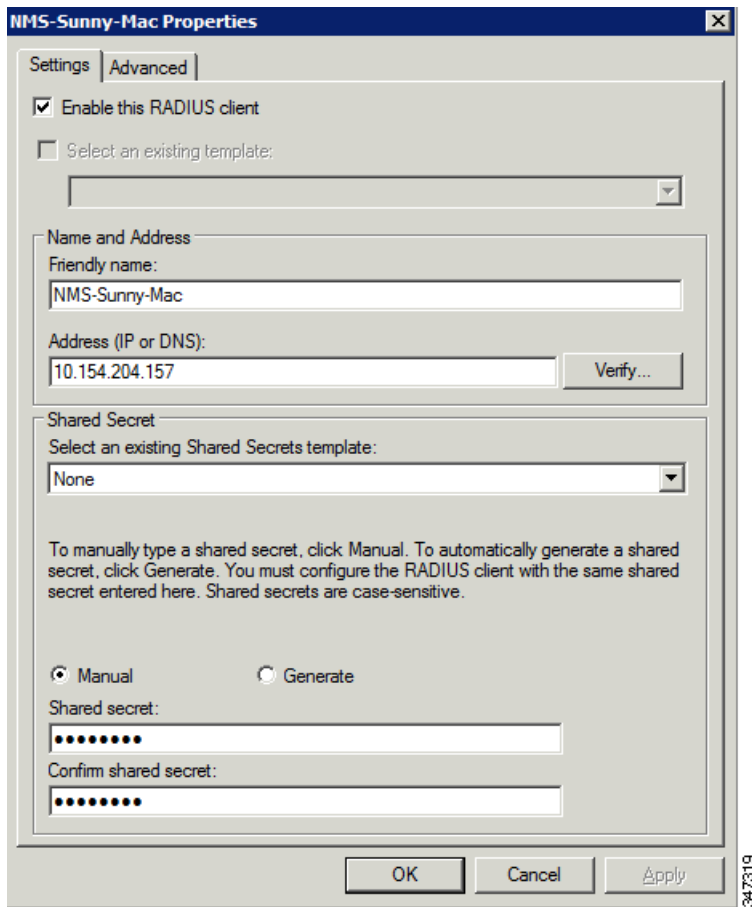
An entry for the RADIUS client appears under RADIUS Clients and Servers.
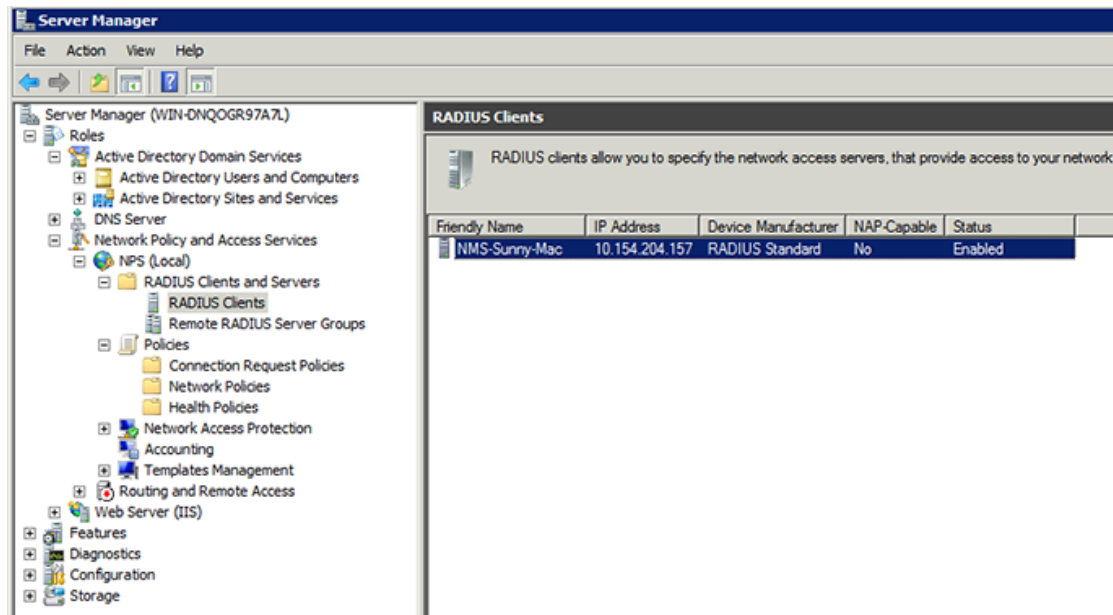
3. Log in to AD and create an organizational unit.

Cisco recommends that you create all security groups (CG-NMS roles) within this organizational unit.

Configuring Remote Authentication
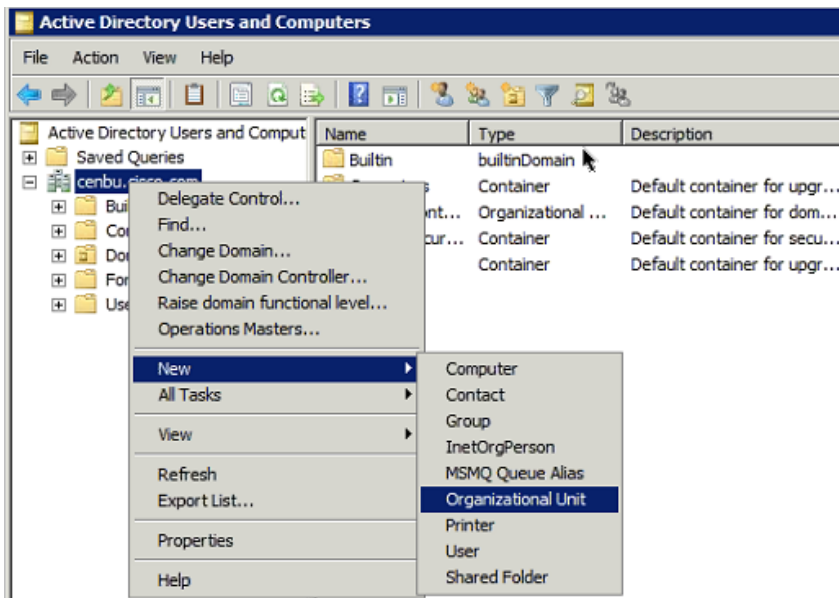
4. Add security groups corresponding to CG-NMS roles to the organizational unit.

The following example shows the security groups defined in the NMS_ROLES organizational unit.
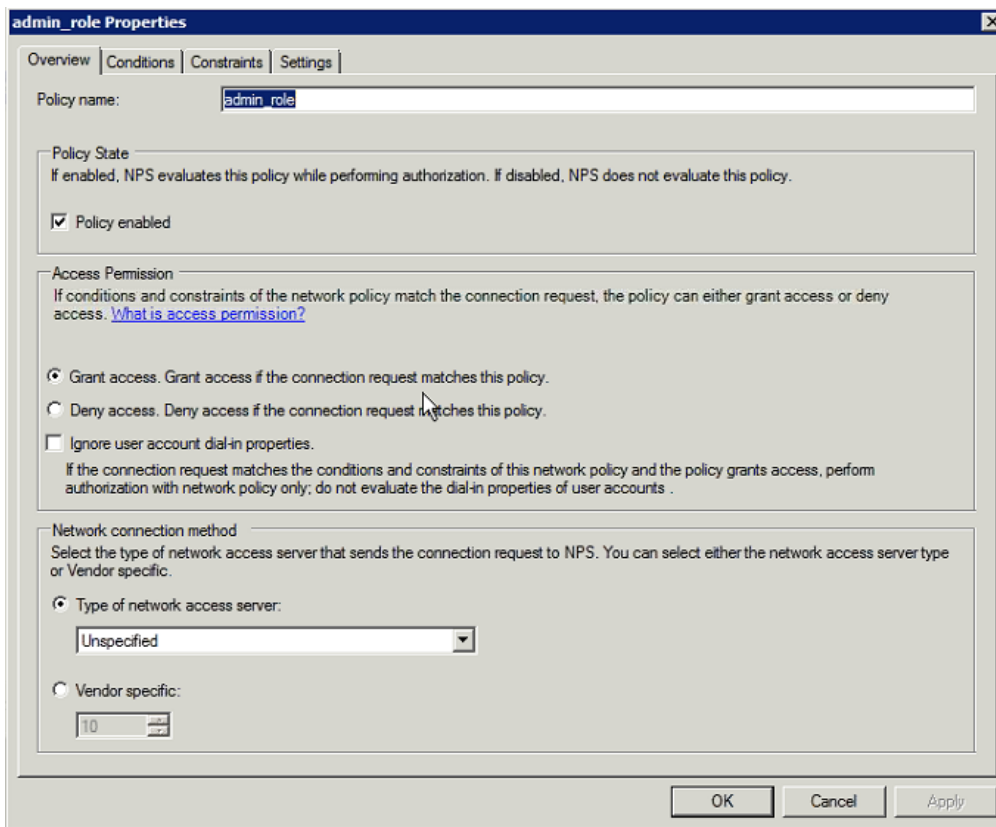
Tip: When creating the security groups, ensure that they map one-to-one to CG-NMS roles (that is, every role defined in CG-NMS maps to only one AD security group). The name of the security group does not have to match a role name in CG-NMS, but for organizational purposes, Cisco recommends using names that correlate the security group name to a CG-NMS role.

Note: You cannot create or assign the CG-NMS root role in AD.
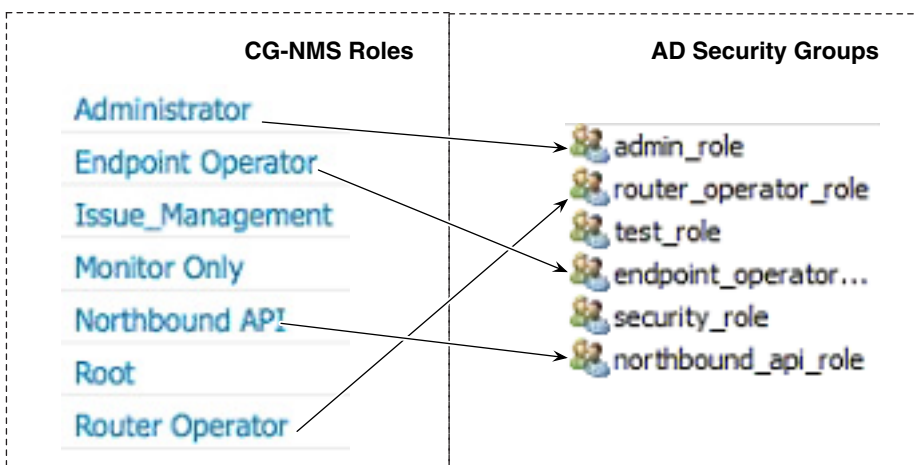
5. Assign AD users a role by adding them to the security group mapping to that role.

    Since, users can only belong to one security group, the CG-NMS role that the user is assigned after log in is dependent on their assigned AD security group.

Configuring Remote Authentication

Tip: In AD, users cannot be assigned multiple CG-NMS roles, and cannot belong to multiple security groups. To assign permissions from more than one role to a group of users, create a new CG-NMS role with the required permissions, and a create the corresponding AD security group. Users in this new group can then carry out the tasks allowed by this role.
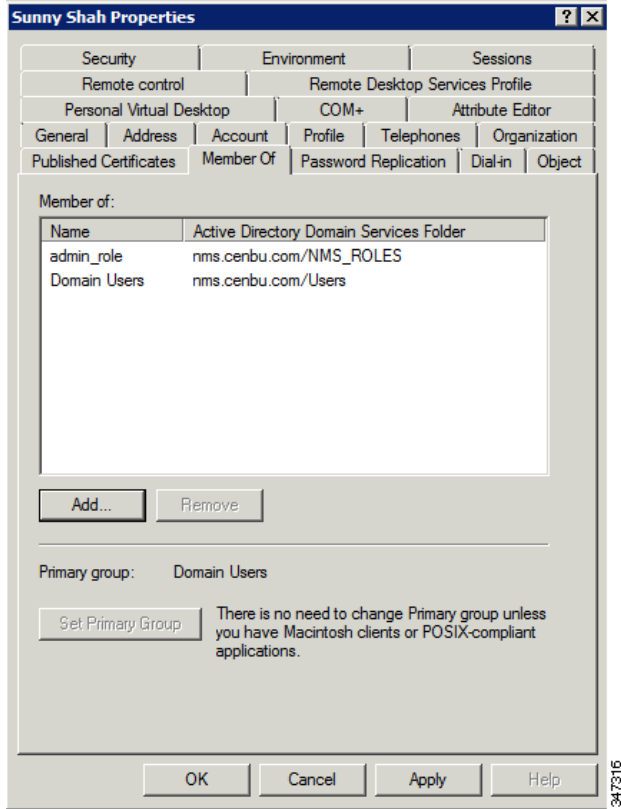
6. Configure the Dial-in Network Access Permission to use the NPS Network Policy.
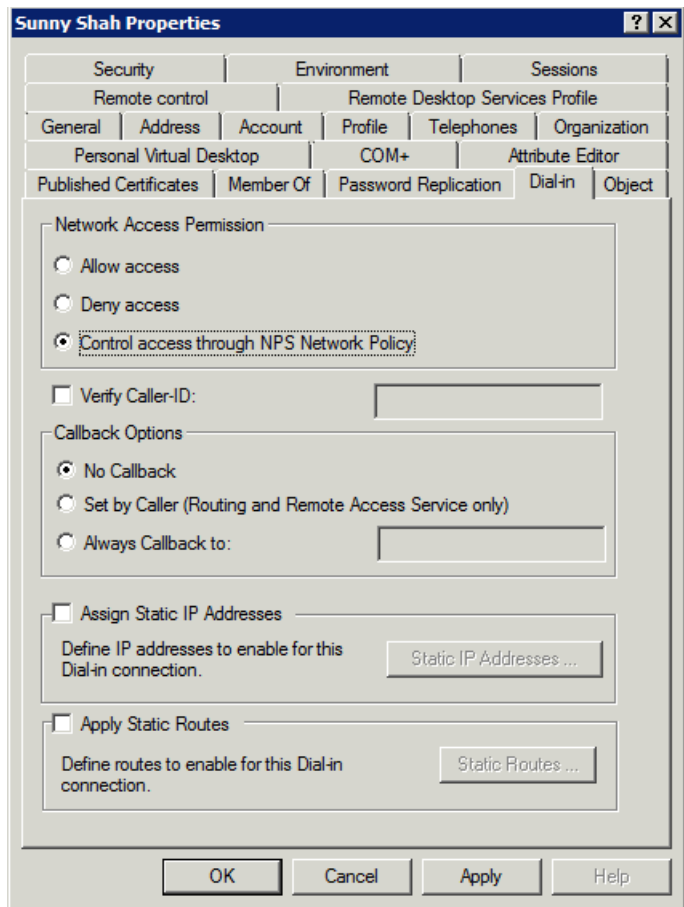
Configuring Security Policies on the RADIUS Server

To authorize users for CG-NMS access, configure security policies for the RADIUS server.

To configure security policies on the RADIUS server, follow these steps:

1. Create a network policy for each security group you created in AD.

2. Configure the policy as follows:

   a. In the Overview pane, define the policy name, enable it, and grant access permissions.
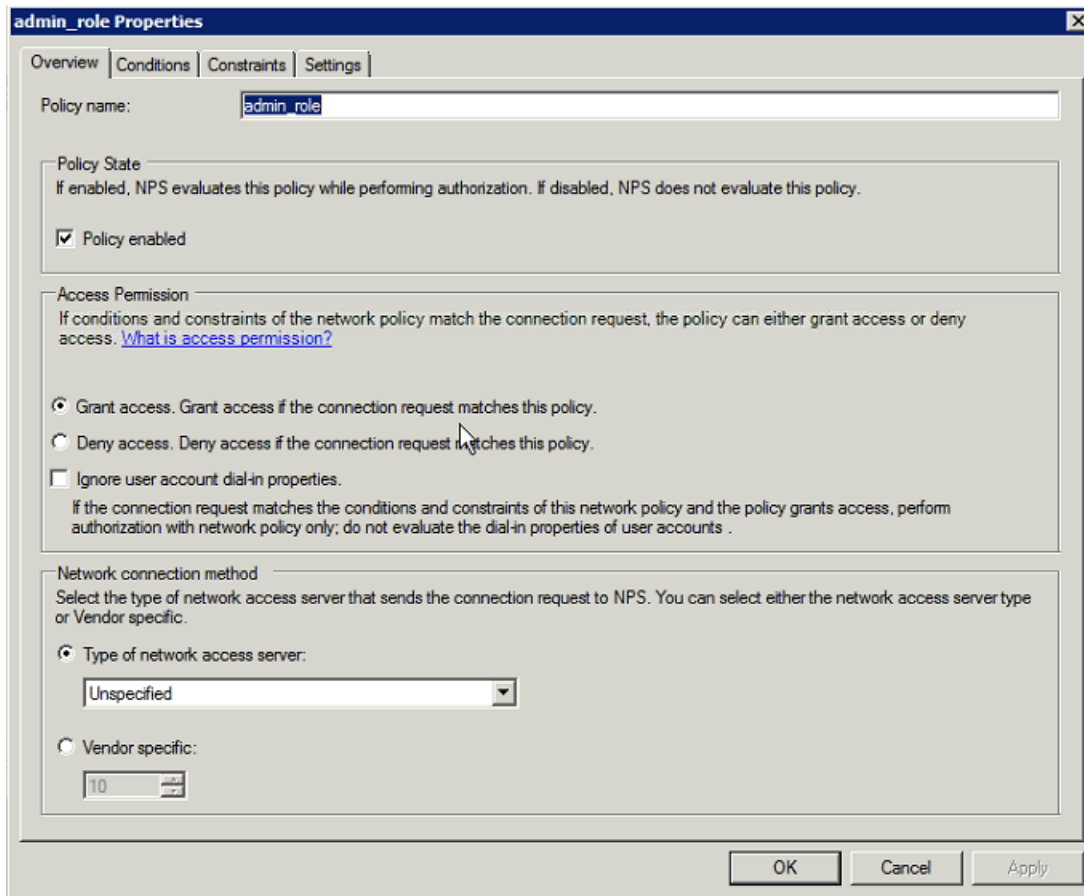
b. Click the **Conditions** tab, select the **User Groups** condition, and click **Add**.
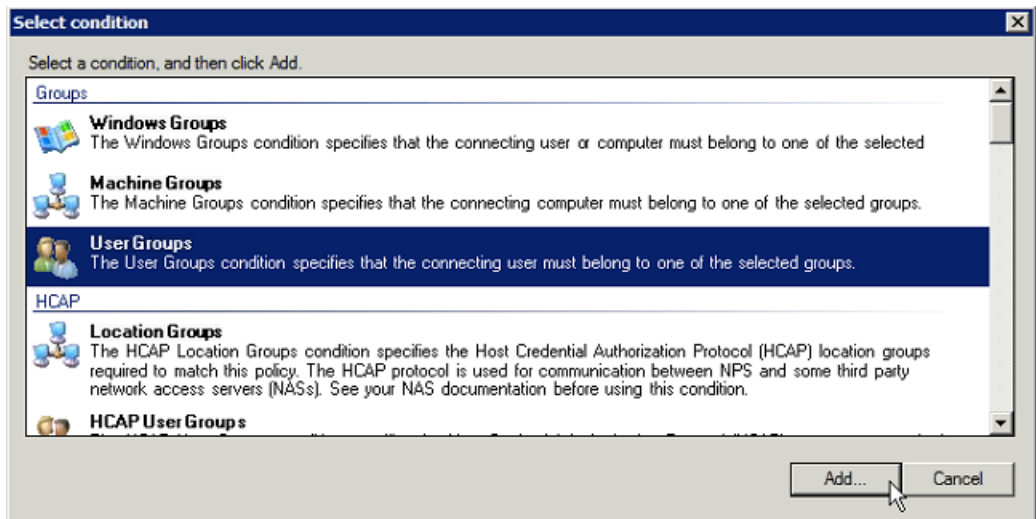
The User Groups condition specifies that the connecting user must belong to the selected group. For this policy to pass, the user being authorized must belong to the user group configured in this policy.

c. In the User Groups window, click **Add Groups**.

Configuring Remote Authentication
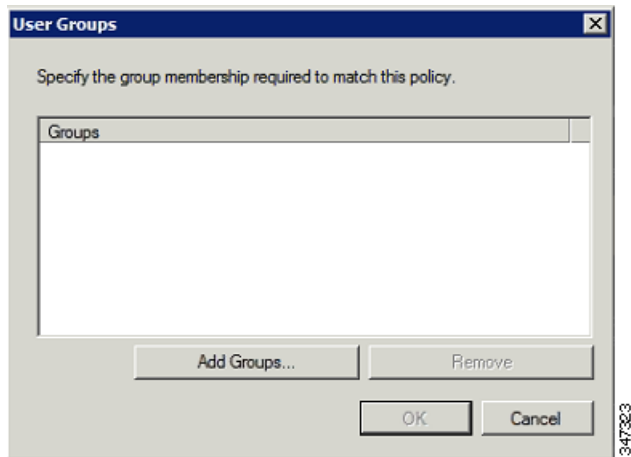
d. In the Select Group window, enter the name of the group

e. Click **OK** to close the Select Group dialog box, and then click **OK** to close the User dialog box.
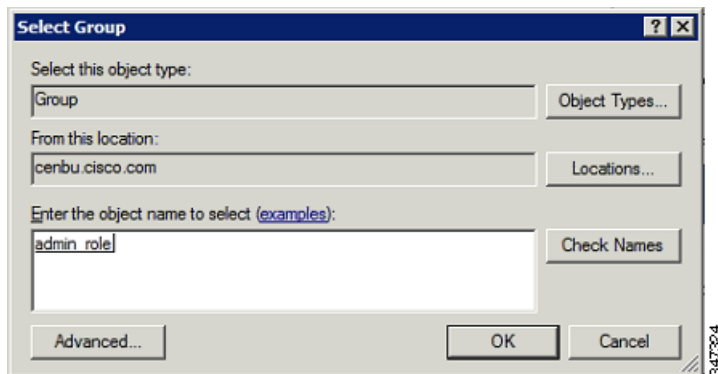
f. Click **Cancel** to close the Select condition window.

The condition appears in the Conditions pane.

Configuring Remote Authentication
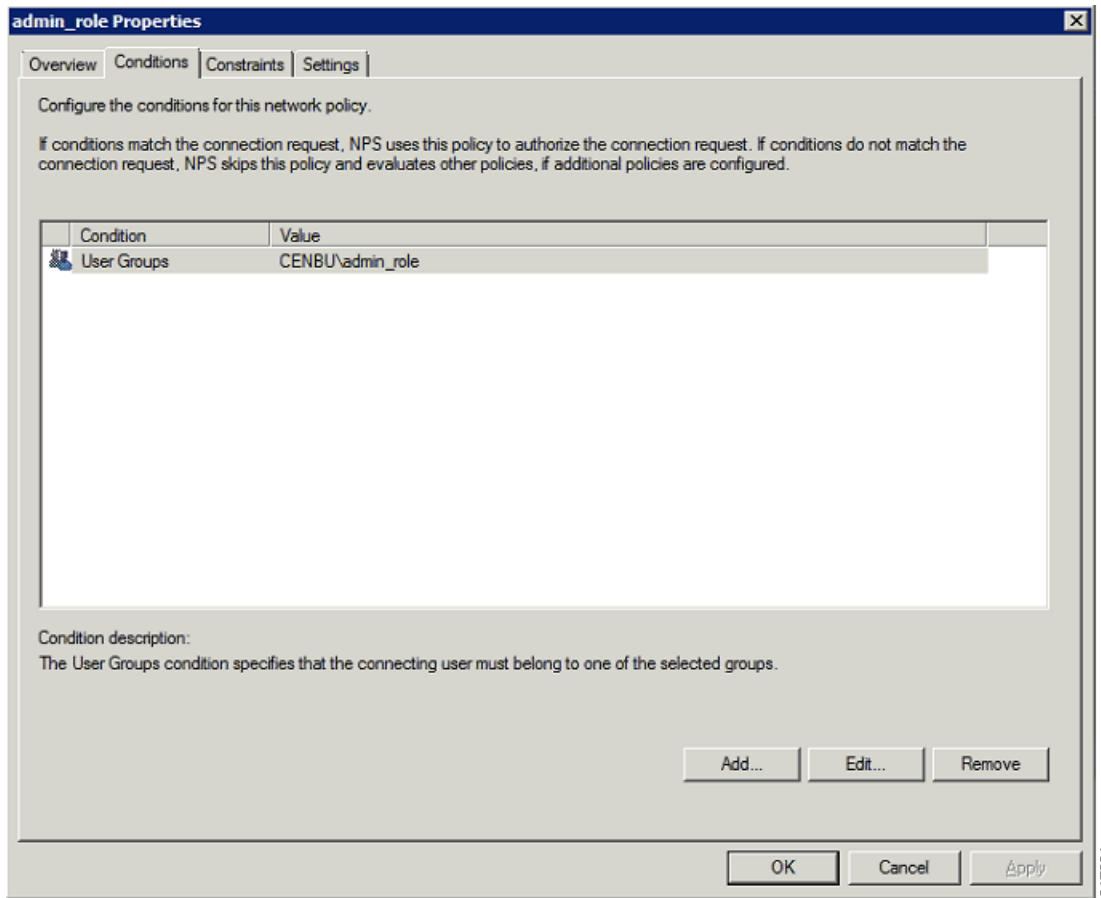
g. Click the **Settings** tab, and then click **Add** to display the Attribute Information window.

```
Add Vendor Specific Attribute                                          [X]

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.


Vendor:
Cisco                                                    [v]

Attributes:
 Name          Vendor
 Cisco-AV-Pair  Cisco




Description:
Specifies the Cisco AV Pair VSA.


                                         [ Add... ]    [ Close ]
```
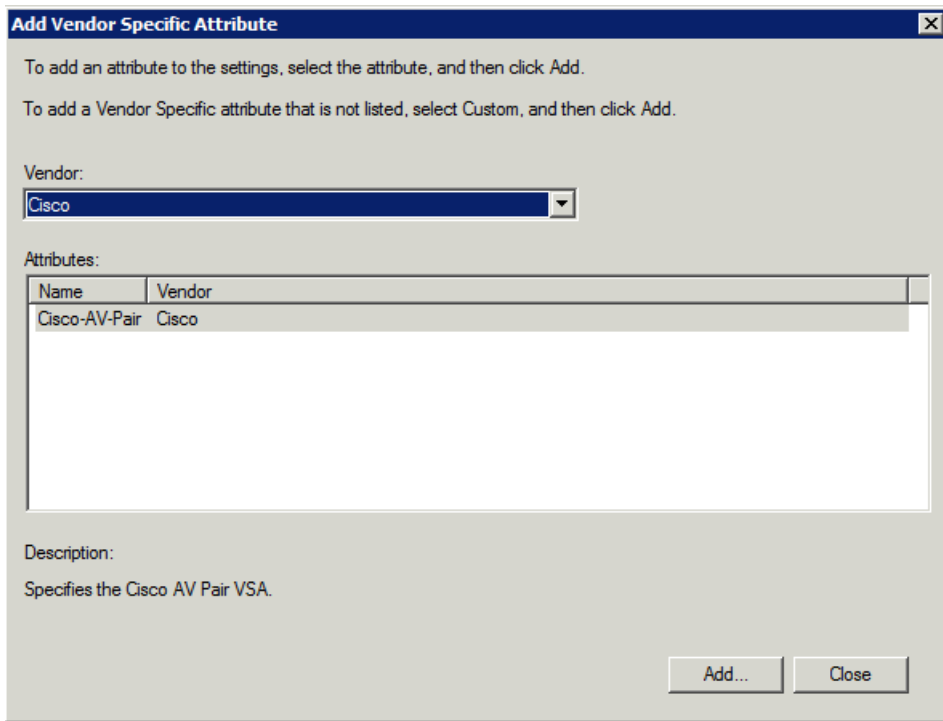
h. Click **Add** to define a Vendor Specific Attribute (VSA) that is sent to CG-NMS (RADIUS client) after the user credentials and security group membership are verified.

The VSA to configure is:

- Attribute Name: Cisco-AV-Pair
- Attribute number: 5000
- Attribute format: String.
- Attribute value: Enter the attribute value to send to CG-NMS.

```
Attribute Information                    [X]

Attribute name:
Cisco-AV-Pair

Attribute number:
5000

Attribute format:
String

Attribute value:
Administrator

              [ OK ]    [ Cancel ]
```
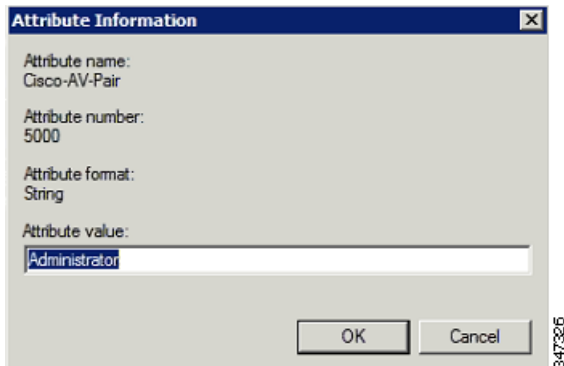
Note: The string entered in the Attribute value field must be the exact string listed in the Radius Server VSA column on the Roles page in CG-NMS (**Admin > Access Management > Roles**).

98

Configuring Remote Authentication
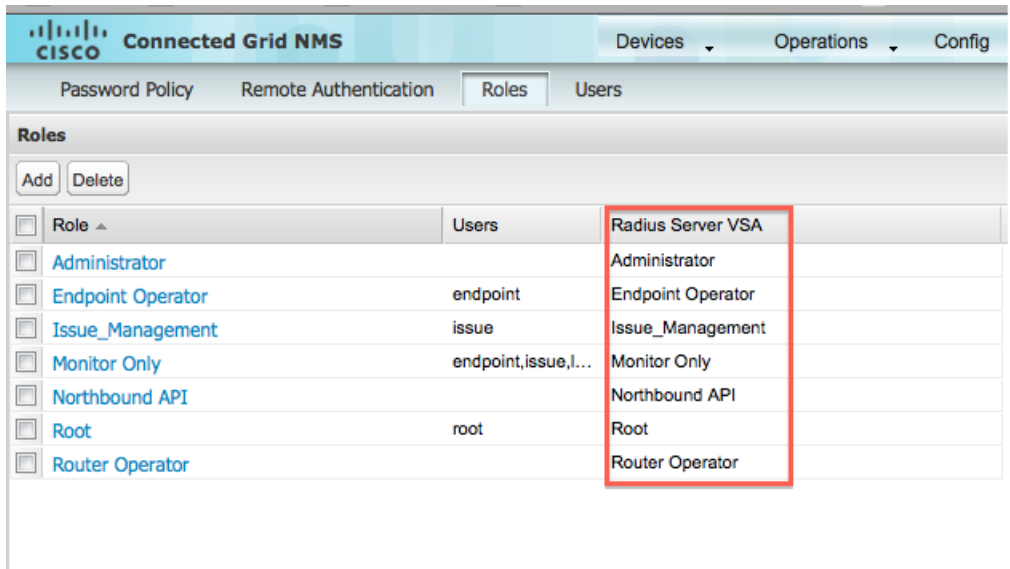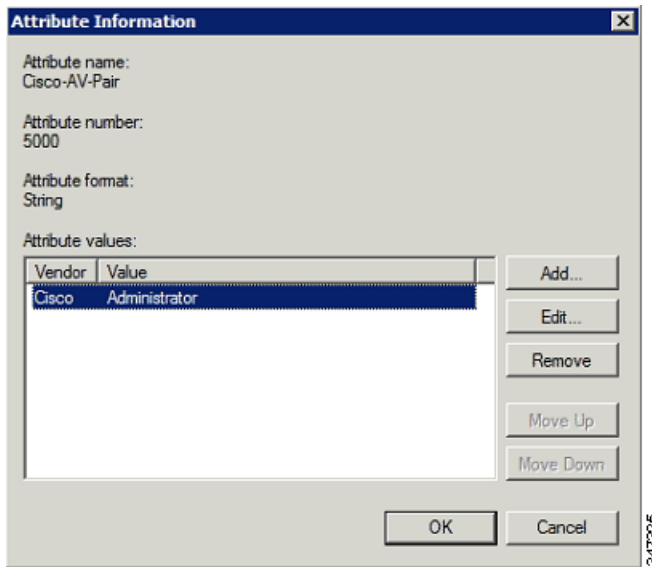
i. Click **OK**.

The VSA attribute appears in the Settings pane.
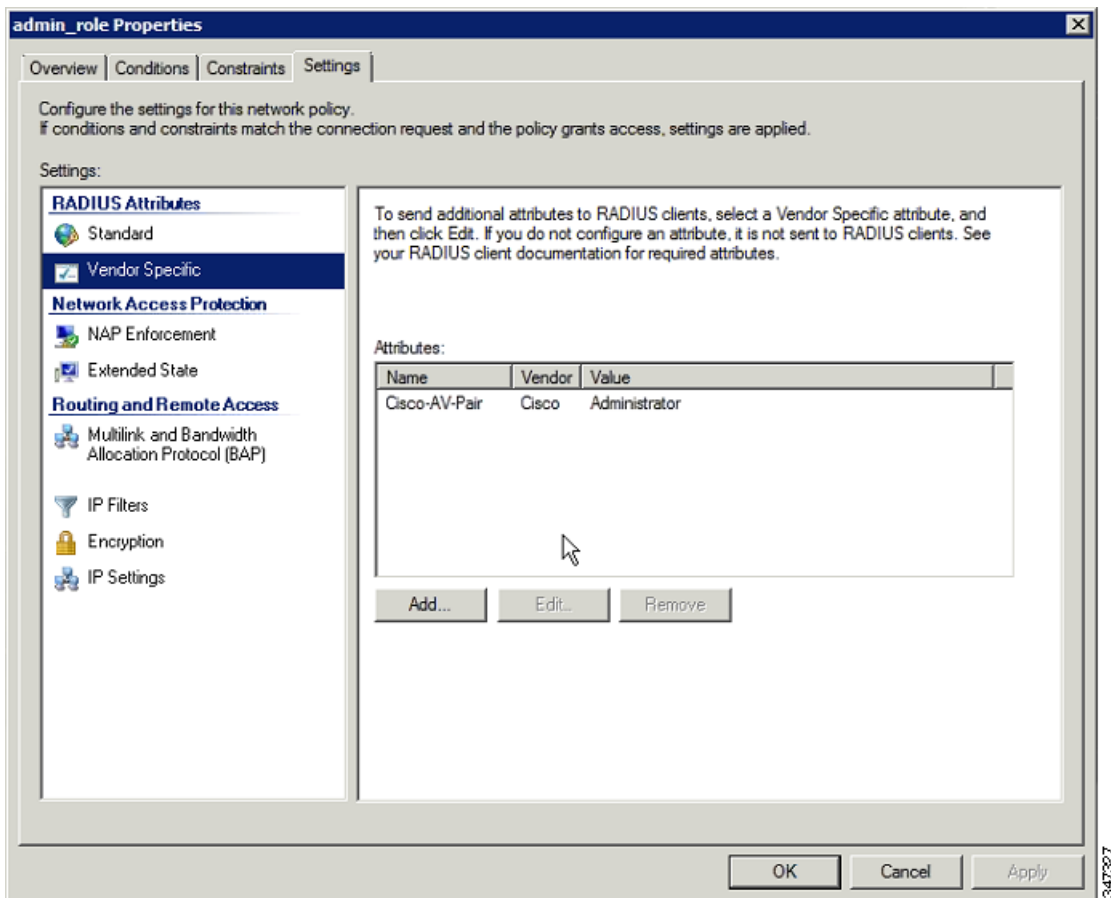
  j. Click **OK**.

Configuring Remote Authentication in CG-NMS

You enable remote user authentication and configure RADIUS server settings on the Remote Authentication page (**Admin > Access Management > Remote Authentication**).

To configure remote authentication:

  1. Choose **Admin > Access Management > Remote Authentication**.
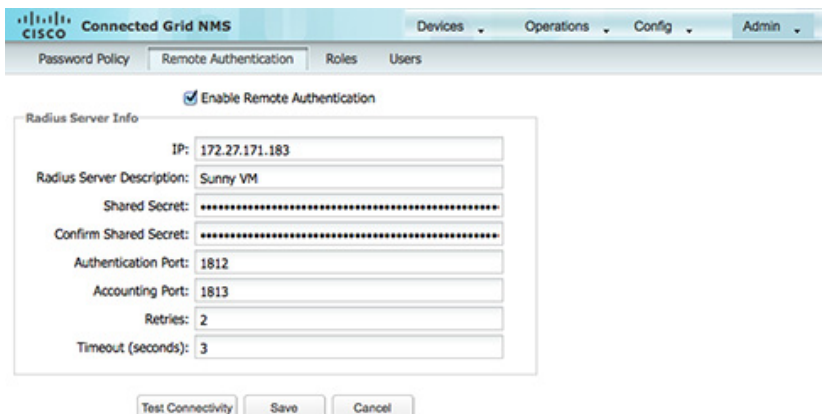
2. Check the **Enable Remote Authentication** check box.

3. Enter this information about the RADIUS server:

Field	Description
IP	The IP address of the RADIUS server.
Name	A descriptive name of the RADIUS server.
Shared Secret	The shared secret you configured on the RADIUS server.
Confirm Shared Secret	
Authentication Port	The RADIUS server port that CG-NMS uses to send request to. The default port is 1812.
Accounting Port	The RADIUS server accounting port. The default port is 1813.
Retries	The number of times to send a request to the RADIUS server before CG-NMS times out and remote authentication fails because no response was received from the RADIUS server.
Timeout	The number of seconds before CG-NMS times out and remote authentication fails because no response was received from the RADIUS server.

4. To ensure that CG-NMS can reach the RADIUS server, click **Test Configuration**.

   a. Enter your AD username and password.

   b. Click **Submit**.

   The results of the configuration test displays.

   c. Click **OK**.

5. Click **Save** when done.

Enabling and Disabling Remote User Accounts

In CG-NMS you cannot enable or disable remote AD user accounts. To enable or disable remote AD user accounts, use your AD server.

Deleting Remote User Accounts

In CG-NMS, you can delete remote user accounts. However, this only removes the user from the CG-NMS Users page (**Admin > Access Management > Users**); it does not delete the user account from AD. If a deleted user logs in to CG-NMS and AD authentication is successful, an entry for the user is added to the CG-NMS Users page.

Logging In to CG-NMS Using a Remote User Account

Logging in to CG-NMS using a remote AD user account is transparent to the user. In the background, CG-NMS checks whether the account is local, and for remote users sends an authentication request to the RADIUS server configured on the Remote Authentication page (**Admin > Access Management > Remote Authentication**). If both authentication and authorization are successful, CG-NMS adds an entry for the user in the Users page (**Admin > Access Management > Users**).

Unlike entries for local users on the Users page, the user name filed in remote user entries is not a link. You cannot click the name of a remote user to obtain more information about the user.

Note: Remote users cannot be managed through CG-NMS. If a remote user wants to update their password, they must use their organization's AD password update tool. Remote users cannot update their password using CG-NMS.

Managing Roles

Use roles to assign permissions based on the role or roles a user plays. Roles define the type of tasks CG-NMS users can perform. This section has the following topics:

- Adding Roles
- Deleting Roles
- Editing Roles
- Viewing Roles

CG-NMS lets you assign a role to any user. The operations the user can perform are based on the permissions enabled for the role. The following topics are discussed in this section:

- Basic User Permissions
- System-Defined User Roles
- Custom User Roles

Basic User Permissions

Table 1 describes basic CG-NMS permissions.

Table 1   CG-NMS User Permissions

Permission	Description
Add/Modify/Delete Devices	Allows users to import, remove and change FAR and endpoint devices.
Administrative Operations	Allows users to perform system administration operations such as user management, role management, and server configuration settings.
Endpoint Configuration	Allows users to edit configuration templates and push configuration to MEs.
Endpoint Firmware Update	Allows users to add and delete firmware images and perform ME firmware update operations.
Endpoint Group Management	Allows users to assign, remove and change devices from ME configuration and firmware groups.
Endpoint Reboot	Allows users to reboot the ME device.
Issue Management	Allows users to close issues.
Label Management	Allows users to add, change, and remove labels.
Manage Device Credentials	Allows users to view FAR credentials such as WiFi pre-shared key, admin user password, and master key.
Manage Head-End Devices Credentials	Allows users to view the ASR admin NETCONF password.
NBAPI Audit Trail	Allows users to query and delete audit trails using CG-NMS NB API.
NBAPI Device Management	Allows users to add, remove, export, and change FAR and endpoint devices using CG-NMS NB API.
NBAPI Endpoint Operations	Allows users to manage endpoint operations using CG-NMS NB API.
NBAPI Event Subscribe	Allows users to search events, subscribe and unsubscribe from events (including Outage events) using CG-NMS NB API.
NBAPI Reprovision	Allows users to reprovision devices using CG-NMS NB API.
NBAPI Rules	Allows users to search, create, delete, activate, and deactivate rules using CG-NMS NB API.

Table 1 **CG-NMS User Permissions (continued)**

Permission	Description
NBAPI Search	Allows users to search devices, get device details, group information, and metric history using CG-NMS NB API.
Router Configuration	Allows users to edit FAR configuration templates and push configuration to FARs.
Router Firmware Update	Allows users to add and delete firmware images and perform firmware update operations for FARs.
Router Group Management	Allows users to assign, remove, and change device assignments to FAR configuration and firmware groups.
Router Reboot	Allows users to reboot the FAR.
Rules Management	Allows users to add, edit, activate, and deactivate rules.
Security Policy	Allows users to block mesh devices, refresh mesh keys, and so on.
Tunnel Provisioning Management	Allows users to manage tunnel groups, edit/apply tunnel-related templates, and perform factory reprovisioning.
Work Order Management	Allows users to manage work orders for CGDM.

System-Defined User Roles

Note: The system-defined Root role cannot be assigned to users.

Table 2 lists system-defined roles. These roles cannot be modified.

Table 2 **System-defined User Roles**

Role	Description
Add Devices	This role can add, modify, and delete devices from CG-NMS.
Administrator	This role combines these basic permissions: ■ Administrative Operations ■ Label Management ■ Rules Management
Endpoint Operator	This role combines these basic permissions: ■ Label Management ■ Endpoint Configuration ■ Endpoint Firmware Update ■ Endpoint Group Management ■ Endpoint Reboot
Monitor Only	This role provides users with read-only access to CG-NMS. By default, this role is defined for every user.

Table 2   System-defined User Roles (continued)

Role	Description
North Bound API	This role combines these basic permissions: ■ NBAPI Audit Trail ■ NBAPI Device Management ■ NBAPI Endpoint Operations ■ NBAPI Event Subscribe ■ NBAPI Orchestration Service ■ NBAPI Rules ■ NBAPI Search
Router Operator	This role combines these basic permissions: ■ Label Management ■ Router Configuration ■ Router Firmware Update ■ Router Group Management ■ Router Reboot
Router Operator with Manage Device Creds	This role combines the permissions of a Router Operator with: ■ Device credential management
Security Policy	This role can manage security policies through CG-NMS.
Tunnel Provisioning Management	This role can provision tunnels.

Custom User Roles

In CG-NMS you can define custom roles. For each role you create, you can assign it one or more basic user permissions (see Table 1). These permissions specify the type of actions users with this role can perform.

Adding Roles

To add CG-NMS user roles:

1. Choose **Admin > Access Management > Roles**.

2. Click **Add**.
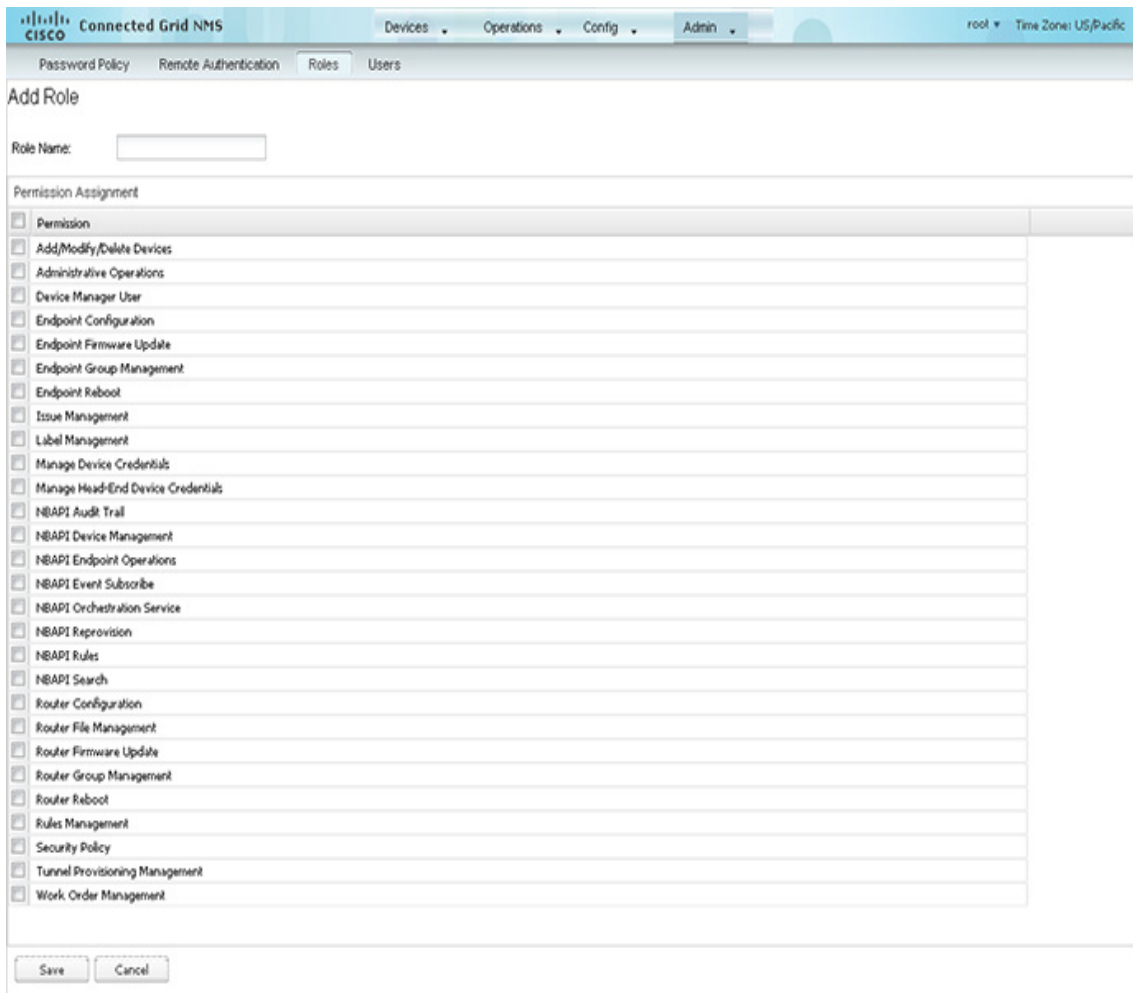
3. Enter the name of the role.

4. Check the appropriate check boxes to assign permissions.

5. Click **Save**.

6. To continue to add roles, click **Yes**; otherwise, click **No** to return to the Roles page.

Deleting Roles

Note: You cannot delete a custom role if it is in use.

To delete CG-NMS user roles:

1. Choose **Admin > Access Management > Roles**.

2. Check the check boxes of the roles to delete.

3. Click **Delete**.

4. Click **Yes**.

5. Click **OK**.

Editing Roles

Note: You cannot edit system-defined roles, but you can edit custom roles.

To edit CG-NMS custom roles:

1. Choose **Admin > Access Management > Roles**.

2. Click the role to edit.

3. Make changes to the permission assignments by checking or unchecking the relevant check boxes.

4. Click **Save**.

Viewing Roles

To view CG-NMS user roles:

1. Choose **Admin > Access Management > Roles**.

For every role, CG-NMS lists the users assigned to this role.

2. To view permission assignments for the role, click the role link.

Managing Users

This section has the following topics on managing users:

- Resetting Passwords

- Viewing Users

- Adding Users

- Deleting Users

- Enabling Users

- Disabling Users

- Editing Users

Resetting Passwords

As the root user of the Linux server on which CG-NMS runs, you can reset your password and use the password utility to reset the password for any other CG-NMS user.

To reset a password, enter this command:

```
[root@yourname-lnx1 bin}#./password_admin.sh root
```

CG-NMS manages its own user account database; therefore, you must add all new local users from the CG-NMS user interface at the **Admin > Access Management > Users** page. Remote users are automatically added to the database. You can also enable, disable, edit, or delete users on this page.

A user with a disabled account cannot log in until an administrator enables their account. After a user account is active, the user must reset their password. There is no limit to the number of users that you can define on the system other than the available database storage.

Viewing Users

To view CG-NMS users, open the Users page (**Admin > Access Management > Users**).

CG-NMS displays this information about users:

Field	Description
User Name	Specifies the user name.
Enabled	Indicates whether the user account is enabled.
Time Zone	Specifies the user's time zone.
Roles	Specifies the roles assigned to the user.
Audit Trail	A link to the user's audit trail.
Remote User	Indicates whether the user account is stored locally. If the value is false, the user account is stored in Active Directory and is accessed via the RADIUS server configured in the Remote Authentication page (**Admin > Access Management > Remote Authentication**).

Adding Users

To add users to CG-NMS:

1. Choose **Admin > Access Management > Users**.

2. Click **Add**.
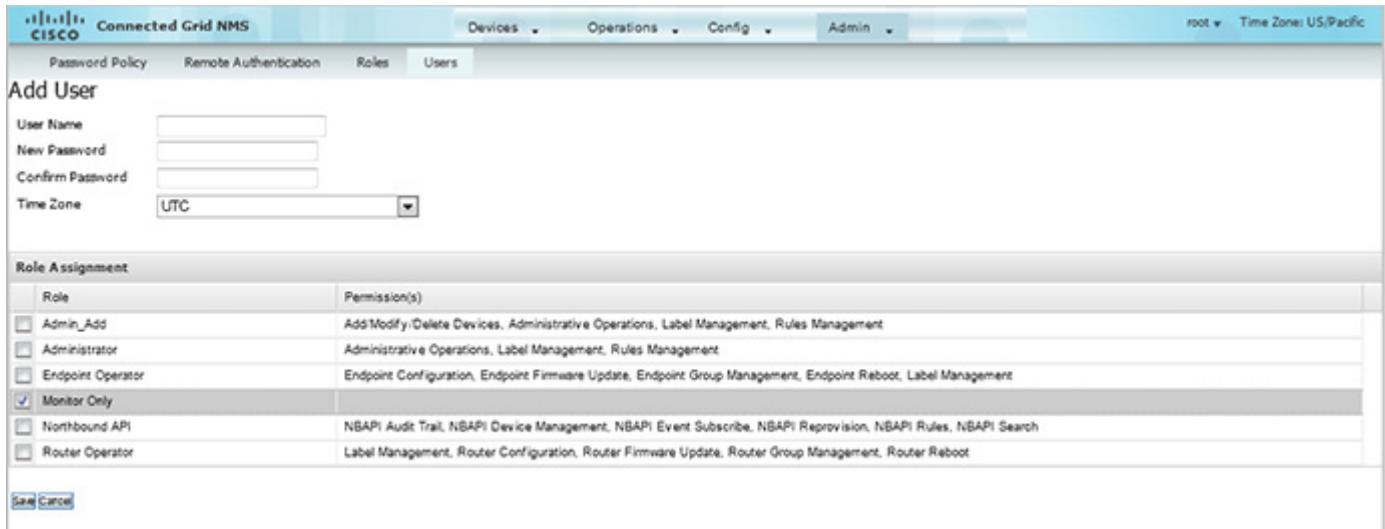
3. Enter the following user information:

Field	Description
User Name	Enter the user name.
New Password	Enter the password. The password must conform to the CG-NMS password policy.
Confirm Password	Re-enter the password.
Time Zone	Choose a time zone from the drop-down menu.

4. Select the user roles to assigned to this user by checking the appropriate check box under Role Assignment.

5. Click **Save**.

CG-NMS creates a record for this user in the CG-NMS database.

6. To add the new user, click **Yes**; otherwise, click **No** to return to the Users page.

Note: A new user account is enabled by default. This means that the user can access CG-NMS.

Deleting Users

Deleting user accounts removes user preferences such as the default map location from the system. Disable a user account to temporarily deactivate it.

To delete users from CG-NMS:

1. Choose **Admin > Access Management > Users**.

2. Check the check boxes of the user accounts to delete.

3. Click **Delete**.

4. Click **Yes** to confirm.

5. Click **OK**.

Enabling Users

You must enable the user account for users to access CG-NMS. When users log in for the first time, CG-NMS prompts them to change their password.

To enable user accounts in CG-NMS:

1. Choose **Admin > Access Management > Users**.

2. Check the check boxes for the user accounts to enable.

3. Click **Enable**.

4. Click **Yes**.

5. Click **OK**.

Disabling Users

To prevent users from accessing CG-NMS, disable their accounts. Disabling user accounts does not delete their records from the CG-NMS database.

To disable user accounts in CG-NMS:

1. Choose **Admin > Access Management > Users**.

2. Check the check boxes for the user accounts to disable.

3. Click **Disable**.

   Note: If you disable a user account, CG-NMS resets the user password.

4. Click **Yes**.

5. Click **OK**.

Editing Users

To edit user settings in CG-NMS:

1. Choose **Admin > Access Management > Users**.

2. To edit user credentials:

   a. Click the user name link.

   b. Edit the role assignments.

   c. Click **Save**.

Managing Users

Managing System Settings

This chapter describes how to manage system settings, and includes the following sections:

- Managing Active Sessions

- Displaying the Audit Trail

- Managing Certificates

- Configuring Data Retention

- Managing Licenses

- Managing Logs

- Configuring Provisioning Settings

- Configuring Server Settings

- Managing the Syslog

Note: To manage system settings, you must be logged in either as root or as a user with Administrative Operations permissions.

System settings are managed from the **Admin > System Management menu (Figure 1)**

Managing Active Sessions

Figure 1   Admin Menu

Managing Active Sessions

CG-NMS tracks active user sessions and lets you log out users.

- Viewing Active Sessions

- Logging Users Out

- Filtering the Active Sessions List

Viewing Active Sessions

To view active user sessions, choose **Admin > System Management > Active Sessions**. CG-NMS displays the Active Sessions page (Figure 2).

Figure 2   Active Sessions Page
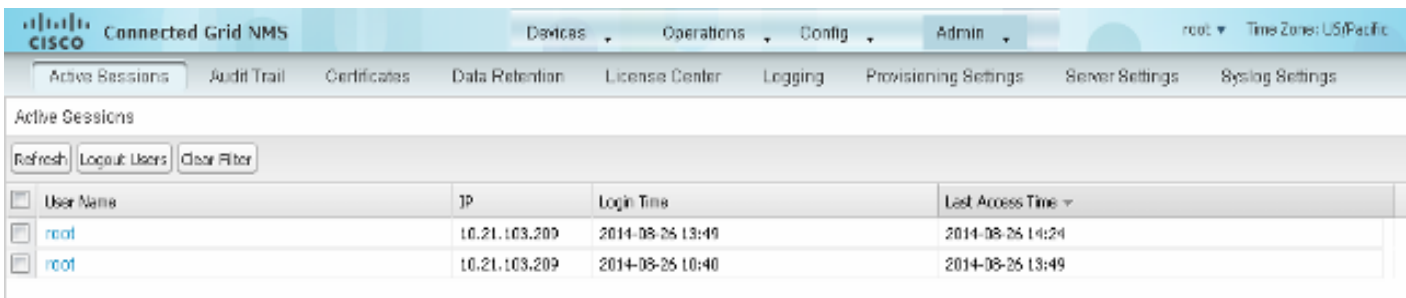
Table 1 describes the Active Session fields.

Table 1   Active Session Fields

Field	Description
User Name	The user name in the session record. To view user settings, click the user name.
IP	The IP address of the system the user employs to access CG-NMS.
Login Time	The log in date and time for the user.
Last Access Time	The last time the user accessed the system.

Tip: Click **Refresh** to update the users list.

Logging Users Out

To log CG-NMS users out:

1. Choose **Admin > System Management > Active Sessions**.

2. Check the check boxes of the users to log out.

3. Click **Logout Users**.

4. Click **Yes**.

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

1. Choose **Admin > System Management > Active Sessions**.

2. From the User Name drop-down menu, choose **Filters** and enter the user name or the first characters in the user name to filter the list.
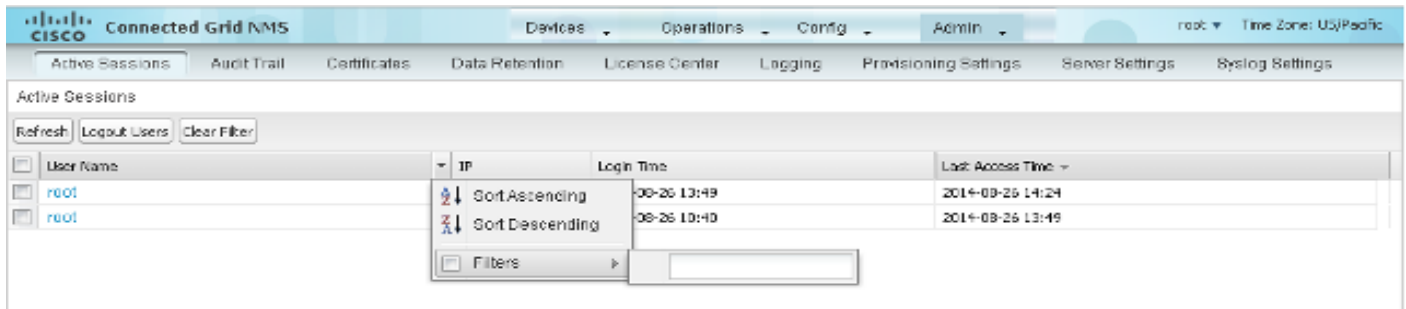
For example, to list the active sessions for the root user, enter **root**.

Tip: To remove the filter, from the User Name drop-down menu, clear the **Filters** check box or click **Clear Filter**.

Displaying the Audit Trail

Use the audit trail to track CG-NMS user activity.

To display the Audit Trail, choose **Admin > System Management > Audit Trail**.

Table 2 describes the Audit Trail fields.

Table 2   Audit Trail Fields

Field	Description
Date/Time	Date and time of the operation.
User Name	The user who performed the operation. To view user settings, click the user name.
IP	IP address of the system that the user employs to access CG-NMS.
Operation	Type of operation performed.
Status	Status of the operation.
Details	Operation details.

Tip: Click **Refresh** to update the list.

Filtering the Audit Trail List

To filter the Audit Trail list using column filtering:

1. Choose **Admin > System Management > Audit Trail**.

2. From the User Name drop-down menu, choose Filters and enter the user name or the first characters of the user name to filter the list.

For example, to list the Audit Trail entries for the user jane, enter **jane**.

Tip: To remove the filter, from the User Name drop-down menu, clear the **Filters** check box or click **Clear Filter**.

Managing Certificates

The Certificates page displays the certificates for CSMP (CoAP Simple Management Protocol), CGDM (Connected Grid Device Manager), and Web used by CG-NMS and lets you download these certificates.

To display the CSMP, CGDM and Web certificates:

1. Choose **Admin > System Management > Certificates**.

2. To view a certificate, click its corresponding tab.
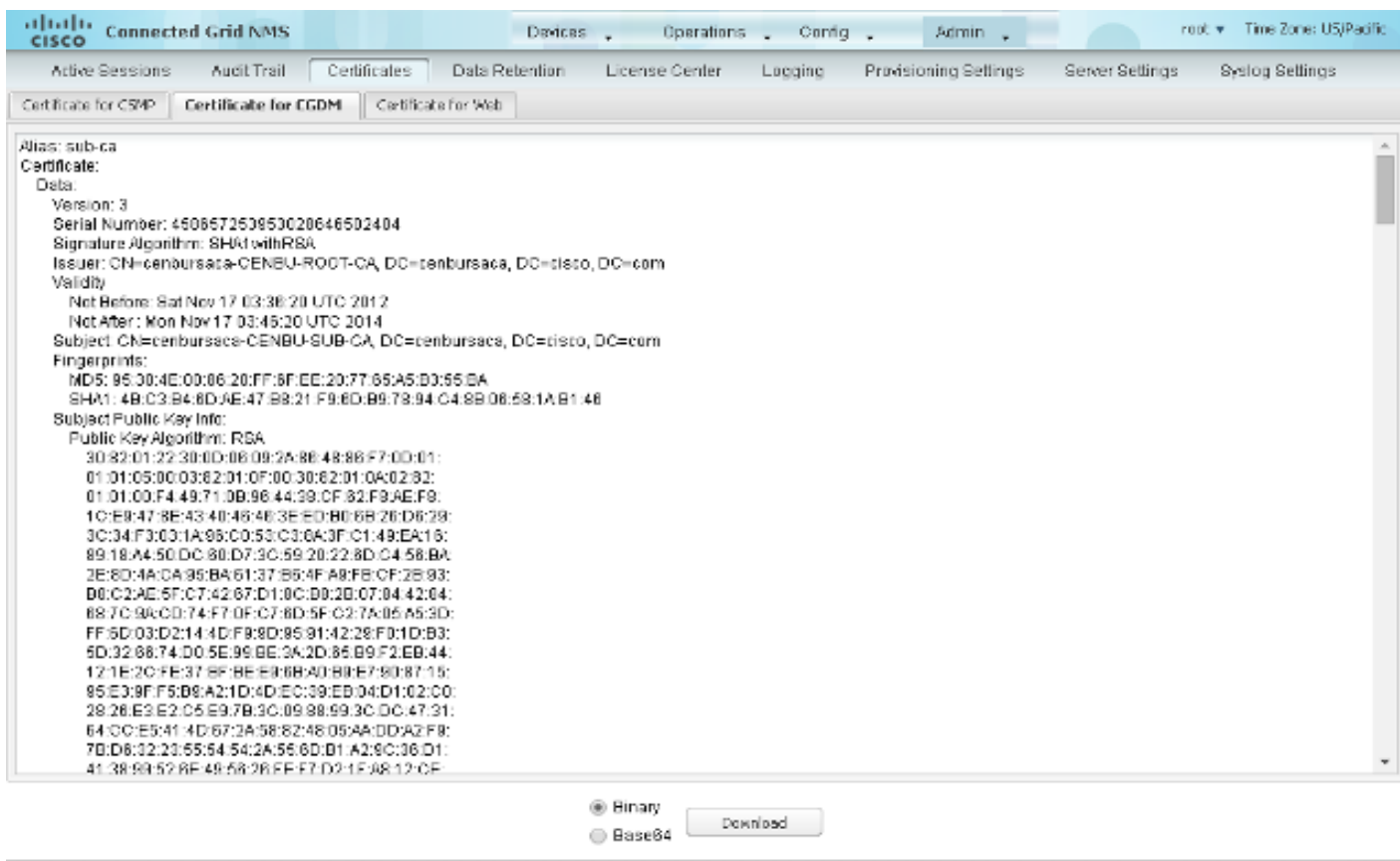
3. To download a certificate, click the encoding (**Binary** or **Base64**) radio button, and then click **Download**.

For more information about certificates, see Generating and Installing Certificates.

Configuring Data Retention

The Data Retention page lets you determine the number of days to keep event, issue, and metric data in the CG-NMS database.

Note: Data retention prunes events even if they have associated open issues.

To set CG-NMS data retention:

1. Choose **Admin > System Management > Data Retention**.
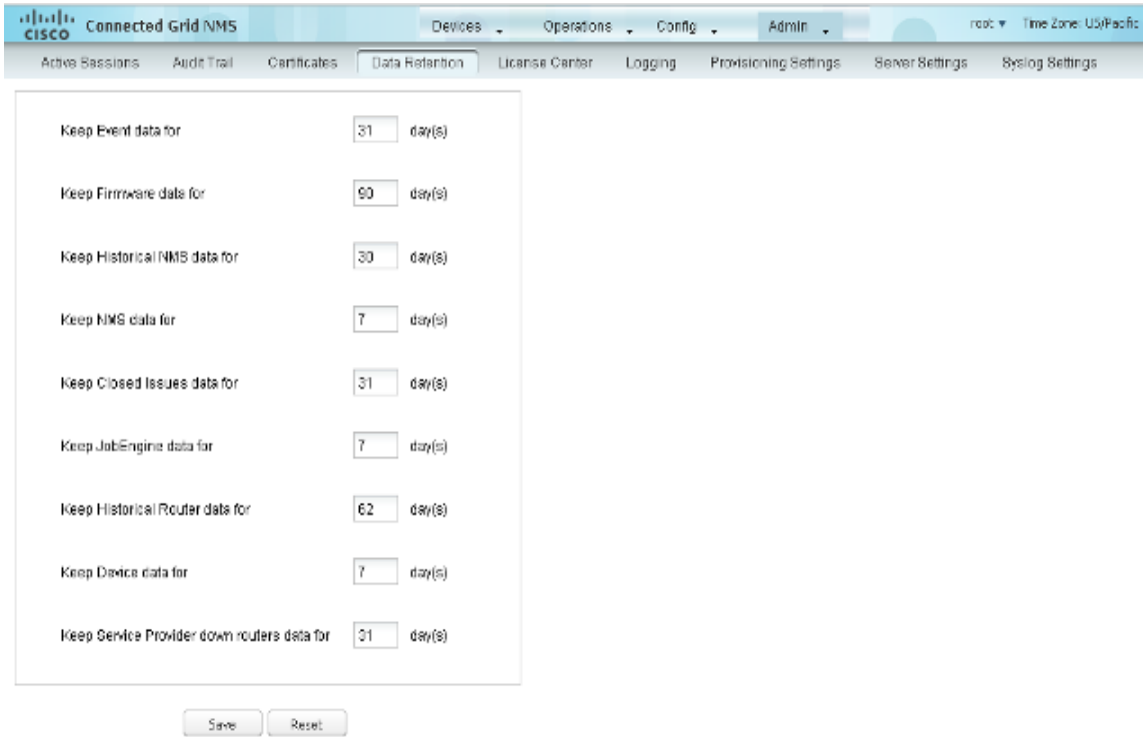
2. For each of the retention categories, specify the number of days to retain data.

   Table 3 lists the allowable maximum values for each field.

Table 3   Data Retention Fields Allowable Maximum Values

Field	Value in Days		
	Minimum	Maximum	Default
Event data	1	90	31
Firmware data	7	180	7
Historical NMS data	1	30	62
NMS data	1	7	7
Closed issues data	1	90	30
Job engine data	1	30	30
Historical router data	1	90	30
Device data	1	7	7
Service provider down routers data	1	31	31

3. Click **Save**.

4. To revert to default settings, click **Reset**.

Managing Licenses

The License Center page (**Admin > System Management > License Center**) lets you view and manage license files.

- Viewing License Summary

- Viewing License Files

- Viewing License File Details

- Adding License Files

- Deleting License Files

Note: CG-NMS performs license enforcement when importing devices. Without licenses, CG-NMS allows only 25 FARs and 10,000 MEs. If you add licenses, CG-NMS only allows the permitted number of devices to be imported, as defined in the licenses.

Viewing License Summary

To view CG-NMS license summary:

1. Choose **Admin > System Management > License Center**.

2. Click **License Summary**.

For every license, CG-NMS displays the information described in Table 4.

Note: IR500s use mesh endpoint licenses, and require no special license.

Table 4   License File Information

Field	Description
Package Name	Name of license package.
Max Router Count	Maximum number of FARs supported.
Max Endpoint Count	Maximum number of mesh endpoints supported.
Max User	Maximum number of users supported.
Max NBAPI User	Maximum number of CG-NMS North Bound API users supported.
Days Until Expire	Number of days remaining until the license expires.

117

Viewing License Files

To view CG-NMS license files:

1. Choose **Admin > System Management > License Center**.

2. Click **License Files**.

For every file, CG-NMS displays the fields described in Table 5.

Table 5   License File Fields

Field	Description
ID	License ID.
PAK	Number for issuing license fulfillment.
Added At	Date and time the license was added to CG-NMS.
License Filename	Filename of the license.

Viewing License File Details

To view license file details:

1. Choose **Admin > System Management > License Center**.

2. Click **License Files**.

3. Choose the licenses to view.

4. Click **Show Details**.

For every selected file, the License File Details section displays the following information:

Table 6   License File Details

Field	Description
Package Name	License package name.
Type	License target (ROUTER, ENDPOINT, USER, NB_USER). The type is an empty string if a value is not applicable.
Max Count	Maximum number of target devices entitled by this license.
Days Until Expire	The number of days remaining until the license expires.

Adding License Files

To add a license file:

1. Choose **Admin > System Management > License Center**.

2. Click **License Files**.

3. Click **Add**.
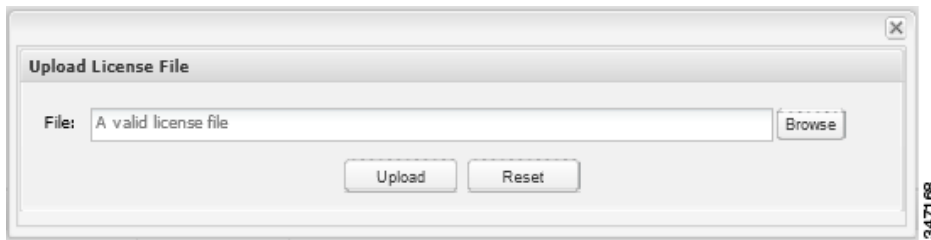
4. Click **Browse** to locate the license file, and then click **Open**.

5. Click **Upload**.

Deleting License Files

Note: You can only delete ALL license files. Ensure that you have access to license files before deleting existing license files. Without licenses, CG-NMS allows registration of only 25 FARs and 10,000 MEs.

To delete license files:

1. Choose **Admin > System Management > License Center**.

2. Click **License Files**.

3. Click **Delete All**, and then click **Yes**.

Managing Logs

- Configuring Log Settings
- Downloading Logs

Configuring Log Settings

CG-NMS lets you change the logging level for the various log categories and download the logs. Logs incur a certain amount of disk space. For example, for 5 million meters at an 8-hour reporting interval and 5000 routers at a 60-minute periodic inventory notification, disk consumption is approximately 7MB/sec. Ensure that your server has enough disk space to contain your logs.

To configure the logging level:

1. Choose **Admin > System Management > Logging**.

2. Click **Log Level Settings**.
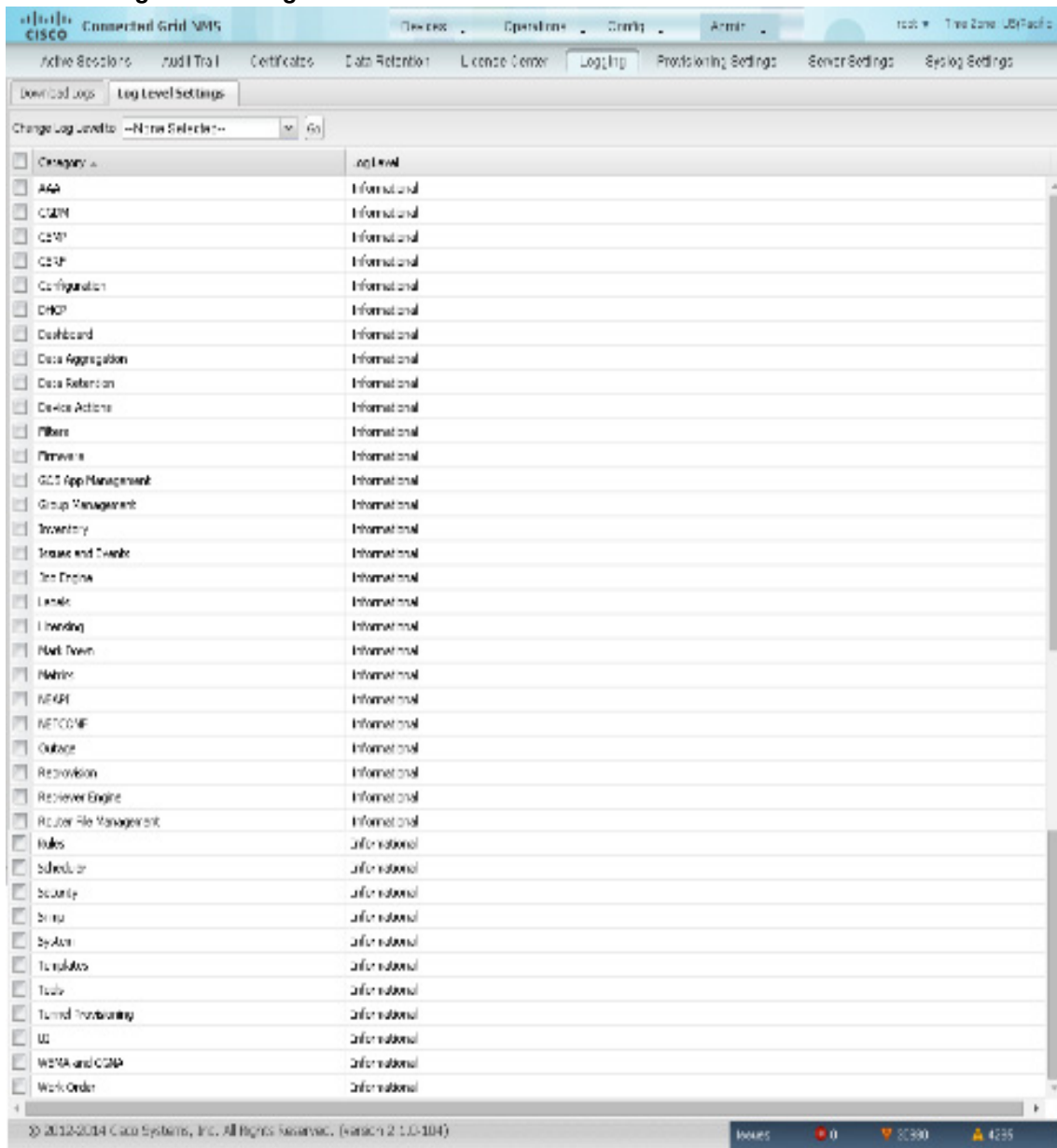
3. Check the check boxes of all logging categories to configure.

4. From the **Change Log Level to** drop-down menu, choose the logging level setting (**Debug** or **Informational**).

■ To generate all possible logging messages, use the **Debug** level.

  Note: Running the **Debug** logging category can impact performance.

■ To generate a subset of these messages, use the **Informational** logging level.

  Note: The **Informational** logging level is the default for all categories when CG-NMS opens. Custom logging level settings are retained between log-in sessions, but not after CG-NMS restarts.

5. To apply the configuration, click **Go**.

> **Note:** The server.log file is rotated based on size.

Downloading Logs

To download logs:

1. Choose **Admin > System Management > Logging**.

2. Click the **Download Logs** tab.
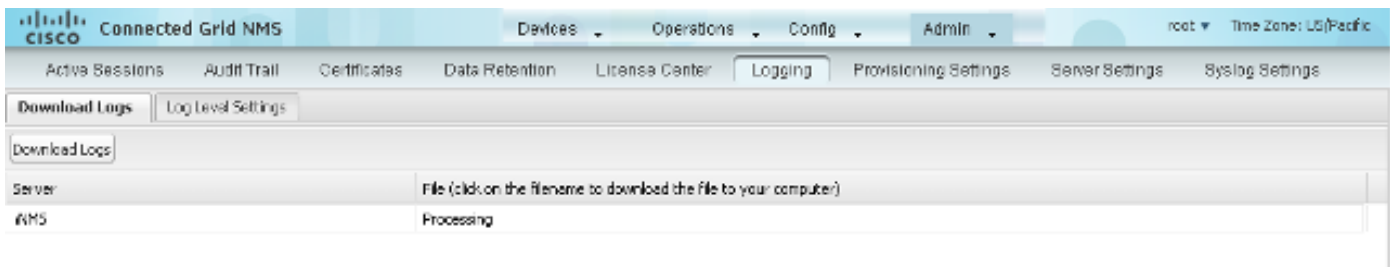
3. Click the **Download Logs** button.

- When you click this button in a single-server deployment, CG-NMS compresses the log files into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.

- In CG-NMS cluster deployments, when you click this button, the CG-NMS server to which you are connected:

  – Compresses the log files on the server into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.

  – Initiates the transfer of the log files in .zip format from the other servers to this server. As files become available, the server adds entries for these files to the Download Logs pane.

4. To download a zip file locally, click its file name.

Tip: In a cluster environment, if you need to send log files to Cisco Support, ensure that you send the log files of all cluster servers.

Configuring Provisioning Settings

The Provisioning Settings page (**Admin > System Management > Provisioning Settings**) lets you configure the CG-NMS URL, DHCPv4 Proxy Client, and DHCPv6 Proxy Client settings required for CG-NMS to create tunnels between FARs and ASRs (Figure 3). See Figure 1 for an example of tunnels as used in the CG-NMS architecture. See Tunnel Provisioning Configuration Process for information on provisioning tunnels. Also, during ZTD you can add DHCP calls to the device configuration template for leased IP addresses.

Note: To configure tunnel and proxy settings, you must be logged in either as root or as a user with Administrative Operations permissions.

Figure 3   Provisioning Settings Page
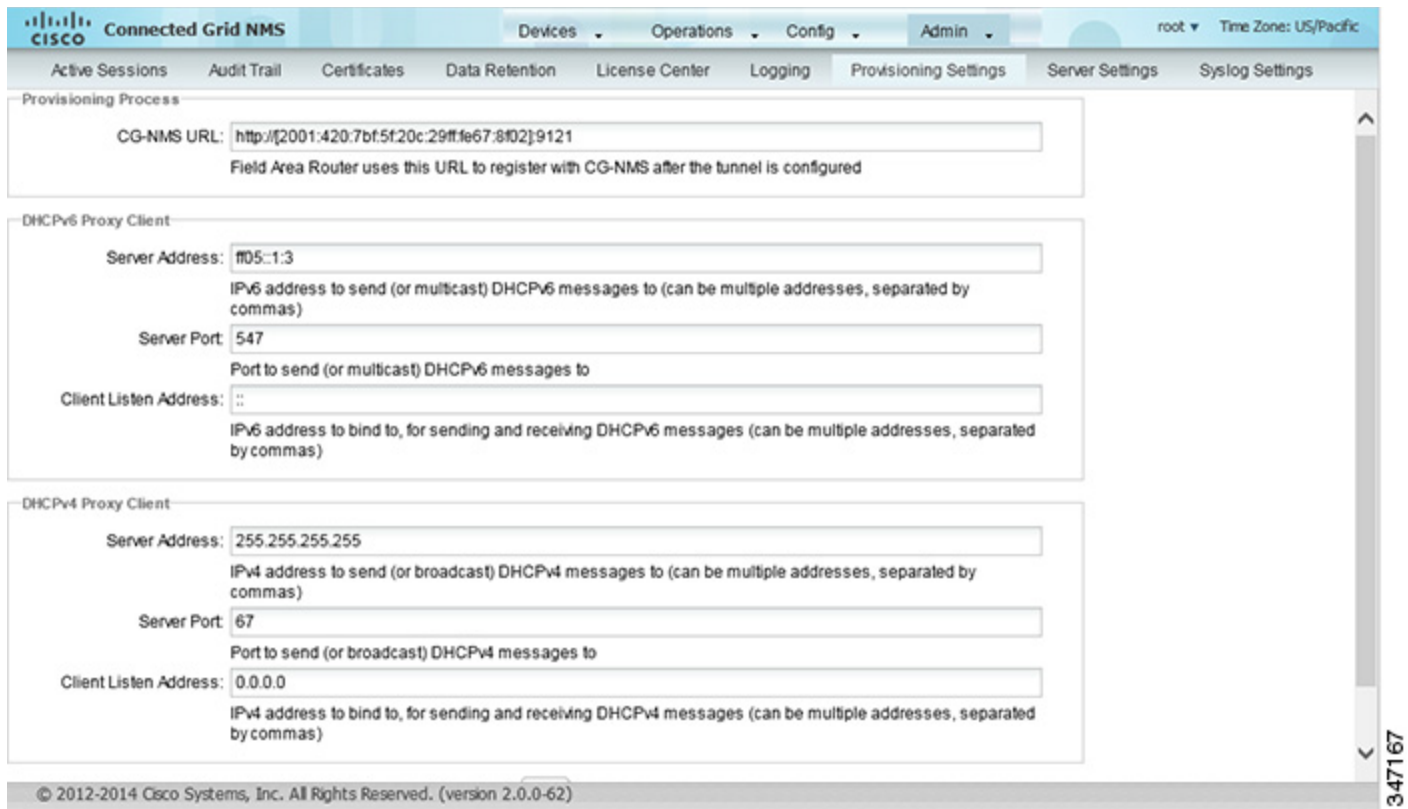
This section provides the following topics for configuring tunnel settings:

- Configuring the CG-NMS Server URL

- Configuring DHCPv6 Proxy Client

- Configuring DHCPv4 Proxy Client

Configuring the CG-NMS Server URL

The CG-NMS URL is the URL that FARs use to access with CG-NMS after the tunnel is established. This URL is also accessed during periodic inventories. During ZTD, FARs transition from accessing CG-NMS through the TPS proxy to using this URL, which must be appropriate for use through the tunnel.

To configure the CG-NMS URL:

1. Choose **Admin > System Management > Provisioning Settings**.

2. In the **CG-NMS URL** field, enter the URL of the CG-NMS server.

   The URL must use the HTTPS protocol and include the port number designated to receive registration requests. By default, the port number is 9121. For example:

   ```
   https://nms.sgbu.example.com:9121
   ```

3. Click **Save**.

Configuring DHCPv6 Proxy Client

To configure DHCPv6 Proxy Client settings:

1. Choose **Admin > System Management > Provisioning Settings**.

2. Configure the DHCPv6 Proxy Client settings:

   a. In the **Server Address** field, enter the address of the DHCPv6 server that provides tunnel IP addresses.

   You can enter multiple addresses separated by commas. However, in most cases, you only need one server. CG-NMS tries to get the tunnel IP addresses using DHCP protocols. If it cannot, it goes to the next server in the list and so on.

   b. In the **Server Port** field, enter the port address on the DHCP server to send DHCPv6 requests.

   Note: Do not change the default port number (547) unless you have configured your DHCP server to operate on a non-standard port.

   c. In the **Client Listen Address** field, enter the address to bind to for DHCPv6 send and receive messages.

   This is the address of the interface that the DHCP server uses to communicate with CG-NMS. You can enter multiple backup addresses separated by commas.

   Tip: For CG-NMS installations where the host has multiple interfaces, the client sends requests using each listed source address. The default values, "0.0.0.0" (IPv4) and "::" (IPv6), cause the client to send requests out each interface. Usually, one interface faces the DHCP server(s). In these installations, setting the **Client Listen Address** field to the IP address of the facing interface sends all client requests out that interface.

3. Click **Save**.

Configuring DHCPv4 Proxy Client

To configure DHCPv4 Proxy Client settings:

1. Choose **Admin > System Management > Provisioning Settings**.

2. Configure the DHCPv4 Proxy Client settings:

   a. In the **Server Address** field, enter the address of the DHCPv4 server that provides tunnel IP addresses.

   You can enter multiple addresses separated by commas. However, in most cases, you only need one server. CG-NMS tries to get the tunnel IP addresses from the first server in the list. If it cannot, it moves to the next server in the list, and so on.

   b. In the **Server Port** field, enter the port address on the DHCP server to send DHCPv4 requests to.

   Note: Do not change the default port number (67) unless you have configured your DHCP server to operate on a non-standard port.

   c. In the **Client Listen Address** field, enter the address to bind to for send and receive DHCPv4 messages.

   This is the address of the interface that the DHCP server uses to communicate with CG-NMS. You can enter multiple backup addresses separated by commas.

3. Click **Save**.

Configuring Server Settings

The Server Settings page (**Admin > System Management > Server Settings**) lets you view and manage server settings.

- Configuring Download Logs Settings

- Configuring Web Sessions

- Configuring Device Down Timeouts

- Configuring Billing Period Settings

- Configuring RPL Tree Polling

- Configuring the Issue Status Bar

Configuring Download Logs Settings

Note: Configuring download log settings is only required for CG-NMS cluster setup.

The Download Logs page lets you configure the Keystore settings.

To configure Download Logs settings:

1. Choose **Admin > System Management > Server Settings**.

2. Click the **Download Logs** tab.
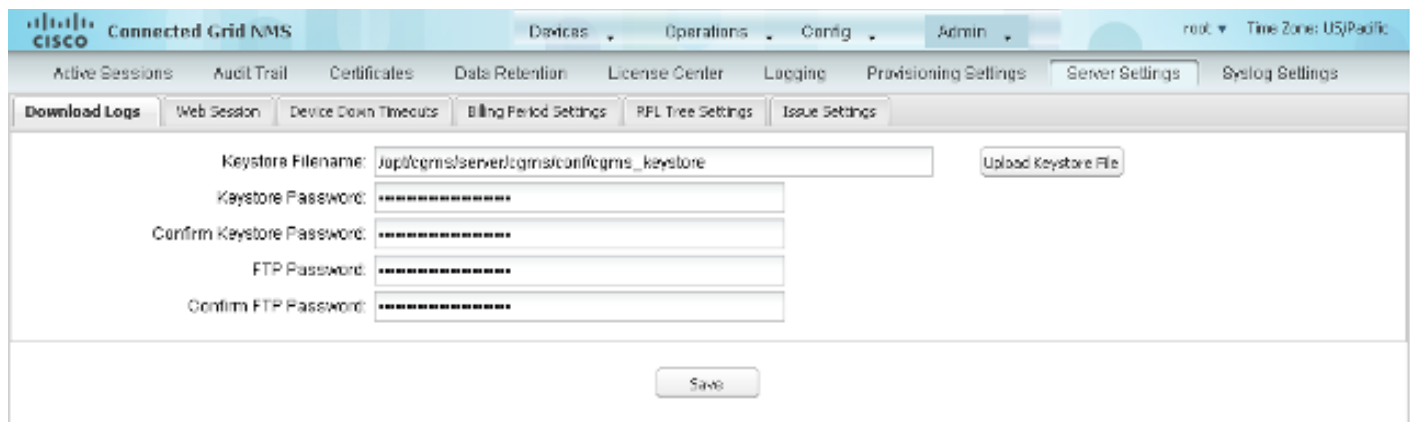
3. Configure these settings:

Table 7   Keystore Settings

Field	Description
Keystore Filename	Click **Upload Keystore File** to upload a Keystore file with the public key of the X.509 certificate that CG-NMS uses. You can reuse the same Keystore file.
Keystore Password	Enter the password that CG-NMS uses to access the Keystore file on start up.
Confirm Keystore Password	
FTP Password	Enter the FTP password.
Confirm FTP Password	
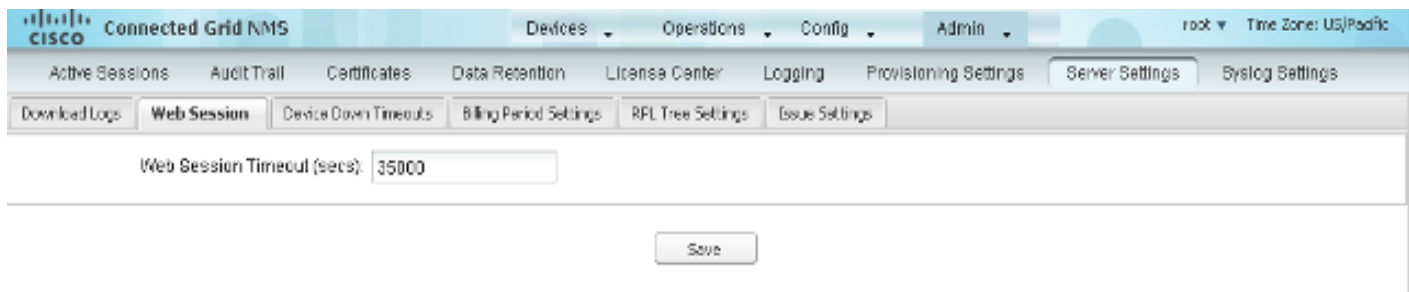
4. Click **Save**.

Configuring Web Sessions

The Web Sessions page lets you specify the number of timeout seconds after which CG-NMS terminates web sessions and logs users out.

To configure web session timeout:

1. Choose **Admin > System Management > Server Settings**.

2. Click the **Web Session** tab.

3. Enter the number of timeout seconds. Valid values are 0–86400 (24 hours).

If a web session is idle for the specified amount of time, CG-NMS terminates the session and logs the user out.

4. Click **Save**.

Configuring Device Down Timeouts

The Device Down Timeouts page lets you specify the number of timeout seconds after which the status of ASRs, FARs, and MEs changes to Down in CG-NMS. The device down poll interval is five minutes, and uses the device down timeouts values and the last heard time to decide whether to change the device status to Down. For example, if the FAR device down timeout value is set to two hours (7200 seconds), all FARs with a last heard time older than 2 hours are marked as status Down. You can also configure the device timeout setting for FAR Config groups.

Device status changes to Up when CG-NMS detects any of the following:

- Periodic inventory notifications

- Events

- Manual metric refreshes

- Device registrations

To configure device down timeout settings:

1. Choose **Admin > System Management > Server Settings**.

2. Click the **Device Down Timeouts** tab.
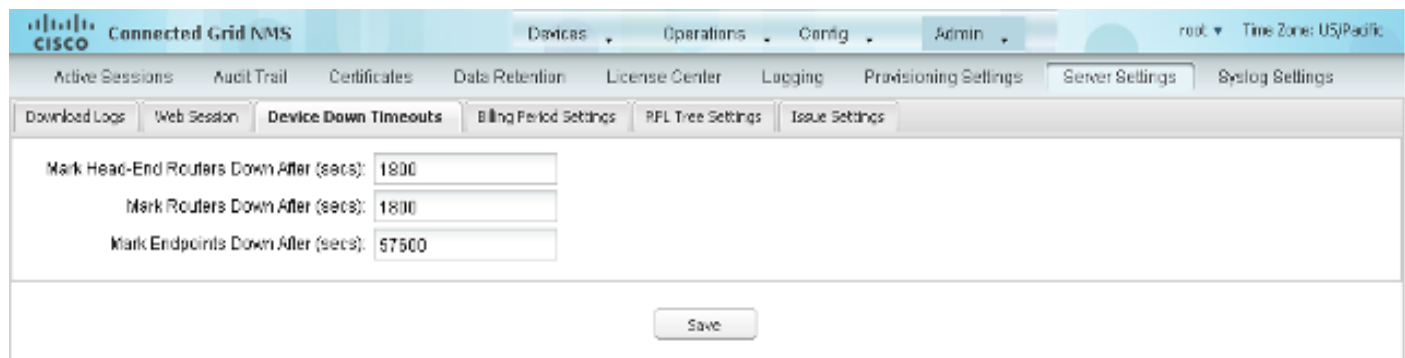
3. For each device type listed, enter the number of seconds after which the device status changes to Down in CG-NMS.

This value must be greater than the corresponding polling intervals. For example, the default polling interval for endpoints is 8 hours (28800 seconds), so the value in the Mark Mesh Endpoints Down After (secs) field must be greater than 28800.

4. Click **Save**.

Device Down Timeout Settings for FAR Config Groups

To configure device down timeout settings for FAR Config groups:

1. Choose **Config > Device Configuration**.

2. Under **ROUTERS** in the left pane, choose the FAR Config group to configure.

3. Click the **Group Properties** tab.
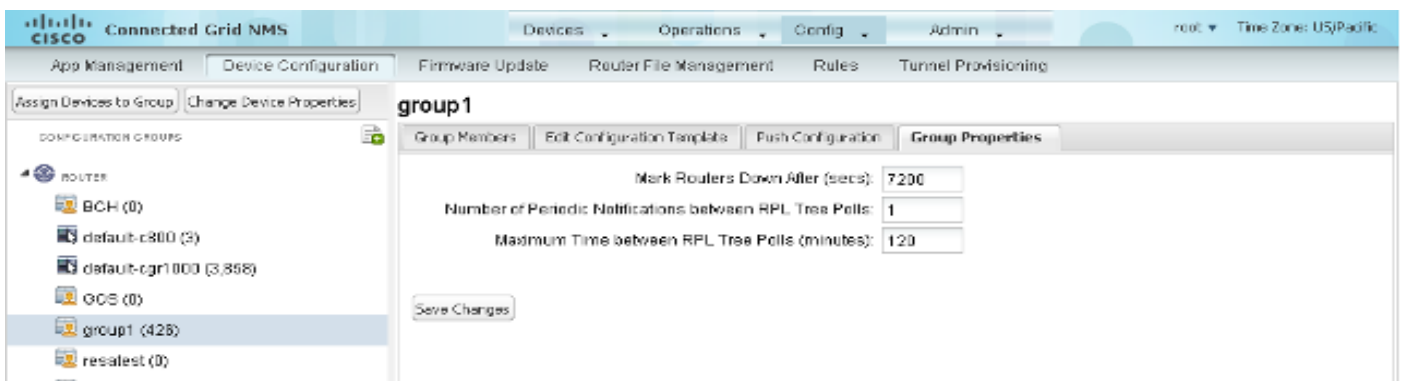
4. In the **Mark Routers Down After (secs)** field, enter the number of seconds after which the status of devices in the group changes to Down in CG-NMS.

This value must be greater than the corresponding polling interval. For example, the default polling interval for FARs is 30 minutes (1800 seconds), so the value in the Mark Routers Down After (secs) field must be greater than 1800.

5. Click **Save Changes**.

Configuring Billing Period Settings

CG-NMS lets you configure the start day of the monthly billing periods for cellular and Ethernet (satellite) services.

To configure the billing period settings:

1. Choose **Admin > System Management > Server Settings**.

2. Click the **Billing Period Settings** tab.

3. Enter the starting days for the cellular and Ethernet billing periods.

4. From the drop-down menu, choose the time zone for the billing period.

5. Click **Save**.

Configuring RPL Tree Polling

RPL tree polls are derived from FAR periodic notification events. Since the RPL tree is not pushed from the FAR with the periodic notification event, CG-NMS must explicitly poll for the RPL tree at the configured intervals. CG-NMS lets you configure the RPL tree polling cycle (that is, how many periodic notification events occur between RPL tree polls), and set the maximum amount of time between tree polls.

Caution: CG-NMS 1.1(5) release does not support router RPL tree updates. Do not enable RPL tree updates from Routers.

To configure RPL tree polling settings:

1. Choose **Admin > System Management > Server Settings**.

2. Choose the **RPL Tree Settings** tab.

3. Choose the **Enable RPL tree update from** radio button for Mesh Nodes or CGR devices to receive the RPL tree update from those devices at the specified intervals.

128

4. For Router polling, enter the number of events that pass between RPL tree polling intervals in the **Number of Periodic Notification RPL Tree Polls** field.

   ■ The default value is 8.

      Note: If thresholds are exceeded during periodic notification events, CG-NMS performs a RPL tree poll.

5. In the **Maximum Time between RPL Tree Polling (minutes)** field, enter the maximum amount of time between tree polls in minutes.

   ■ The default value is 480 minutes (8 hours).

6. Click **Save**.

Configuring the Issue Status Bar

The Issue Status bar displays issues by device type (as set in user preferences; see Setting User Preferences) and severity level in the lower-left browser frame.

To enable the Issue Status bar and configure the refresh interval:

1. Choose **Admin > System Management > Sever Settings > Issue Settings**.
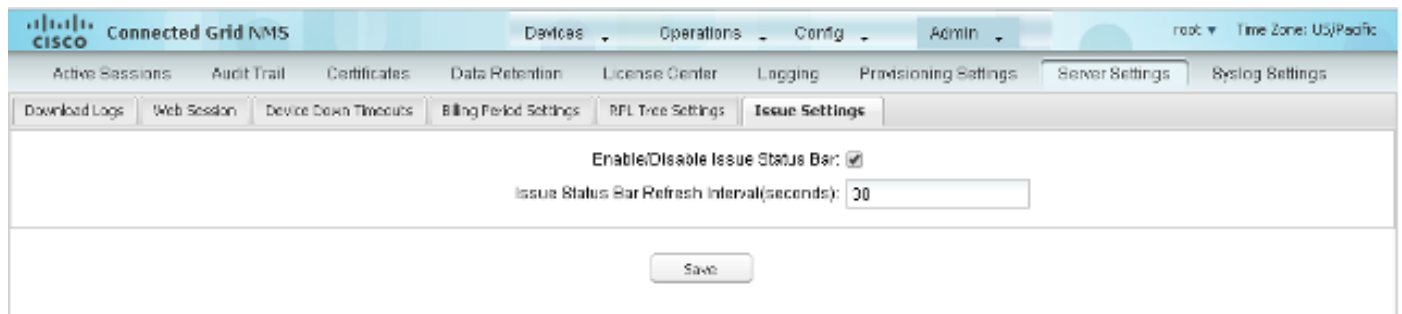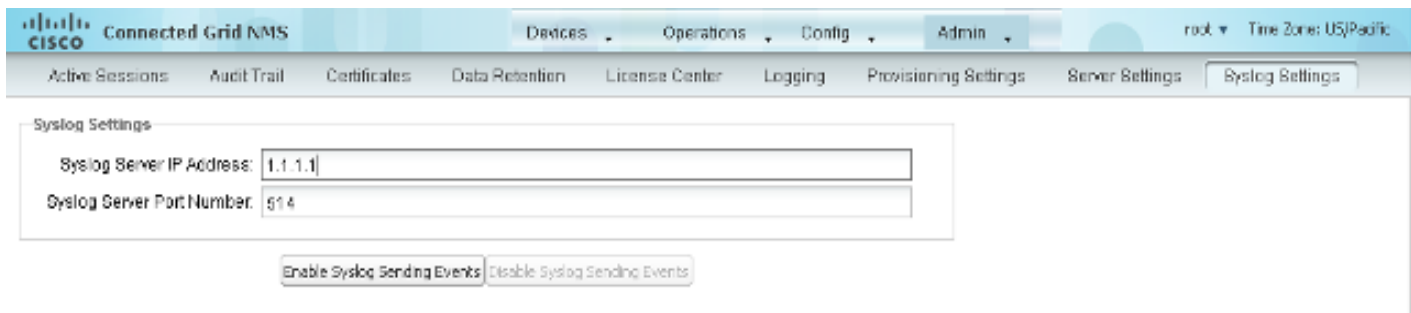
2. To display the Issue status bar in the browser frame, check the **Enable/Disable Issue Status Bar** check box.

3. In the Issue **Status Bar Refresh Interval** field, enter a refresh value in seconds.

   ■ Valid values are 30 secs (default) to 300 secs. (5 minutes).

Managing the Syslog

When CG-NMS receives device events it stores them in its database and sends syslog messages to a syslog server that allows third-party application integration.

To configure Syslog forwarding:

1. Choose **Admin > System Management > Syslog Settings**.

2. In the **Syslog Server IP Address** field, enter the IP address of the Syslog server.

3. In the **Syslog Server Port Number** field, enter the port number (default is 514) over which to receive device events.

- To enable message forwarding to the Syslog server, click **Enable Syslog Sending Events**.
- To disable message forwarding to the Syslog server, click **Disable Syslog Sending Events**.

For CG-NMS cluster solutions, each server in the cluster sends events to the same Syslog server.

Managing Devices

This chapter describes how to manage devices in CG-NMS:

- Overview

- Managing Routers

- Managing Mesh Endpoints

- Managing Head-End Routers

- Managing Servers

- Common Device Operations

- Configuring Rules

- Configuring Devices

- Managing a Guest OS

- Managing Work Orders

- Device Properties

Overview

CG-NMS has the following pages to monitor, add, and remove devices, and perform other device management tasks that do not include device configuration:

- To work with FARs and MEs, use the Field Devices page (**Devices > Field Devices**).

- To work with HERs, use the Head-End Routers page (**Devices > Head-End Routers**).

- To work with database and NMS servers, use the Servers page (**Devices > Servers**).

- To configure the device properties of routers and MEs, use the Device Configuration page (**Config > Device Configuration**).

Managing Routers

You manage routers on the Field Devices page (**Devices > Field Devices**). By default, the page displays devices in Default view. This section includes the following topics:

- Working with Router Views

- Creating Work Orders

- Using Router Filters

- Refreshing the Router Mesh Key

- Using Router Filters

- Displaying Router Configuration Groups

- Displaying Router Firmware Groups

- Displaying Router Tunnel Groups

131

Working with Router Views

Unless you select the **Default to map view** option in user preferences (see Setting User Preferences), the Field Devices page defaults to List view, which contains basic device properties. Select a router or group of routers in the Browse Devices pane to display tabs in the main pane that display the following router properties:

- Cellular-GSM

- Cellular-CDMA

- WiMAX

- Mesh

- Physical

- Config

- Firmware

- Tunnel

- DHCP Config

Each of these views displays different sets of device properties. For example, the Default view displays basic device properties, and the Cellular-GSM view displays device properties particular to the cellular network.

For information on how to customize router views, see Customizing Device Views.

For information about the device properties that display in each view, see Device Properties.

For information about common actions performed in these views (for example, adding labels and changing device properties), see Common Device Operations.

Viewing Routers in Map View

To view routers in Map view, check the **Enable map** check box in **<user> > Preferences**, and then click the **Map** tab in the main pane (see Setting User Preferences). You can view any RPL tree by clicking the device in Map view, and closing the information popup window. The RPL tree connection displays data traffic flow as blue or orange lines, as follows:

- Orange lines indicate that the link is an uplink: data traffic flows in the up direction on the map

- Blue lines indicate that the link is a downlink: data traffic flows in the down direction on the map

Figure 1   Map View: Downlink Data Flow RPL Trees
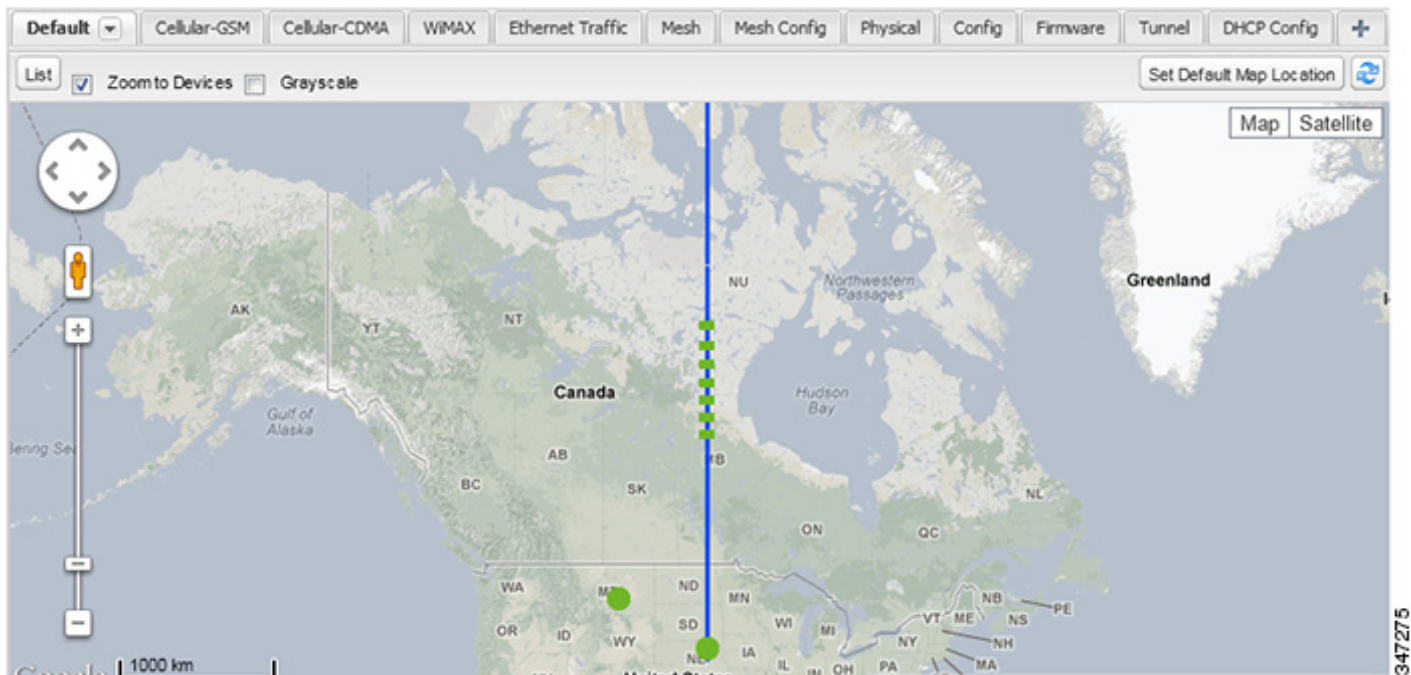
Creating Work Orders

Create work orders in CG-NMS to deploy field technicians for device inspections. Field technicians use the CGDM client to connect to CG-NMS and download the work order.

Note: The Work Orders feature works with Release 3.0 or later of Device Manager (CGDM) only. See *"Accessing Work Authorizations"* in the *Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1* for integration instructions for CG-OS installations. For Cisco IOS installations, please refer to the *Cisco Connected Grid Device Manager Installation and User Guide, Release 4.0*.

Note: Before you can create a work order, your user account must have Work Order Management permissions enabled. See Managing Roles.

To create work orders for FARs, select a router or group of routers in the Browse Devices pane, and then in Default view:

1. Check the check box of the faulty FAR.

2. Choose **More Actions > Create Work Order**.
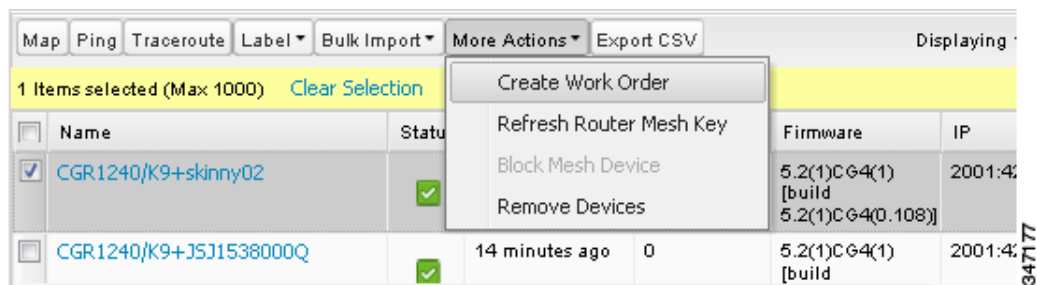
The Work Orders page appears (**Config > Device Configuration > Work Orders**). On that page, CG-NMS adds the names of the selected FARs to the List of FAR Names field as a comma-separated list.

133

3. Follow the steps in Creating Work Orders to create the work order.

For more information about work orders, see Managing Work Orders.

Refreshing the Router Mesh Key

If you suspect unauthorized access attempts to a FAR, refresh its mesh key.

Caution: Refreshing the router mesh key can result in MEs being unable to communicate with the FAR for a period of time until the MEs re-register with the FAR, which happens automatically.

To refresh the router mesh key, select a router or group of routers in the Browse Devices pane, and then in Default view:

1. Check the check boxes of the of the FARs to refresh.

2. Choose **More Actions > Refresh Router Mesh Key** from the drop-down menu.

3. Click **Yes** to continue.

Using Router Filters

To refine the list of displayed routers, use the built-in router filters under ROUTERS in the Browse Devices pane or saved custom searches in the Quick View pane (left pane). For example, to display all operational FARs, click the **Up** group under ROUTERS in the Browse Devices pane. Click a filter to insert the corresponding search string in the Search Devices field. For example, clicking the **Up** group under ROUTERS inserts the search string **status:up** in the Search Devices field.

Displaying Router Configuration Groups

Use the Browse Devices pane to display the router devices that belong to one of the groups listed under ROUTERS.

Displaying Router Firmware Groups

Use the Browse Devices pane to display the router devices that belong to one of the groups listed under ROUTER FIRMWARE GROUPS.

Displaying Router Tunnel Groups

Use the Browse Devices pane to display the router devices that belong to one of the groups listed under ROUTER TUNNEL GROUPS.

Managing Mesh Endpoints

To manage MEs, view the **Devices > Field Devices** page. By default, the page displays the MEs in List view. This section includes the following topics:

- Viewing Mesh Endpoints in Default View

- Viewing Mesh Endpoints in Map View

- Blocking Mesh Devices

- Displaying Mesh Endpoint Configuration Groups

- Displaying Mesh Endpoint Firmware Groups

Viewing Mesh Endpoints in Default View

When you open the Field Devices page in Default view, CG-NMS lists all FAN devices and basic device properties. When you select an ENDPOINT device or group in the Browse Devices pane, CG-NMS provides tabs to display additional ME property views:

- RF Mesh

- PLC Mesh

- Security

- Config

- Firmware

Each one of these views displays different sets of device properties. For example, the Firmware view displays the device properties that fall under the firmware category, such as Hardware ID, Firmware Group, and FW Uploaded Version.

For information on how to customize ME views, see Customizing Device Views.

For information about the device properties displayed in each view, see Device Properties.

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see Common Device Operations.

Viewing Mesh Endpoints in Map View

To view MEs in Map view, select Enable map in *<user>* **> Preferences**, and click the **Map** tab.

Blocking Mesh Devices

If you suspect unauthorized access attempts to a mesh device, block it from accessing CG-NMS.

Caution: If you block an ME, you cannot unblock it using CG-NMS. To re-register the ME with CG-NMS, you must escalate and get your ME administrator involved.

To block an ME device, in Default view:

1. Check the check boxes of the mesh devices to refresh.

2. Choose **More Actions > Block Mesh Device** from the drop-down menu.
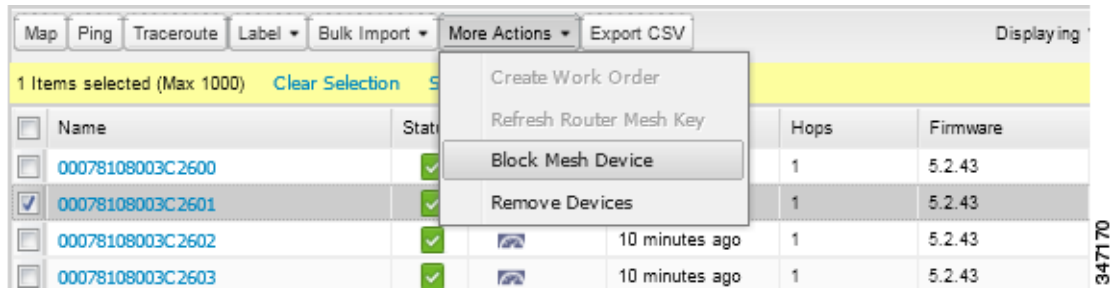
3. Click **Yes** in the Confirm dialog box.

Displaying Mesh Endpoint Configuration Groups

You can use the Browse Devices pane to display the ME devices that belong to one of the groups listed under MESH DEVICE CONFIGURATION GROUPS.

Displaying Mesh Endpoint Firmware Groups

You can use the Browse Devices pane to display the ME devices that belong to one of the groups listed under ENDPOINTS.

Managing Head-End Routers

To manage head-end routers (HERs), open the Head-End Routers page by choosing **Devices > Head-End Routers** (Figure 2). Unless Enable Map is selected in user preferences, by default, the page displays the HERs in List view. When you open the Head-End Routers page in List view, CG-NMS displays the Default list view. This view displays basic HER device properties. In addition, CG-NMS provides these tabs to display additional HER property views:

■ Tunnel 1

■ Tunnel 2

Each one of these views displays different sets of device properties. These views display information about the HER tunnels.

Figure 2   Head-End Routers Page
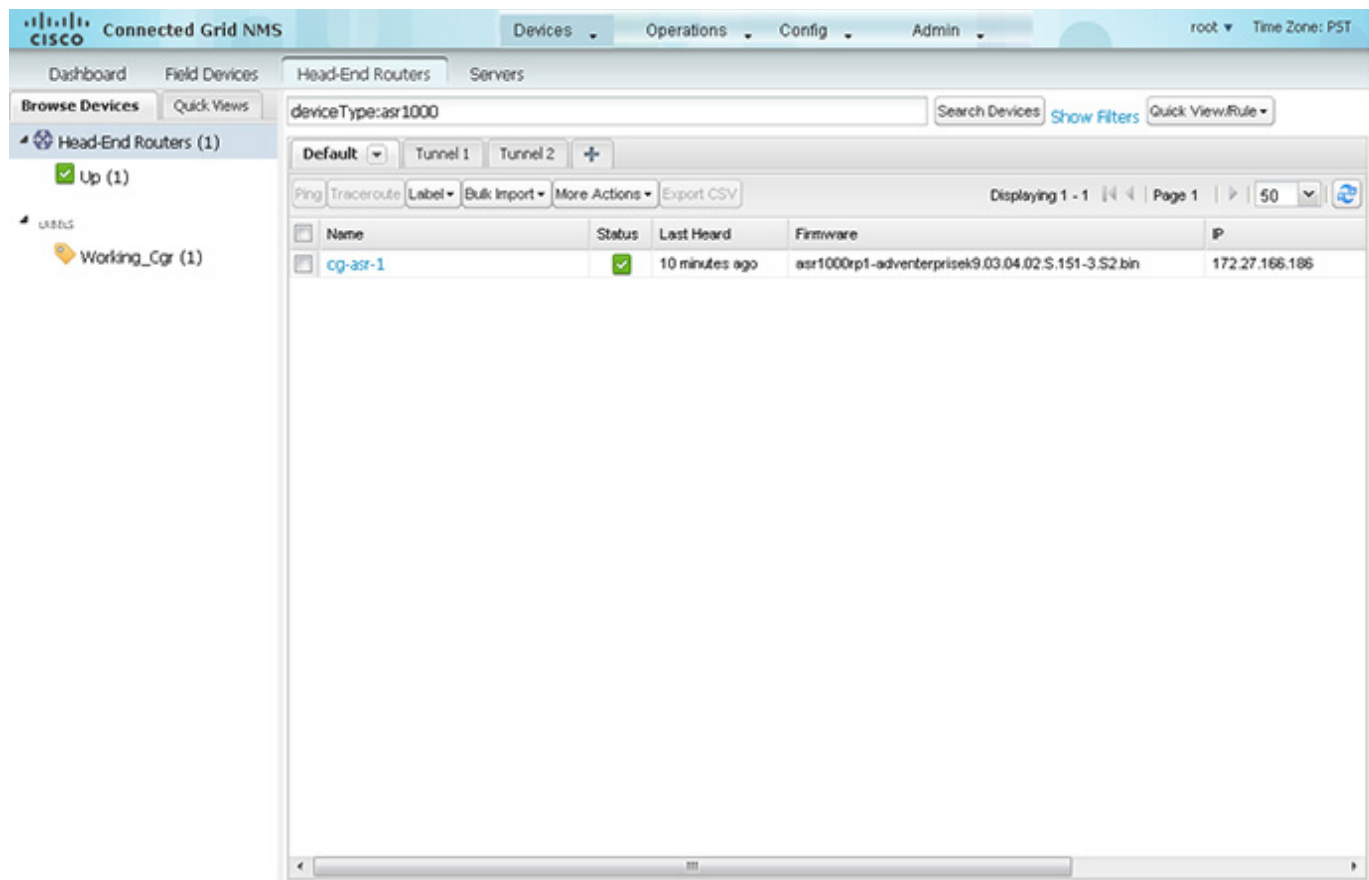
For information on how to customize HER views, see Customizing Device Views.

For information about the device properties displayed in each view, see Device Properties.

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see Common Device Operations.

Managing Servers

To manage servers, open the Servers page by choosing **Devices > Servers**. By default, the page displays the servers in List view. When you open the Servers page in List view, CG-NMS displays the Default list view. This view displays basic server device properties. To obtain information about a server, click its name.

To add additional views, see Customizing Device Views.

For more information about the device properties displayed in each view, see Device Properties.

For information about the common actions in this view, see Common Device Operations.

Managing NMS Servers

In the Browse Devices pane, NMS servers appear under NMS Servers. In single-NMS server deployments, only one server appears under NMS Servers. In cluster deployments, multiple NMS servers appear under NMS Servers. To filter the list pane:

- To display all NMS servers, click **NMS Servers** in the Browse Devices pane.

- To display only operational servers, click **Up**.

- To display only non-operational servers, click **Down**.

Managing Database Servers

In the Browse Devices pane, CG-NMS database servers appear under Database Servers. In single-server deployments, only one database server appears under Database Servers. If a secondary database is configured, it also appears under the same entry.

- To display all database servers in List view, click **Database Servers** in the Browse Devices pane.

- To only display servers that are operational, click **Up**.

- To only display servers that are non-operational, click **Down**.

Common Device Operations

This section describes how to use CG-NMS to manage and view information about devices, and includes the following topics:

- Selecting Devices

- Customizing Device Views

- Viewing Devices in Map View

- Configuring Map Settings

- Changing the Sorting Order of Devices

- Exporting Device Information

- Pinging Devices

- Tracing Routes to Devices

- Managing Device Labels

- Removing Devices

- Displaying Detailed Device Information

- Using Filters to Control the Display of Devices

- Performing Bulk Import Actions

Selecting Devices

In List view, CG-NMS lets you select devices on a single page and across pages. When you select devices, a yellow bar displays that maintains a count of selected devices and has the **Clear Selection** and **Select All** commands. The maximum number of devices you can select is 1000. Perform the following to select devices:

- To select devices across all pages, click **Select All**.

- To select all devices listed on a page, check the check box next to **Name**.

- To select a group of devices, check the check boxes of individual devices listed on a page and across pages. The count increments with every device selected, and selections on all pages are retained.

Customizing Device Views

CG-NMS lets you customize device views. For List views you can:

- Add and delete tabs

- Specify the properties to display in the columns for each view (see Device Properties by Category for available properties)

- Change the order of columns

Adding Device Views

To add a custom device view tab to a device page in list view:

1. Click the + tab.

2. In the **Add New View** dialog box, enter the name of the new tab.
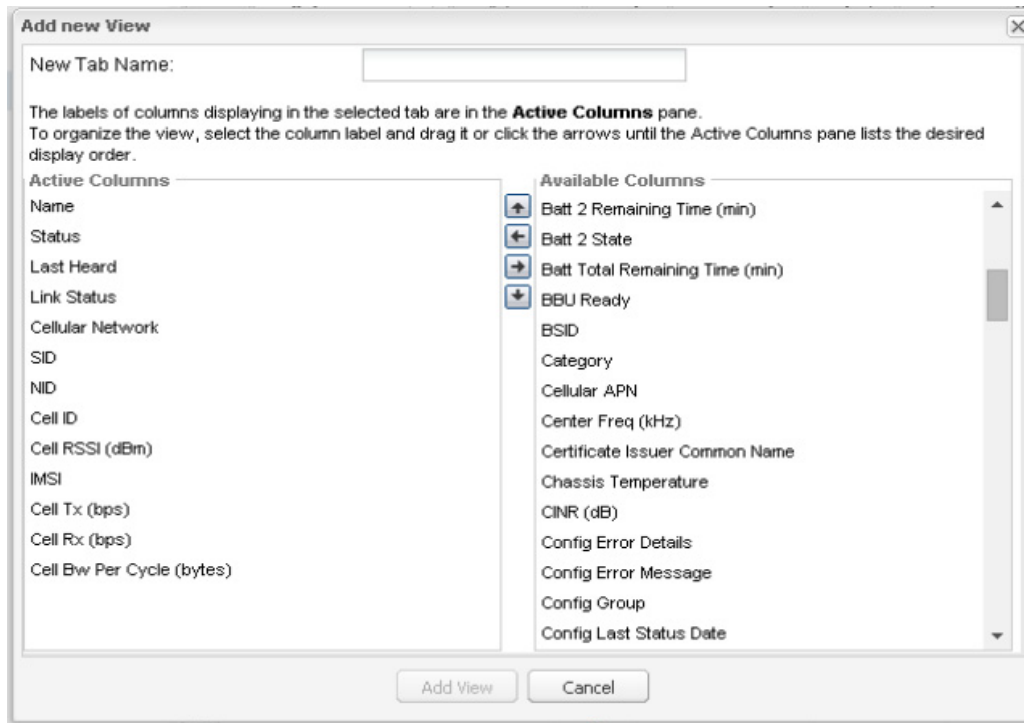
3. Add properties to the Active Columns list by selecting them from the Available Columns list, and then clicking the left arrow button, or dragging them into the Active Columns list.

  ■ To change column order, use the up and down arrow buttons or drag them to the desired position.

  ■ To remove properties from the Active Columns list, select those properties and click the right arrow button, or drag them out of the list.

  Tip: Hold the Shift key to select multiple column labels and move them to either list.

4. Click **Save View**.

Editing Device Views

To edit a device view:

1. Click the drop-down arrow on the desired tab.

2. In the Edit/Delete View dialog box:

  a. To remove properties from the Active Columns list, select those properties and click the right-arrow button or drag them out of the Active Columns list.

  b. To add properties to the Active Columns list, select those properties from the Available Columns list and click the left-arrow button, or drag them into position in the Active Columns list.

  c. To change the sort order of the active columns, use the up- and down-arrow buttons, or drag them to the desired position.

Common Device Operations
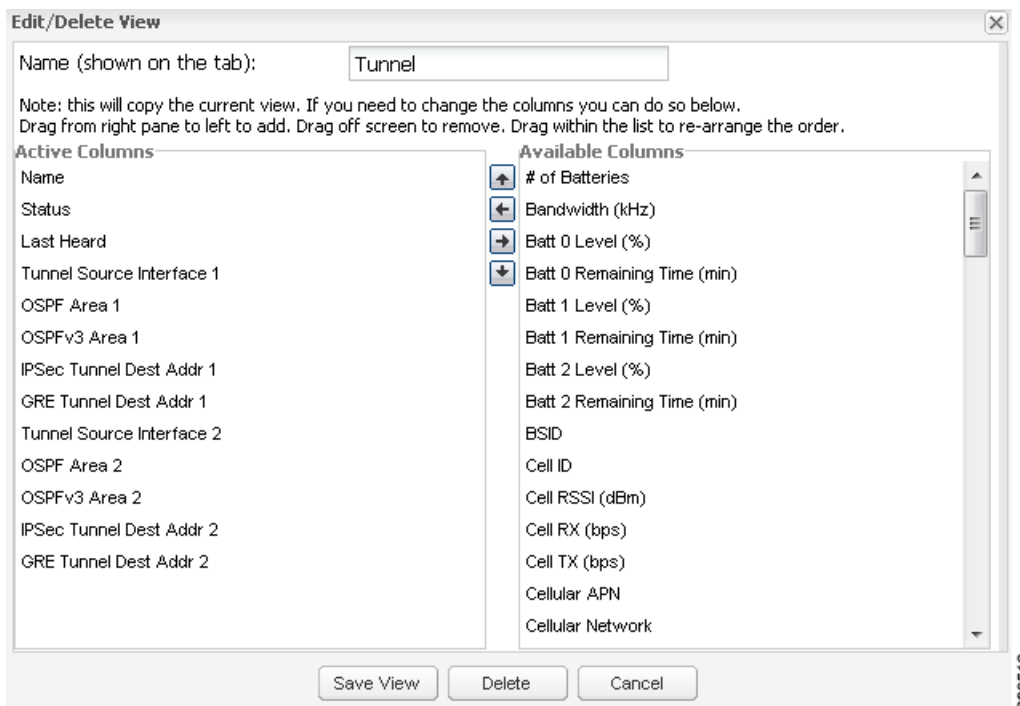
3. Click **Save View**.

Deleting Device Views

To delete a device view:

1. Click the arrow on the tab of the device view to delete.
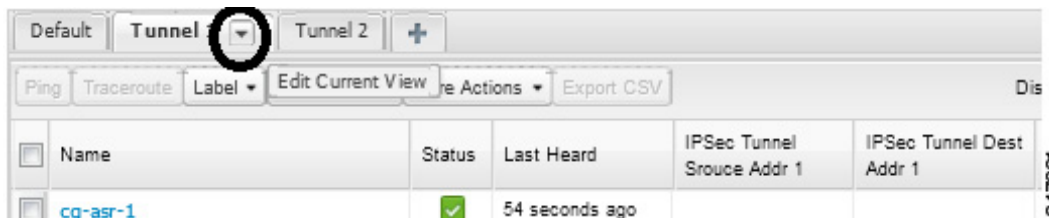
2. In the Edit/Delete View dialog box, select the desired label in the Active Columns pane.

Edit/Delete View ⊠

Name (shown on the tab): | Tunnel

Note: this will copy the current view. If you need to change the columns you can do so below.
Drag from right pane to left to add. Drag off screen to remove. Drag within the list to re-arrange the order.

Active Columns		Available Columns
Name	⬆	# of Batteries
Status	⬅	Bandwidth (kHz)
Last Heard	➡	Batt 0 Level (%)
Tunnel Source Interface 1	⬇	Batt 0 Remaining Time (min)
OSPF Area 1		Batt 1 Level (%)
OSPFv3 Area 1		Batt 1 Remaining Time (min)
IPSec Tunnel Dest Addr 1		Batt 2 Level (%)
GRE Tunnel Dest Addr 1		Batt 2 Remaining Time (min)
Tunnel Source Interface 2		BSID
OSPF Area 2		Cell ID
OSPFv3 Area 2		Cell RSSI (dBm)
IPSec Tunnel Dest Addr 2		Cell RX (bps)
GRE Tunnel Dest Addr 2		Cell TX (bps)
		Cellular APN
		Cellular Network

[Save View] [Delete] [Cancel]

390512

3. Click **Delete**.

Viewing Devices in Map View

CG-NMS provides a map view for visualizing device information based on geographic location. In Map view, CG-NMS displays a Geographic Information System (GIS) map and uses GIS Map services to show device icons on the map based on the latitude and longitude information of the device. When this information is not defined for a device, CG-NMS does not display the device on the map.

Common Device Operations

To view devices in Map view:

1. Choose *<user>* **> Preferences**, check the **Enable map** check box, and click **Apply**.
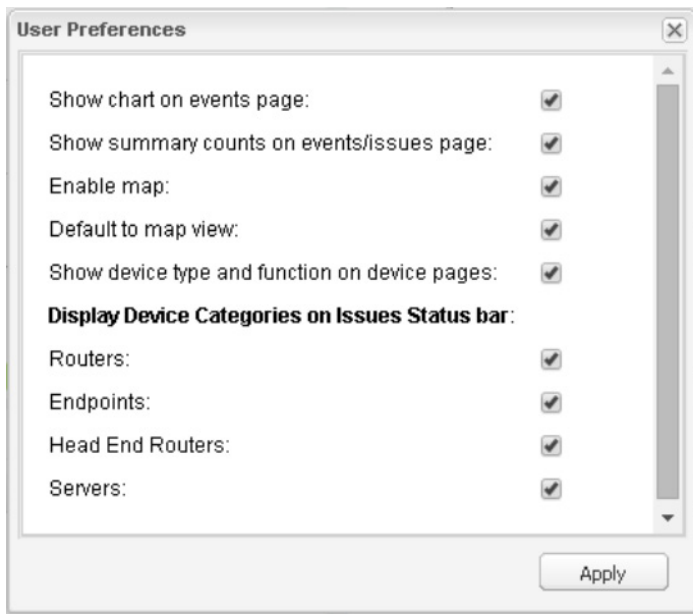
2. Choose **Devices > Field Devices**.

3. Click the **Map** tab.

   By default, CG-NMS displays all devices registered in its database on the map. Depending on the zoom level of the map and the device count, individual device icons might not display. Instead, CG-NMS displays device group icons.

Common Device Operations
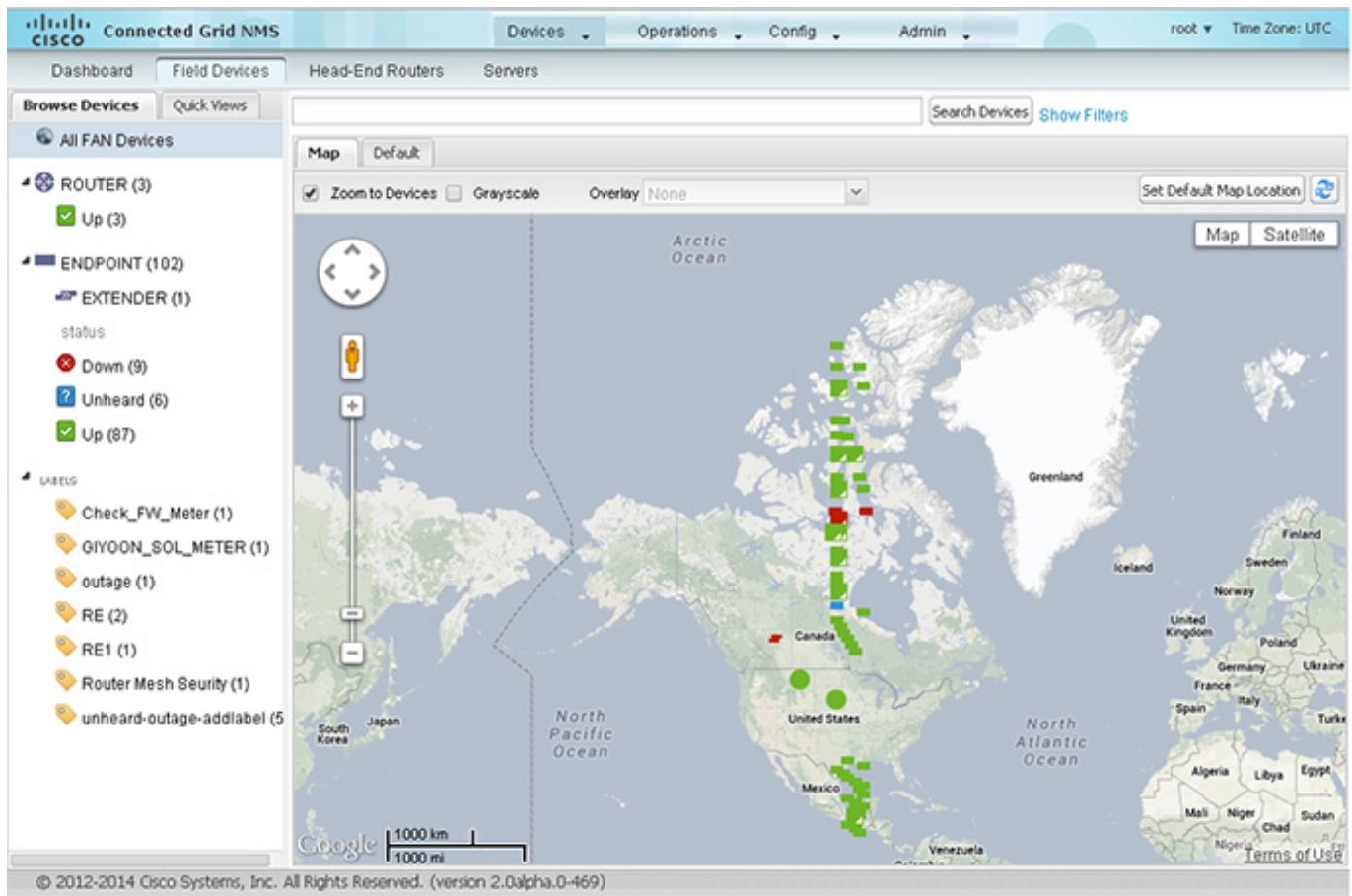
To view individual devices, zoom in until the device icons appear. You can also click on a device to display a pop-up window that includes the **Zoom In** link to move the map display to the device level.

Common Device Operations
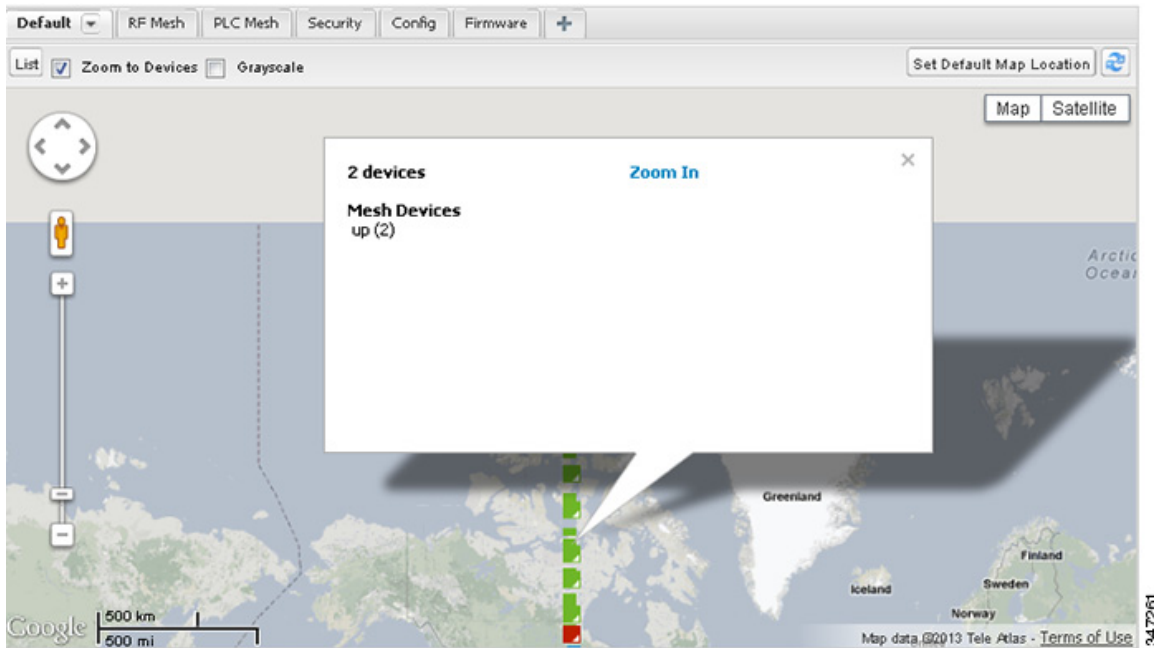
CG-NMS displays the device count next to each device group or category in the Browse Devices pane (left pane).

- To display a subset of all devices, click one of the filters listed in the Browse Devices pane.

  CG-NMS changes the map region based on your selection and displays the devices found by the filter. For example, you can use the **Routers > Up** filter to display all FARs that are up and running. You can also use saved custom filters in the Quick View pane (left pane) to filter the device view. For information about creating custom filters, see Creating a Quick View Filter.

- To display information about a device or group, click its icon on the map.

145

Common Device Operations
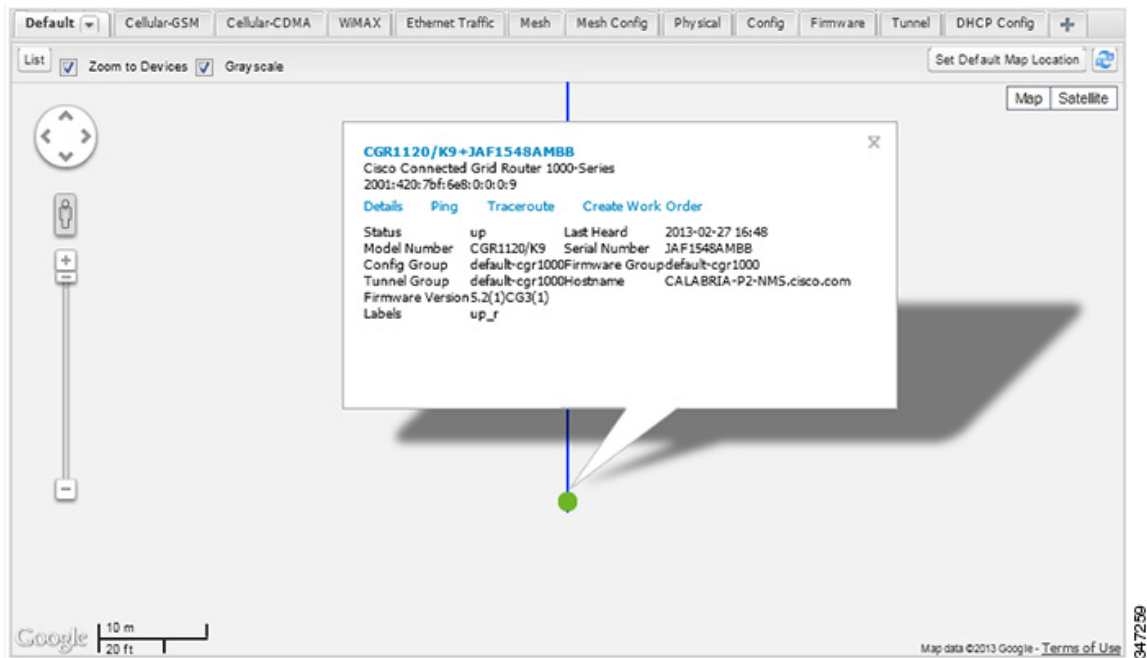
A popup window displays listing basic device or group information.

- To view device specifics, click **Details** or the device EID link in the Device popup window.

You can also ping the device, perform a trace route, and create a work order from this window.

4. Close the Device popup window to view the RPL tree associated with the device. See Configuring RPL Tree Polling
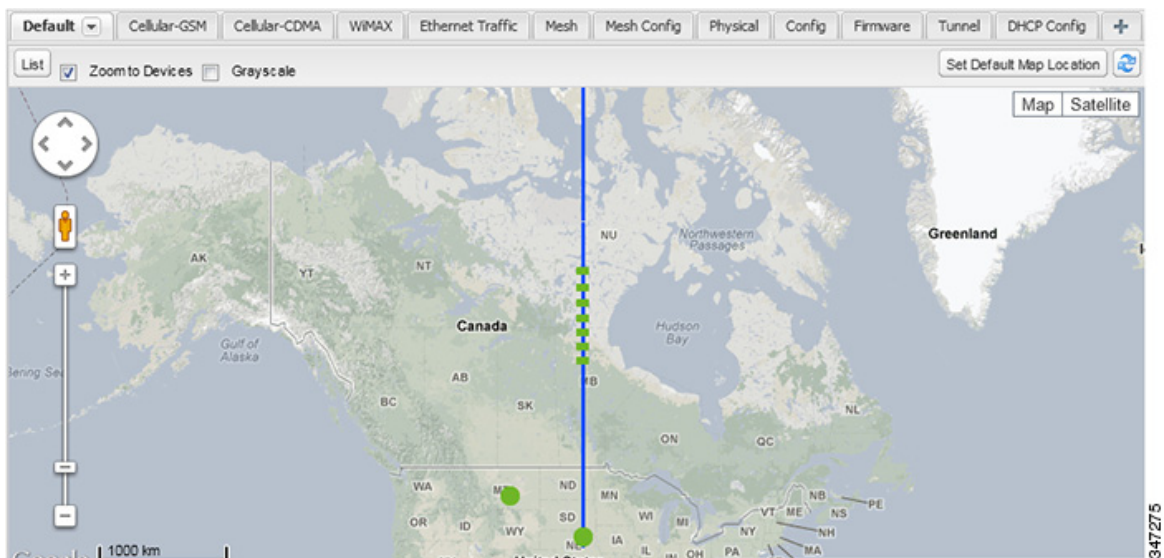
The RPL tree connection displays as blue or orange lines; where blue indicates that the link is down, and orange indicates that the link is up.

5. Click the refresh button (C) to update the Map view.

Configuring Map Settings

In Map view, CG-NMS lets you configure these settings for maps:

- Automatically zoom to devices

- Display the map in grayscale

- Default map location (set to North America by default)

To configure map settings:

1. Choose **Devices > Field Devices**.

2. Click the **Map** tab.

    - To automatically zoom to devices, check the **Zoom to Devices** check box.
    - To display the map in grayscale, check the **Grayscale** check box.
    - To overlay all associated wireless personal area network (WPAN) endpoints on the map, select **Associated WPAN Endpoints** from the Overlay drop-down menu.
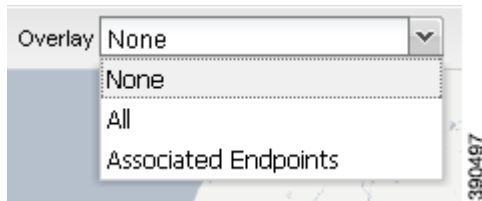
    - To set the map location to always open to a certain area, display the area of the map to display by default, and then click **Set Default Map Location** (top right).

3. Click **OK**.

Changing the Sorting Order of Devices

To change the sorting order of devices, click the right side of the column heading and choose a sort command from the drop-down menu.
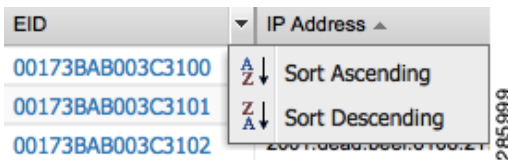
Exporting Device Information

CG-NMS lets you export the device properties of the selected devices in List view. CG-NMS exports only properties in the current view.

To export device information displayed in the current view, in List view:

1. Select the devices to export by checking their corresponding check boxes.

2. Click **Export CSV**.

   3. Click **Yes** in the confirmation dialog box.

CG-NMS creates a CSV file, export.csv, containing the information displayed in the List view pane. By default, CG-NMS saves this file to your default download directory. When a file with the same name exists, CG-NMS adds a number to the default filename (for example, export-1.csv and export-2.csv).

The export.csv file consists of one header line defining the exported fields followed by one or more lines, each representing a device. Here is an example of an export of selected devices from the Routers page:

```
name,lastHeard,meshEndpointCount,uptime,runningFirmwareVersion,openIssues,labels,lat,lng
CGR1240/K9+JSJLABTES32,2012-09-19 00:58:22.0,,,,Door Open|Port Down,,50.4,-130.5
sgbuA1_cgr0,,,,,,,42.19716359,-87.93733641
sgbuA1_cgr1,,,,,,,44.3558597,-114.8060403
```

Pinging Devices

When troubleshooting device issues, ping registered devices to rule out network connectivity issues. If you can ping a device, it is accessible over the network.

To ping selected devices, in List view:

   1. Check the check boxes of the devices to ping.

      Note: If the status of a device is Unheard, a ping gets no response.

   2. Click **Ping**.

      A window displays the ping results. If you check the check box for **Auto Refresh**, CG-NMS pings the device at predefined intervals until you close the window. Click the **Refresh** button to ping the device at any time.

   3. Click **Close** when done.

Tracing Routes to Devices

The Traceroute command lets you determine the route used to reach a device IP address.

To trace routes to selected devices, in List view:

   1. Check the check boxes of the devices to trace.

      Note: You can only trace routes to devices registered with CG-NMS. If the status of a device is Unheard, you cannot trace the route to it.

   2. Click **Traceroute**.

      A window displays with the route-tracing results.

Common Device Operations

Expand the Result column to view complete route information.

Click the **Refresh** button to resend the Traceroute command. Check the **Auto Refresh** check box to resend the Traceroute command at predefined intervals until you close the window.

3. Click **Close** when done.

Managing Device Labels

You use labels to create logical groups of devices to facilitate locating devices and device management.

Managing Labels

You use the Label Management window to display all custom labels, label properties, and search for custom labels.

To manage labels, in the Browse Device pane on any devices page:

1. Hover your mouse over LABELS and click the edit icon (✎).

149

Common Device Operations
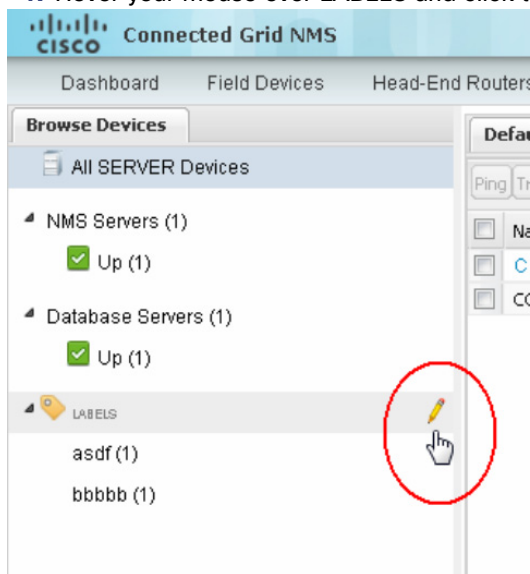
- To find a specific label, enter the label name in the **Search** field.
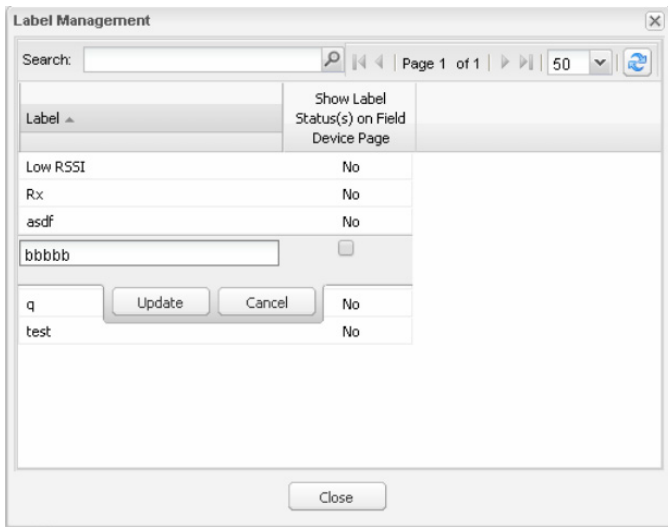
Tip: Click the Label column title to reverse label name sort order.

- To change label properties, double-click a label row, edit the label name and device status display preference.

2. Click **Update** to accept label property changes or **Cancel** to retain label properties.

3. Click **Close**.

Adding Labels

To add labels to selected devices, in List view:

1. Check the check boxes of the devices to label.

2. Choose **Label > Add Label**.
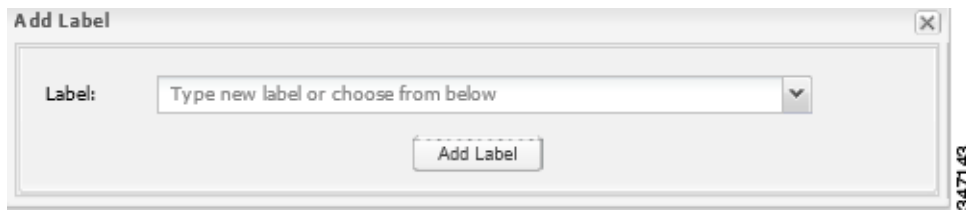
3. Enter the name of the label or choose an existing label from the drop-down menu.

4. Click **Add Label**.

Tip: You can add multiple labels to one device.

5. Click **OK**.

To add labels in bulk, see Adding Labels in Bulk.

Common Device Operations

Removing Labels

To remove labels from selected devices, in List view:

1. Check the check boxes of the devices from which to remove the label.

2. Choose **Label > Remove Label**.

3. Click **OK**.

To remove labels in bulk, see Removing Labels in Bulk.

Removing Devices

Caution: When you remove FARs, CG-NMS returns all the leased IP addresses associated with these devices to the Cisco Network Registrar (CNR) server and removes the corresponding tunnels from the HERs.

To remove devices, in List view:

1. Check the check boxes of the devices to remove.
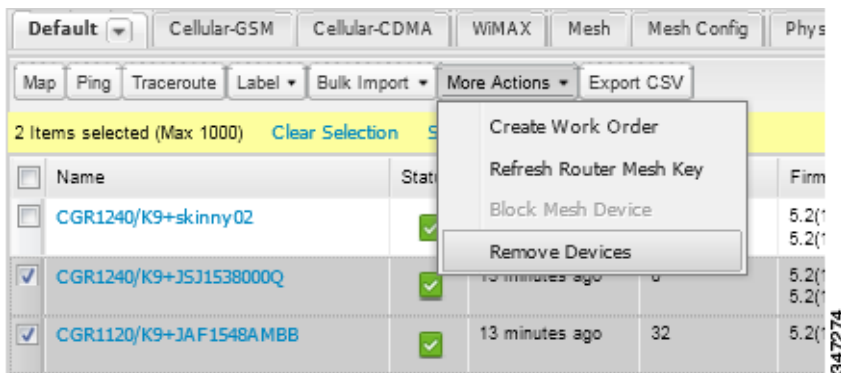
2. Choose **More Actions > Remove Devices**.

3. Click **Yes**.

Displaying Detailed Device Information

CG-NMS keeps detailed information about every device in the system. To access detailed information about a device, click its name or EID.

- Detailed Information Displayed

- Actions You Can Perform from the Detailed Device Information Page

Detailed Information Displayed

- Server Information

- HER, FAR, and ME Information

Note: CG-NMS automatically refreshes the detailed information without the need to reload the page.

Server Information

CG-NMS displays the following information about the system running the NMS and database servers.

Table 1   NMS Server Pane Areas

Area and Field Name	Description
Host System Information	
Hostname	Hostname of the CG-NMS server.
Host Operating System	Operating system.
CPU	CPU specifications.
Total Memory	Total amount of RAM memory (GB) available on the system.
Current System Time	Current system time.
Host Disk Information	
File System	File system.
Size	Size of file system disk space (GB).
Used	Amount of file system disk space used (GB).
Available	Available file system disk space (GB).
Use %	Percentage of file system disk space used.
Mounted On	The directory in which the file system is mounted.
CG-NMS Application Information	
EID	EID of the server.
Start Time	Time when the CG-NMS server started.
Number of Restarts	The number of times the CG-NMS application has restarted.
Memory Allocation	Memory space allocation in GB for the CG-NMS application.

HER, FAR, and ME Information

CG-NMS groups the detailed device information it displays about HERs, FARs, and MEs into the following categories:

Information Category	Description
Device Info	Displays detailed device information (see Device Properties).
	For FARs and MEs, CG-NMS also displays charts (see Viewing Device Charts).
Events	Displays information about events associated with the device.
Config Properties	Displays the configurable properties of a device (see Device Properties).
	You can configure these properties by importing a CSV file specifying the properties to configure and their new values, as described in Changing Device Configuration Properties.
Running Config (FARs)	Displays the running configuration on the device.
Mesh Routing Tree (FARs and MEs)	Displays the mesh routing tree.
	For FARs, the Mesh Routing Tree pane displays all the possible routers from the MEs to the FAR.
	For MEs, the Mesh Routing Tree pane displays the mesh route to the FAR.
Mesh Link Traffic (FARs)	Displays the type of mesh link traffic over time in bits per second.
Router Files (FARs)	Lists files uploaded to the .../managed/files/ directory.

Actions You Can Perform from the Detailed Device Information Page

Depending on device type, the Detailed Device Information page lets you perform these actions:

Action	Description
Show on Map (MEs only)	Displays a pop-up window with a map location of the device. This is the equivalent of entering **eid:***Device_EID* in the search field in Map View.
Ping	Sends a ping to the device to determine its network connectivity. See Pinging Devices
Traceroute	Traces the route to the device. See Tracing Routes to Devices
Refresh Metrics (HERs and FARs only)	Instructs the device to send metrics to CG-NMS. **Note:** CG-NMS assigns historical values for metrics for each device. To access historical metric values, use the GetMetricHistory North Bound API call.
Refresh Router Mesh Key (FARs only)	Refreshes the router ME key. See Refreshing the Router Mesh Key
Create Work Order (FARs only)	Creates a work order. See Creating Work Orders
Sync Config Membership (MEs only)	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership
Sync Firmware Membership (MEs only)	Click **Sync Firmware Membership** to synchronize the firmware membership for this device, and then click **Yes** to complete the process.
Block Mesh Device (MEs only)	Blocks the ME device. **Caution:** This is a disruptive operation.

Using Filters to Control the Display of Devices

Depending on your deployment, the number of devices managed by CG-NMS can be very large (CG-NMS supports up to 10 million devices). To facilitate locating and displaying devices in Map View and List view, CG-NMS provides filters and lets you add customized filters. Filters are listed in the Browse Devices and Quick View tabs.

Browse Devices Filters

Built-in device filters display in the Browse Devices pane. These filters control the display of devices in List and Map views. For every filter entry, CG-NMS provides a device count in parenthesis. CG-NMS automatically updates the device count without having to reload the page. In the example in Figure 3, the top-level Endpoints label is selected, which inserts the following built-in filter in the Search Devices field: *deviceType:cgmesh firmwareGroup:default-cgmesh*.

Common Device Operations

Figure 3   Built-in Filter to Search for MEs

Creating and Editing Quick View Filters

The Quick View pane displays custom filters. Click a filter in this pane to view the devices that fulfill the search criteria defined in the filter.

Creating a Quick View Filter

To create a Quick View filter:

1. On any device page, click **Show Filters** and add filters to the Search field.

   For more information about adding filters, see Adding a Filter.

2. From the **Quick View/Rule** drop-down menu, choose **Create Quick View**.

3. In the Name field of the Save Quick View dialog box, enter the name for the Quick View filter.

4. Click **Save**.

Editing a Quick View Filter

To edit or delete a Quick View filter:

1. Click the Quick View tab and select the filter to edit.

2. From the **Quick View/Rule** drop-down menu, choose **Edit Quick View**.

3. In the **Update Quick View** dialog box, make the necessary modifications, and then click **Save**.

4. To delete the Quick View, click the **Delete** button.

Adding a Filter

To add a filter to the Search field:

1. If the Add Filter fields are not present under the Search field, click **Show Filters**.

2. From the **Label** drop-down menu, choose a filter.

   The drop-down menu defines filters for all device information categories. For more information about these categories, see Working with Router Views.

3. From the **Operator** (:) drop-down menu, choose an operator.

   For more information about operators, see Table 2. If you choose a numeric metric from the Label menu (for example, **Transmit Speed**), you can specify a range of values in the filter you are adding. For date/time filters, "between" is the operator. Use the calendar buttons to specify the date range for the filter.

4. In the **Value** field, enter a value to match or a range of values in the case of numeric metrics or select an available value from the drop-down menu.

5. Click the Add (**+**) button to add the filter to the existing filter syntax in the Search field.

6. (Optional) Repeat the process to continue adding filters.

Filter Operators

Table 2 describes the operators you can use to create filters.

Table 2   Filter Operators

Operator	Description
:	Equal to
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
<>	Not equal to

Search Syntax

CG-NMS supports this simple query language syntax:

Search := filter [filter ...]

Filter := fieldname operator value

operator := < | <= | > | >= | <> | = | :

Note the following when creating filters to search fields:

- Each field has a data type (String, Number, Boolean, and Date).

- String fields can contain a string, and you can search them using string equality (":").

- Numeric fields can contain a decimal number (stored as a double-precision float), and you can search them using the numeric comparison operators (">", ">=", "<", "<=", "<>").

- Boolean fields can contain the strings "true" or "false".

- Date fields can contain a date in this format: yyyy-MM-dd HH:mm:ss:SSS. You can search dates using numeric comparison operators.

Table 3 describes filter examples.

Table 3   Filter Examples

Filter	Description
`configGroup:"default-cgr1000"`	Finds all devices that belong to the default-cgr1000 group.
`name:00173*`	Finds all FARs with a name starting with 00173.
`deviceType:cgr1000 status:up` `label:"Nevada"`	Finds all CGR 1000s in the Nevada group that are up and running.

Performing Bulk Import Actions

In CG-NMS, you can perform these bulk import device actions:

- Adding Devices in Bulk

- Removing Devices in Bulk

- Changing Device Properties in Bulk

- Adding Labels in Bulk

- Removing Labels in Bulk

Adding Devices in Bulk

The **Add Devices** option in the Bulk Import drop-down menu lets you add FARs and HERs to CG-NMS in bulk using a CSV file.

To add devices in bulk:

1. On any device page, from the Bulk Import drop-down menu, choose **Add Devices**.
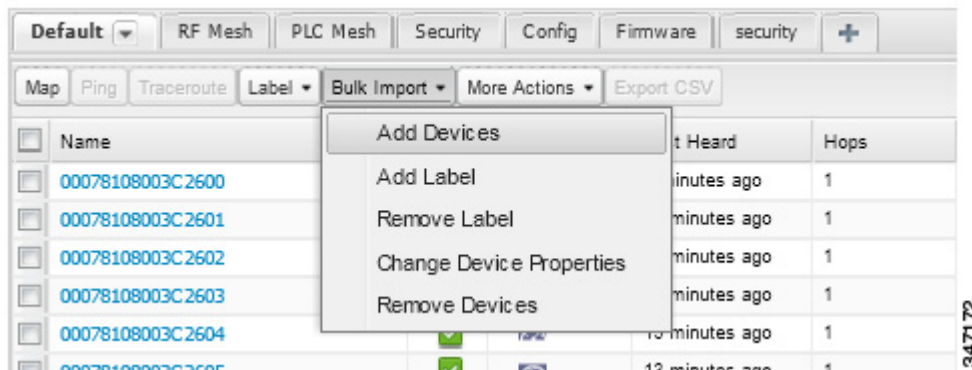
2. Click **Browse** to locate the CSV file containing the device information to import, and then click **Open**.

   For more information about adding HERs, see Adding HERs to CG-NMS.

   For more information about adding FARs, see Adding FARs to CG-NMS.

   Note: For FARs, you can also use the Notice-of-Shipment XML file provided by your Cisco partner to import FARs.

3. Click **Add**.

156

Common Device Operations

    4. Click **Close**.

Adding HERs to CG-NMS

Configuring HERs Before Adding them to CG-NMS

Before you can add an HER to CG-NMS, configure the HER to allow management by CG-NMS using Netconf over SSH as follows:

```
hostname <her_hostname>
ip domain-name <domain.com>
aaa new-model
no ip domain-lookup
ip ssh time-out 120
ip ssh version 2
crypto key gen rsa
netconf ssh
netconf max-sessions 16
```

Where *<her_hostname>* is the hostname or IP address of the CG-NMS server, and *<domain.com>* is the name of the domain name where the HER and CG-NMS reside. The time-out value of 120 is required for large networks.

After configuring the HER to allow management by CG-NMS, ensure that you can:

- Ping the management interface of the HER.

- Access the management interface of the HER over SSH and vice versa.

Adding HERs

To add HERs, create a CSV file like the following example that consists of a header line followed by one or more lines, each representing an HER:

```
eid,deviceType,lat,lng,ip,netconfUsername,netconfPassword
ASR1001+JAE15460070,asr1000,40.0,-132.0,172.27.166.57,admin,cisco
ASR1001+JAE15460071,asr1000,40.0,-132.0,172.27.166.58,admin,cisco
```

Table 4 describes the fields to include in the CSV file.

Note: For device configuration field descriptions, see Device Properties.

Table 4   HER Import Fields

Field	Description
eid	The element identifier (EID) of the device, which consists of the product ID (PID), a plus sign, and the serial number (SN) of the HER (for example, *HER_PID+HER_SN*).
deviceType	The device type must be asr1000 or isr3900.
lat	(Optional) The location (latitude and longitude) of the HER.
lng	
ip	The IP address of the HER. The address must be reachable from the CG-NMS server.
netconfAddress	
netconfUsername	The SSH username and password that CG-NMS uses to connect to the HER.
netconfPassword	

When you add an HER, CG-NMS displays its status as Unheard. CG-NMS changes the status to Up after it polls the HER. CG-NMS polls HERs in the background every 15 minutes to collect device metrics, so it should take no more than 15 minutes for the status of HERs to change to Up after you add them to CG-NMS. However, you can trigger the polling of

HERs by clicking **Refresh Metrics** (Refresh Metrics).

Adding FARs to CG-NMS

Typically, when adding FARs to CG-NMS, you use the Notice-of-Shipment XML file sent to you by your Cisco partner. This file contains an R record for every FAR shipped to you. This is an example of an R record for a CGR:

```
<AMI>
    <Relays>
        <DCG deviceClass=?10.84.82.56?>
            <PID>CGR1240/K9</PID>
            <R>
                <ESN>2.16.840.1.114416.3.2286.333498</ESN>
                <SN>FIXT:SG-SALTA-10</SN>
                <wifiSsid>wifi ssid 1</wifiSsid>
                <wifiPsk>wifi psk 1</wifiPsk>
                <adminPassword>ppswd 1</adminPassword>
                <type6PasswordMasterKey>secret 1</type6PasswordMasterKey>
                <tunnelSrcInterface1>Ethernet2/3</tunnelSrcInterface1>
            </R>
        </DCG>
    </Relays>
</AMI>
```

Table 5 describes the FAR properties defined in the R record used in this example:

Table 5   FAR Import Fields

Field	Description
PID	The product ID, as supplied by Cisco. This is not printed on the product.
SN	The FAR serial number. **Note:** CG-NMS forms the FAR EID by combining the PID and SN.
ESN	A serial number assigned by your Cisco partner to the WPAN mesh card inside the FAR. This field is not used by CG-NMS.
wifiSsid	This information is configured on the FAR by your Cisco partner during the manufacturing configuration process. CG-NMS stores this information in its database for future use. **Note:** For CG-OS CGRs, a maximum of two SSIDs is allowed.
wifiPsk	
adminPassword	
adminUsername	
type6PasswordMasterKey	
tunnelSrcInterface1	

Mapping FARs to HERs

After you determine the FAR-to-HER mapping, which is essential for tunnel provisioning, you can configure the mapping in CG-NMS in one of two ways:

- Adding the mapping information to every FAR record in the Notice-of-Shipment XML file.

- Creating a CSV file specifying the mapping of FARs to HERs.

Adding FAR-to-HER Mappings to the Notice-of-Shipment XML File

To map a FAR to an HER, add the tunnelHerEid and ipsecTunnelDestAddr1 HER properties to the FAR record in the Notice-of-Shipment XML file.

- The tunnelHerEid property specifies the EID of the HER

- The ipsecTunnelDestAddr1 property specifies the tunnel IP address of the HER.

Common Device Operations

For example:

```
...
        <tunnelHerEid>ASR1001+JAE15460070</tunnelHerEid>
        <ipsecTunnelDestAddr1>172.27.166.187</ipsecTunnelDestAddr1>
    </R>
</DCG>
```

Adding FAR-to-HER Mappings to a CSV File

To map FARs to HERs using a CSV file, add a line for every FAR-to-HER mapping. The line must specify the EID of the FAR, the EID of the corresponding HER, and the tunnel IP address of the HER, as in this example for a CGR:

```
eid,tunnelHerEid,ipsecTunnelDestAddr1
CGR1240/K9+FIXT:SG-SALTA-10,ASR1001+JAE1546007O,172.27.166.187
```

Removing Devices in Bulk

You can remove devices in bulk using a CSV file listing the EIDs of the devices to remove.

Caution: When you remove FARs, CG-NMS returns all the leased IP addresses associated with these devices to CNR and removes the corresponding tunnels from the HERs.

To remove devices in bulk:

1. Choose **Devices >** *Device Type*.

2. Choose **Bulk Import** > **Remove Devices**.
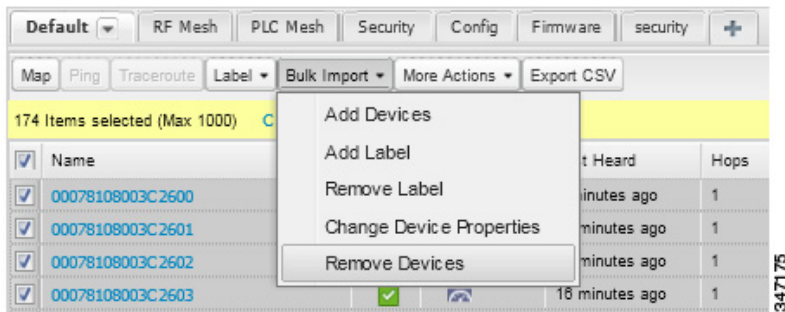
3. Click **Browse** to locate the CSV file containing the devices to delete, and then click **Choose**.

   This is an example of the CSV format expected. In this case, the CSV file specifies three CGRs and one HER:

```
eid
cgr1000-CA-107
cgr1000-CA-108
cgr1000-CA-109
asr1000-CA-118
```

4. Click **Remove**.

   The Status section of the Remove Devices window displays the status of the operation. The History section describes additional information about the operation. If there was any failure, click the corresponding link in the Failure# column to get more information about the error.

5. Click **Close** when done.

Changing Device Properties in Bulk

CG-NMS lets you configure device properties in bulk using a CSV file. For example, this CSV file changes the latitude and longitude for the specified HER:

```
eid,lat,lng,ip,
ASR1001+JAE1546007O,42.0,-120.0
```

To configure device properties in bulk:

1. On any device page, choose **Bulk Import > Change Device Properties**.
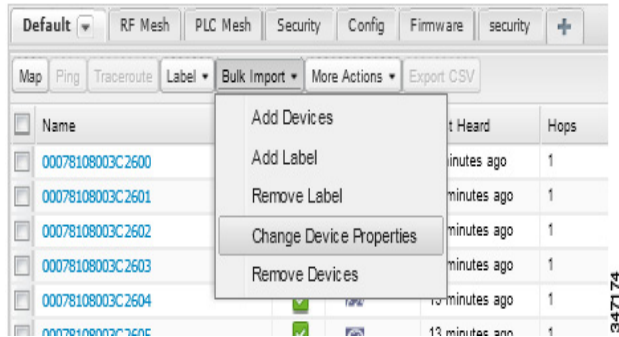
2. Click **Browse** to locate the CSV containing the list of devices and corresponding properties to configure, and then click **Open**.

3. Click **Change**.

4. Click **Close** when done.

Adding Labels in Bulk

You can group devices logically by assigning them labels. Labels are independent of device type, and devices of any type can belong to any label. A device can also have multiple labels. Unlike configuration groups and firmware groups, there are no policies or metadata associated with labels.

CG-NMS lets you add labels in bulk using a CSV file. In the CSV file, specify the list of devices to be labeled.

To add device labels:

1. On any device page, choose **Bulk Import > Add Label**.
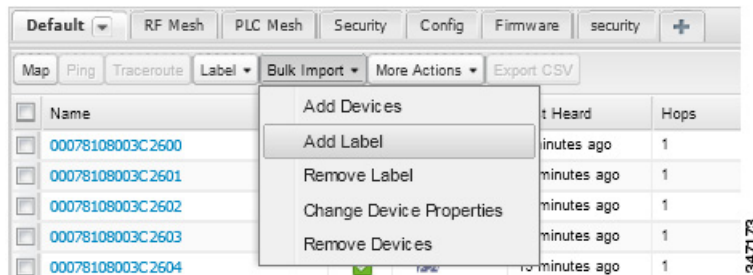
2. Click **Browse** to locate the CSV file that contains the list of devices to label, and then click *Open*.

This is an example of the expected CSV format:

```
eid
cgr1000-CA-107
cgr1000-CA-108
cgr1000-CA-109
```

```
asr1000-CA-118
```

3. In the **Label** field, enter the label or choose one from the drop-down menu.

4. Click **Add Label**.

   The label appears in the Browse Devices tab (left pane) under LABELS.

5. Click **Close** when done.

Removing Labels in Bulk

CG-NMS lets you delete labels in bulk using a CSV file.

To delete device labels:

1. On any device page, choose **Bulk Import > Remove Label**.
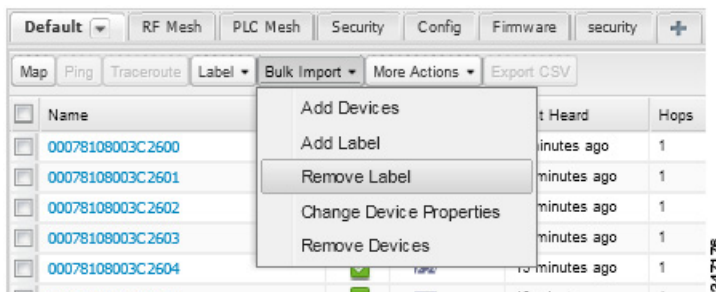
2. Click **Browse** to locate the CSV containing the list of devices to remove the label from, and then click **Open**.

3. From the drop-down menu, choose the label to remove.

4. Click **Remove Label**.

5. Click **Close**.

Configuring Rules

A CG-NMS rule defines a filter and actions that CG-NMS performs after an event or after it receives metrics that match the search criteria defined in the filter. Rules can check for event conditions and metric thresholds.

For example, whenever the status of a FAR in a configuration group changes to Up, you can add a custom message to the server log (server.log) and add the appropriate labels to the device. This helps you automate the process of adding labels to devices.

When working with rules, you can do the following:

■ Add rules with conditions and actions.

■ Define a rule with a condition using a device search query, which matches devices according to properties and metrics.

■ Define a rule with a condition using an event search query, which matches events according to event properties.

■ Define a rule with an action that adds labels to matching devices or to the devices that sent a matching event.

■ Define a rule with an action that removes a label from a matching device or the device that sent a matching event.

■ Define a rule with an action that places a *user alert* event into the log, which includes a user-defined message.

Viewing and Editing Rules

To view rules:

1. Choose **Config > Rules**.

CG-NMS displays the list of rules stored in its database. Table 6 describes the fields displayed in the list.

Table 6   Rule Fields

Field	Description
Name	The name of the rule.
Active?	Whether the rule is active. Rules are not applied until you activate them.
Rule definition	The syntax of the rule. For example, CG-NMS executes this rule when a device battery 0 level drops below 50%: `battery0Level<50`
Rule Actions	The actions performed by the rule. For example: `Log Event With: CA-Registered , Add Label: CA-Registered` In this example, the actions: ■ Set the eventMessage property of the Rule Event generated by this rule to CA-Registered. ■ Add the label CA-Registered to the matching device.
Updated By	The username of user who last updated the rule.
Updated At	The date and time when the rule was last updated.

2. To edit a rule, click its name.

For information on how to edit rules, see Adding a Rule.

Adding a Rule

To add a rule:

1. Choose **Config > Rules**.

2. Click **Add**.

3. Enter a name for the rule.

Note: If you enter invalid characters (for example, "=", "+", and "~"), CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button.

4. To activate the rule, check the **Active?** check box.

5. Enter the syntax of the rule.

Use the same syntax used for creating filters. See Search Syntax.

6. Check the check box of at least one action:

■ **Log event with**—Specify the message to add to the log entry of the event in the server log.

For example, if you enter Red Alert in this field, the eventMessage field in the logged entry for the event that matches the rule is set to Red Alert, as shown in this sample entry from the server log (server.log):

```
16494287: NMS-200-5: May 02 2012 22:32:41.964 +0000: %CGMS-7-UNSPECIFIED:
%[ch=EventProducer][sev=DEBUG][tid=com.espertech.esper.Outbound-CgmsEventProvider-1]: Event
Object which is send = EventObject [netElementId=50071, eventTime=1335997961962,
eventSeverity=0, eventSource=cgr1000, eventType=UserEventType, eventMessage=Red Alert,
lat=36.319324, lng=-129.920815, geoHash=9n7weedx3sdydv1b6ycjw, eventTypeId=1045,
eid=CGR1240/K9+JAF1603BBFF]
```

In CG-NMS, the message you define in the "Log event with" field is displayed in the Message field of the matching event entries listed in the Events page (**Operations > Events**).

■ **Severity**—Select the severity level to assign to the event.

■ **Add Label**—Enter the name of a new label or choose one from the **Add Label** drop-down menu.

163

- ■ **Show label status on Field Devices page**–Check this check box to show the status of the device that triggered this rule in the LABELS section of the Browse Devices pane.
- ■ **Remove Label**–Choose the label to remove from the **Remove Label** drop-down menu.

7. Click **Save**.

Activating Rules

CG-NMS does not apply rules if they are not activated.

To activate a rule:

1. Choose **Config > Rules**.

2. Check the check boxes of the rules to activate.

3. Click **Activate**.

4. Click **Yes** to activate the rule.

5. Click **OK**.

Deactivating Rules

If you deactivate a rule, CG-NMS does not apply it.

To deactivate rules:

1. Choose **Config > Rules**.

2. Check the check boxes of the rules to deactivate.

3. Click **Yes** to deactivate the rule.

4. Click **OK**.

Deleting Rules

To delete rules:

1. Choose **Config > Rules**.

2. Check the check boxes of the rules to delete.

3. Click **Delete**.

4. Click **Yes** to delete the rule.

5. Click **OK**.

Configuring Devices

This section describes how to configure devices in CG-NMS, including:

- Configuring Device Group Settings

- Editing the ROUTER Configuration Template

- Editing the ENDPOINT Configuration Template

- Pushing Configurations to FARs

- Pushing Configurations to Endpoints

Configuring Device Group Settings

CG-NMS uses groups to manage devices in bulk. When you add FARs to CG-NMS, CG-NMS automatically adds them to the appropriate default ROUTER configuration groups, for example, **default-cgr1000**. When you add MEs (meters and range extenders), CG-NMS adds them to the default ENDPOINT configuration group, **default-cgmesh**.

- Creating Device Groups

- Changing Device Configuration Properties

- Moving Devices to Another Group

- Listing Devices in a Configuration Group

- Configuring Periodic Inventory Notification and Mark-Down Time

- Renaming a Device Configuration Group

- Deleting Device Groups

Creating Device Groups

By default, CG-NMS defines these device groups:

Group Name	Description
default-cgr1000	By default, all CGRs are members of this group.
default-cgmesh	By default, all MEs are members of this group.

Each default group defines a default configuration template that you can push to all devices in that group. However, if you need to apply a different template to a group of devices, create a new group and modify its default configuration template as needed.

Note: You cannot delete the default groups, but you can change their names, although we do not recommend it. Also, the default ROUTER and ENDPOINT groups use the same icon, while custom groups use a different icon. See Table 5 for icon definitions.

- Creating ROUTER Groups

- Creating ENDPOINT Groups

Creating ROUTER Groups

Note: To create a ROUTER configuration group:

1. Choose **Config > Device Configuration**.

2. Select the default group: **default-cgr1000**.

3. Click the **Add Group** button.

4. Enter the name of the group.
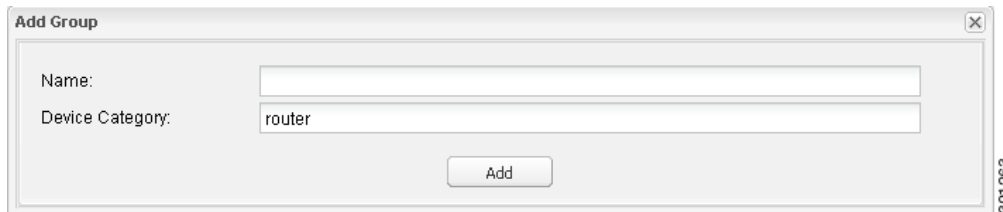
The device category is selected by default.

Note: If you enter invalid characters (for example, "=", "+", and "~"), CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button.

5. Click **Add**.

The new group entry appears in the ROUTERS list (left pane).

- To change the name of a group, see Renaming a Device Configuration Group.

- To remove a group, see Deleting Device Groups.

Creating ENDPOINT Groups

To create an ENDPOINT configuration group:

1. Choose **Config > Device Configuration**.

2. Select the default group (**default-cgmesh**).

3. Click the **Add Group** ( ) button.

4. Enter a name for the group.
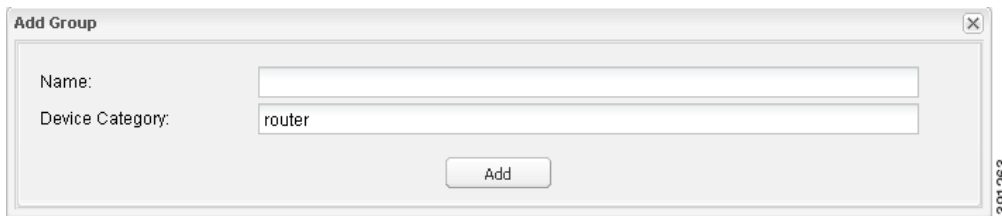
Note: If you enter invalid characters (for example, "=", "+", and "~"), CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button.

5. Click **Add**.

The new group entry appears in the ENDPOINT list (left pane).

■ To change the name of a group, see Renaming a Device Configuration Group.

■ To remove a group, see Deleting Device Groups.

Changing Device Configuration Properties

You can change the configurable properties of devices by uploading a Device Properties CSV file with modified values for the devices.

To change device configuration properties:

1. Choose **Config > Device Configuration**.

2. Click **Change Device Properties**.
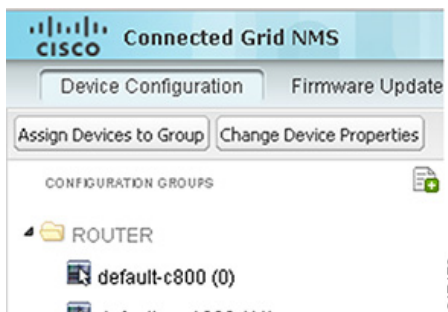
3. Click **Browse** and select the Device Properties CSV file to upload.

4. Click **Change**.

5. Click **Close** when done.

■ For a list of configurable device properties in CG-NMS, see Device Properties.

Moving Devices to Another Group

There are two ways to move devices from one configuration group to another:

■ Moving Devices to Another Configuration Group Manually

■ Moving Devices to Another Configuration Group in Bulk

Moving Devices to Another Configuration Group Manually

To move devices to another configuration group:

1. Choose **Config > Device Configuration**.

2. Select a group from the list of configuration groups (left pane).

3. Check the check boxes of the devices to move.

4. Click **Change Configuration Group**.
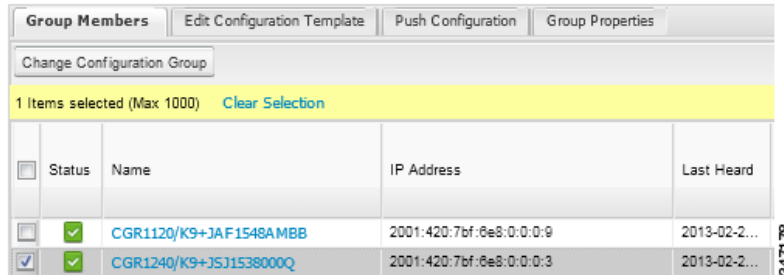
5. From the drop-down menu in the dialog box, choose the target group for the devices.

6. Click **Change Config Group**.

7. Close **OK**.

Moving Devices to Another Configuration Group in Bulk

To move a large number of devices from one group to another, you can import a CSV file containing the list of the devices to move.

For example, this CSV file specifies the EIDs of three CGRs to move:

```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

To move devices to another configuration group in bulk:

1. Choose **Config > Device Configuration**.

2. Click **Assign Devices to Group**.
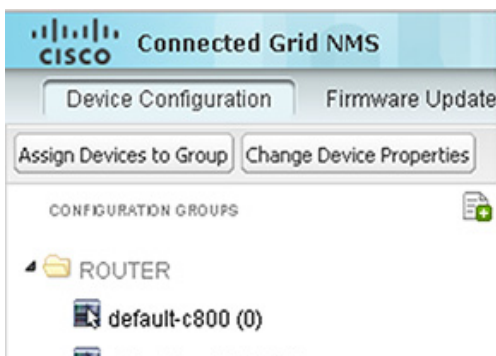
3. Click **Browse** to locate the CSV file containing the list of devices to move, and then click **Open**.

4. From the Group drop-down menu, choose the target group for the devices.

168

5. Click **Change Group**.

6. Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

1. Choose **Config > Device Configuration**.

2. Select a group from the list of configuration groups (left pane).

3. To get more information about a device in the list, click its EID.

Configuring Periodic Inventory Notification and Mark-Down Time

You can change the periodic inventory notification interval for a configuration group of FARs without affecting the logic that CG-NMS uses to mark those FARs as **Down**. However, for this to happen, you must enable the periodic configuration notification frequency for the FAR group so that it is less than the mark-down timer.

You can configure the mark-down timer by clicking the Group Properties tab for the group and modifying the value of the Mark Routers Down After field.

■ Configuring Periodic Inventory Notification

■ Configuring the Mark-Down Timer

Configuring Periodic Inventory Notification

To configure the periodic inventory notification interval for a ROUTER configuration group:

1. Click **Config > Device Configuration**.

2. Select a ROUTER configuration group.

3. Click **Edit Configuration Template**.

```
Group Members    Edit Configuration Template    Push Configuration    Group Properties

Current Configuration revision #10 - Last Saved on 2014-05-07 14:05

<#if far.isRunninglos()>
 <#--
   If a Loopback0 interface is present on the device (normally configured
   during tunnel provisioning) then use that as the source interface for
   the HTTP client and SNMP traps. The source for the HTTP client is not
   changed during tunnel provisioning because usually the addresses assigned
   to the loopback interface are only accessible through the tunnels.
   Waiting insures the tunnel is configured correctly and comes up.
   -->

 <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
 cgna profile cg-nms-periodic
   interval 15
 exit

 <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
 cgna heart-beat interval 5

<#elseif far.isRunningCgOs()> <--
 <#-- Enable periodic inventory notification every 6 hours to report metrics. -->
 callhome
   periodic-inventory notification frequency 360
 exit

 <#-- Enable periodic configuration (heartbeat) notification every 1 hour. -->
 <#if far.supportsHeartbeat()>
 callhome
   periodic-configuration notification frequency 60
 exit
</#if>
```

CG-IOS CGRs

CG-OS CGRs

347219

4. This step is OS-specific:

■ For Cisco IOS CGRs, change the value of the **cgna heart-beat interval** parameter. The time is in minutes

For example, to enable periodic inventory notification to report metrics every 20 minutes for an IOS CGR, add these lines to the template:

```
<#-- Enable periodic configuration (heartbeat) notification every 20 min. -->
cgna heart-beat interval 20
exit
```

■ For CG-OS CGRs, change the value of the **periodic-inventory notification frequency** parameter to the new value. The time unit is minutes.

5. Click **Save Changes**.

Configuring the Mark-Down Timer

To configure the mark-down timer for a ROUTER configuration group:

1. Click **Config > Device Configuration**.

2. Select a ROUTER configuration group.

3. Click **Group Properties**.
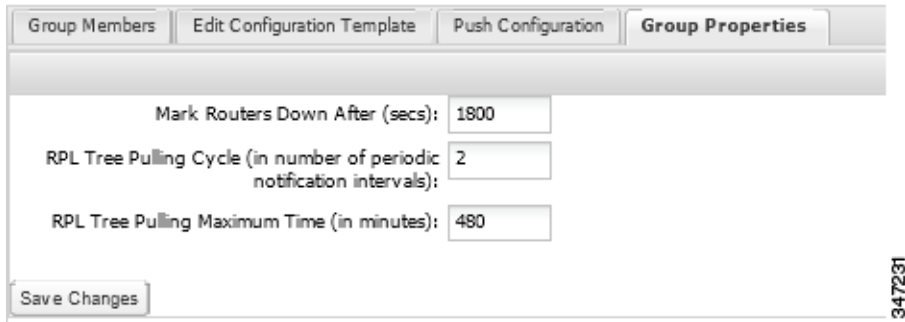
4. In the **Mark Routers Down After** field, enter the number of seconds after which CG-NMS marks the FARs as down if they do not send periodic configuration notifications (heartbeats) to CG-NMS during that time.

   Note: We recommend a 1:3 ratio of heartbeat interval to mark-down timer.

5. Click **Save Changes**.

6. Ensure that the periodic-configuration notification frequency in the configuration template is less than the value you entered the **Mark Routers Down After** field:

   a. Click **Edit Configuration Template**.

   b. Ensure that the value of the periodic-configuration notification frequency parameter is less than the **Mark Routers Down After** value.

   Use a notification value that is at most one-third of the mark-down value. For example, if you choose a mark-down value of 3600 seconds (60 minutes), set the periodic-configuration notification frequency parameter to 20 minutes:

   ```
   <#-- Enable periodic configuration (heartbeat) notification every 20 minutes. -->
   <#if far.supportsHeartbeat()>
   callhome
     periodic-configuration notification frequency 20
   exit
   </#if>
   ```

   Note: The ability to control the periodic inventory notification interval and the periodic-configuration notification frequency applies to CGR image version 3.2.

Renaming a Device Configuration Group

To rename a device configuration group:

1. Choose **Config > Device Configuration**.

2. Select a group from the list of configuration groups (left pane).

3. Click the **Edit Group** icon.

   The Edit Group button displays as a pencil icon when you hover over the name of the group in the list.
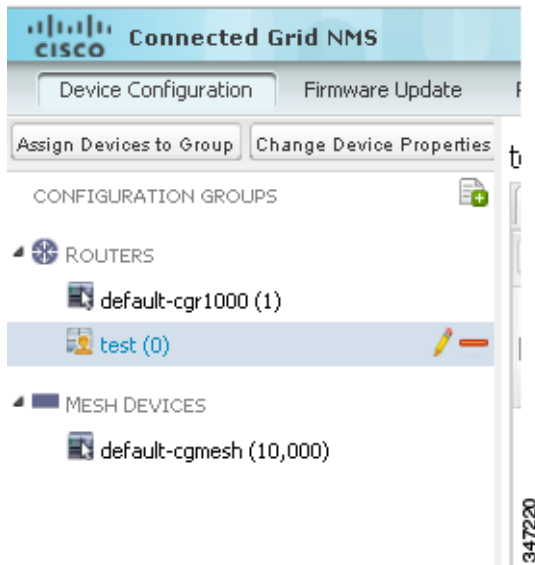
4. Enter the new name in the **Rename Group** dialog box, and then click **OK**.

Note: If you enter invalid characters (for example, "=", "+", and "~"), CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button.

Deleting Device Groups

Note: Before deleting a group, move all devices in that group to another group. You cannot delete a non-empty group.

To delete a configuration group:

1. Choose **Config > Device Configuration**.

2. Select a group from the list of configuration groups (left pane).

3. Ensure that the group is empty.

4. Click **Delete Group** (➖).

   The Delete icon displays as a red minus sign when you hover over the name of the group in the list.

5. Click **Yes** to confirm, and then click **OK**.

Synchronizing Endpoint Membership

MEs maintain information about the CG-NMS group to which they belong. If the group information changes, the ME becomes out of sync. For example, if you rename an ME group, the members of the group might not be modified immediately (for example, due to a packet loss). If a device is out of sync, any operation you perform on the group through CG-NMS does not reach the device. To ensure that the MEs remain in sync, use the Sync Membership button to push the group information to group members.

To send group information to MEs:

1. Choose **Config > Device Configuration**.

2. Select an ENDPOINT group (left pane).

3. Check the check boxes of the members in the group to sync.

4. Click **Sync Membership**.
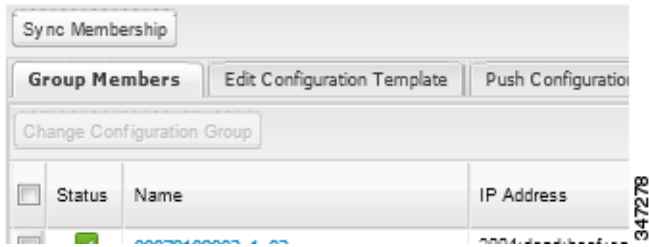
5. When prompted to synchronize membership for the group, click **Yes**.

6. Click **OK**.

Devices sync for the first time after they register with CG-NMS.

Editing the ROUTER Configuration Template

CG-NMS lets you configure FARs in bulk using a configuration template. When a FAR registers with CG-NMS, CG-NMS pushes the configuration defined in the default template to the device and commits the changes to the router startup configuration. CG-NMS then retrieves the running configuration from the router before changing the device status to **Up**.

To edit a ROUTER group configuration template:

1. Choose **Config > Device Configuration**.

2. Under CONFIGURATION GROUPS (left pane), select the group with the template to edit.

3. Click **Edit Configuration Template**.

Group Members	**Edit Configuration Template**	Push Configuration	Group Properties

Current Configuration revision #10 - Last Saved on 2014-05-07 14:05

```
<#if far.isRunningIos()>
  <#--
    If a Loopback0 interface is present on the device (normally configured
    during tunnel provisioning) then use that as the source interface for
    the HTTP client and SNMP traps. The source for the HTTP client is not
    changed during tunnel provisioning because usually the addresses assigned
    to the loopback interface are only accessible through the tunnels.
    Waiting insures the tunnel is configured correctly and comes up.
  -->

  <#-- Enable periodic inventory notification every 1 hour to report metrics. -->
    cgna profile cg-nms-periodic
      interval 15
    exit

  <#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
  cgna heart-beat interval 5

<#elseif far.isRunningCgOs()>  <--
  <#-- Enable periodic inventory notification every 6 hours to report metrics. -->
  callhome
    periodic-inventory notification frequency 360
  exit

  <#-- Enable periodic configuration (heartbeat) notification every 1 hour. -->
  <#if far.supportsHeartbeat()>
  callhome
    periodic-configuration notification frequency 60
  exit
  </#if>
```

347219

4. Edit the template.

The template is expressed in FreeMarker syntax. For more information about FreeMarker, see Tunnel Provisioning Template Syntax.

Note: The router configuration template does not validate the configuration data entered. Verify the configuration before saving.

5. Click **Save Changes**.

CG-NMS commits the changes to the database and increases the template version number.

Enabling Dual PHY Support

You can configure CGR master and slave interfaces.

Enabling Router GPS Tracking

You can enable GPS traps to trigger an event if the router moves a distance threshold, after a time threshold, or both. For example, you can configure stationary, pole-top CGR monitoring for a distance threshold, to detect movement from theft or pole incident; for mobile routers, set both thresholds to determine distance over time. The recommended distance threshold is 100 feet (30 m).

To enable GPS traps, uncomment these lines in the default configuration template.

```
<#--
Enable the following configurations to generate events that track if the router
moves by a certain distance (unit configurable) or within a certain time (in minutes)
-->
<#-- cgna geo-fence interval 10 -->
<#-- cgna geo-fence distance-threshold 100 -->
```

```
<#-- cgna geo-fence threshold-unit foot -->
<#-- cgna geo-fence active -->
```

Tip: Because GPS traps only generate Informational logs, we recommend that you create a rule-based event with high severity (such as CRITICAL) to inform the administrator of router movement. An example of this type of rule definition is: configGroup:name eventName:deviceLocChanged (see Adding a Rule).

Configuring SNMP v3 Informational Events

For Cisco IOS routers you configure SNMP v3 Informational Events to replace the default SNMP v3 traps. In CG-OS by default, SNMP v3 traps are configured for any CG-NMS event-related changes that generate a trap on the router. CG-NMS maps these traps to the corresponding event. For Cisco IOS routers, converting these SNMP v3 traps to SNMP v3 Informational Events sends an acknowledgment to the router for every event received from the router. The router then verifies that the trap was received by CG-NMS. To enable SNMP v3 Informational Events, uncomment the following lines in the default configuration file and push the new configuration file to all router(s) in the group:

```
<#-- Enable the following configurations for the nms host to receive informs instead of traps -->
<#-- no snmp-server host ${nms.host} traps version 3 priv ${far.adminUsername} -->
<#-- snmp-server engineID remote ${nms.host} ${nms.localEngineID} -->
<#-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha ${far.adminPassword}
priv aes 256 ${far.adminPassword} -->
<#-- snmp-server host ${nms.host} informs version 3 priv ${far.adminUsername} -->
```

Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

1. Choose **Config > Device Configuration**.

2. Under CONFIGURATION GROUPS (left pane), select the **ENDPOINT group** with the template to edit.

3. Click **Edit Configuration Template**.

175

Configuring Devices

4. Edit the template.

For example, in the **Report Interval** field, you can enter the number of seconds between data updates. By default, MEs send a new set of metrics every 28,800 seconds (8 hours).

You can change the following values on the Edit Configuration Template tab:

- **Report Interval**: The number of seconds between data updates.
- **BBU Settings**: Enable this option to configure BBU Settings for range extenders with a battery backup unit.
- **Enable Ethernet**: Check this check box to enable Ethernet for selected devices or configure NAT 44 settings on selected DA Gateway devices.

  Note: For NAT 44 configuration, you must specify values for all three fields in a CSV file. The default values are 127.0.0.1, 0, 0, respectively. You do not need to configure any other settings for a particular map index. If these settings are invalid for that map index, they are ignored during a configuration push.

- **Map-T Settings**: The IPv6 and IPv4 settings for the device.

  Note: For Cisco IOS CGRs, Map-T rules are set by indicating the Map-T IPv6 basic mapping rule (BMR), IPv4 BMR, and IPv6 default mapping rule (DMR). On Cisco IR509 devices, the Map-T IPv6 is an IPv6 prefix that integrates the Map-T BMR IPv6 rules, IPv4 suffix value, and length being based on the BMR EA length value.

- **Serial Interface 0 (DCE) Settings**: The data communications equipment (DCE) communication settings for the selected device.

  Note: There can be only one session per serial interface. You must configure the following parameters for all TCP raw socket sessions (for each virtual line and serial port) for the selected DA Gateway device(s):

- Initiator – Designate the device as the client/server.
- TCP idle timeout (min) – Set the time to maintain an idle connection
- Local port – Set the port number of the device.
- Peer port – Set the port number of the client/server connected to the device.
- Peer IP address – Set the IP address to the host connected to the device.
- Connect timeout – Set the TCP client connect timeout for Initiator DA Gateway devices.
- Packet length – Sets the maximum length of serial data to convert into the TCP packet.
- Packet timer (ms) – Sets the time interval between each TCP packet creation.
- Special Character – Sets the delimiter for TCP packet creation.
- **Serial Interface 1 (DTE) Settings**: The data terminal equipment (DTE) communication settings for the selected device.

  Note: The IPv6 prefix must valid. Maximum prefix lengths are:

  – IPv6: 0–128
  – IPv4: 0–32

5. Click **Save Changes**.

CG-NMS commits the changes to the database and increases the version number.

Pushing Configurations to FARs

Note: To push the configuration to FARs:

1. Choose **Config > Device Configuration**.

2. Select the group or subset of a group to push the configuration to in the CONFIGURATION GROUPS pane.

3. Click the **Push Configuration** tab.

Configuring Devices

4. Click **Start Push**.

5. Click **Yes** to confirm.

The Push Configuration page displays the status of the push operation for every device in the group. If an error occurs while pushing configuration to a device, the error and its details display in the relevant columns.

In the Status column, one of these values appear:

- NOT_STARTED—The configuration push has not started.
- RUNNING—The configuration push is in progress.
- PAUSED—The configuration push is paused. Active configuration operations complete, but those in the queue are not started.
- STOPPED—The configuration push was stopped. Active configuration operations complete, but those in the queue are not started.
- FINISHED—The configuration push to all devices is complete.
- STOPPING—The configuration push is in the process of being stopped. Active configuration operations complete, but those in the queue are not started.
- PAUSING—The configuration push is in the process of being paused. Active configuration operations complete, but those in the queue are not started.

To refresh the status information, click the **Refresh** button.

Enabling CGR SD Card Password Protection

Password protection for the SD card in the CGR helps prevent unauthorized access and prevents transference of the CGR SD card to another system with a different password.

Note: This does not apply to C800s.

The Device Info pane displays CGR SD card password protection status in the Inventory section. The Config Properties tab displays the SD card password in the Router Credentials section.

To enable CGR SD card password protection:

1. Choose **Config > Device Configuration**.

2. Select the CGR group or CGRs to push the configuration to in the CONFIGURATION GROUPS pane.

3. Select the **Push Configuration** tab.
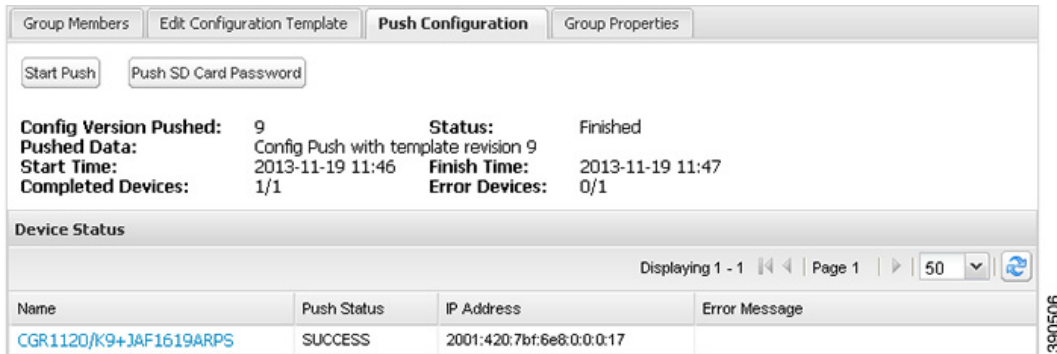
4. Click **Push SD Card Password**.

5. Select **SD Card protection > Enable**.
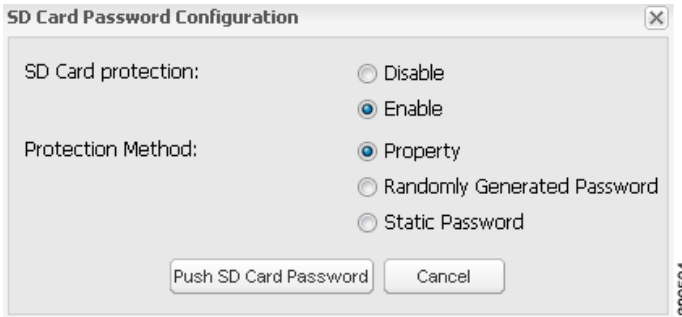
6. Select the desired protection method:

- Property: This password is set using a CSV or XML file, or using the Notification Of Shipment file.
- Randomly Generated Password: Enter the password length.
- Static Password: Enter a password.

7. Click **Push SD Card Password**.

Pushing Configurations to Endpoints

To push configuration to mesh endpoints:

1. Choose **Config > Device Configuration**.

2. Select the group or subset of a group to push the configuration to in the ENDPOINT list.

3. Click the **Push Configuration** tab.

4. Click **Start Push**.

5. Click **Yes** to confirm.

The Push Configuration page displays the status of the push operation for every device in the group. If an error occurs while pushing configuration to a device, the error and its details display in the relevant columns.

In the Status column, one of these values appear:

- NOT_STARTED—The configuration push has not started.
- RUNNING—The configuration push is in progress.
- PAUSED—The configuration push is paused. Active configuration operations complete, but those in the queue are not started.
- STOPPED—The configuration push was stopped. Active configuration operations complete, but those in the queue are not started.
- FINISHED—The configuration push to all devices is complete.
- STOPPING—The configuration push is in the process of being stopped. Active configuration operations complete, but those in the queue are not started.
- PAUSING—The configuration push is in the process of being paused. Active configuration operations complete, but those in the queue are not started.

To refresh the status information, click the **Refresh** button.

Managing a Guest OS

Cisco IOS CGRs support a virtual machine to run applications on a Guest OS (GOS) instance running beside the Cisco IOS virtual machine. The GOS is Linux. Applications running on the GOS typically collect statistics from the field for monitoring and accounting purposes. The Cisco IOS firmware bundle installs a reference GOS on the VM instance on the CGR. CG-NMS supports the following role-based features on the GOS:

- Monitoring GOS status
- Managing GOS applications
- Upgrading the reference GOS in the Cisco IOS firmware bundle

  Note: CG-NMS only supports the reference GOS provided by Cisco.

You manage and monitor a GOS on the **Config > Device Configuration** page, on the **Guest OS** tab.

Managing a Guest OS

Figure 4   Config > Device Configuration Page – Guest OS Tab Restart GOS Button
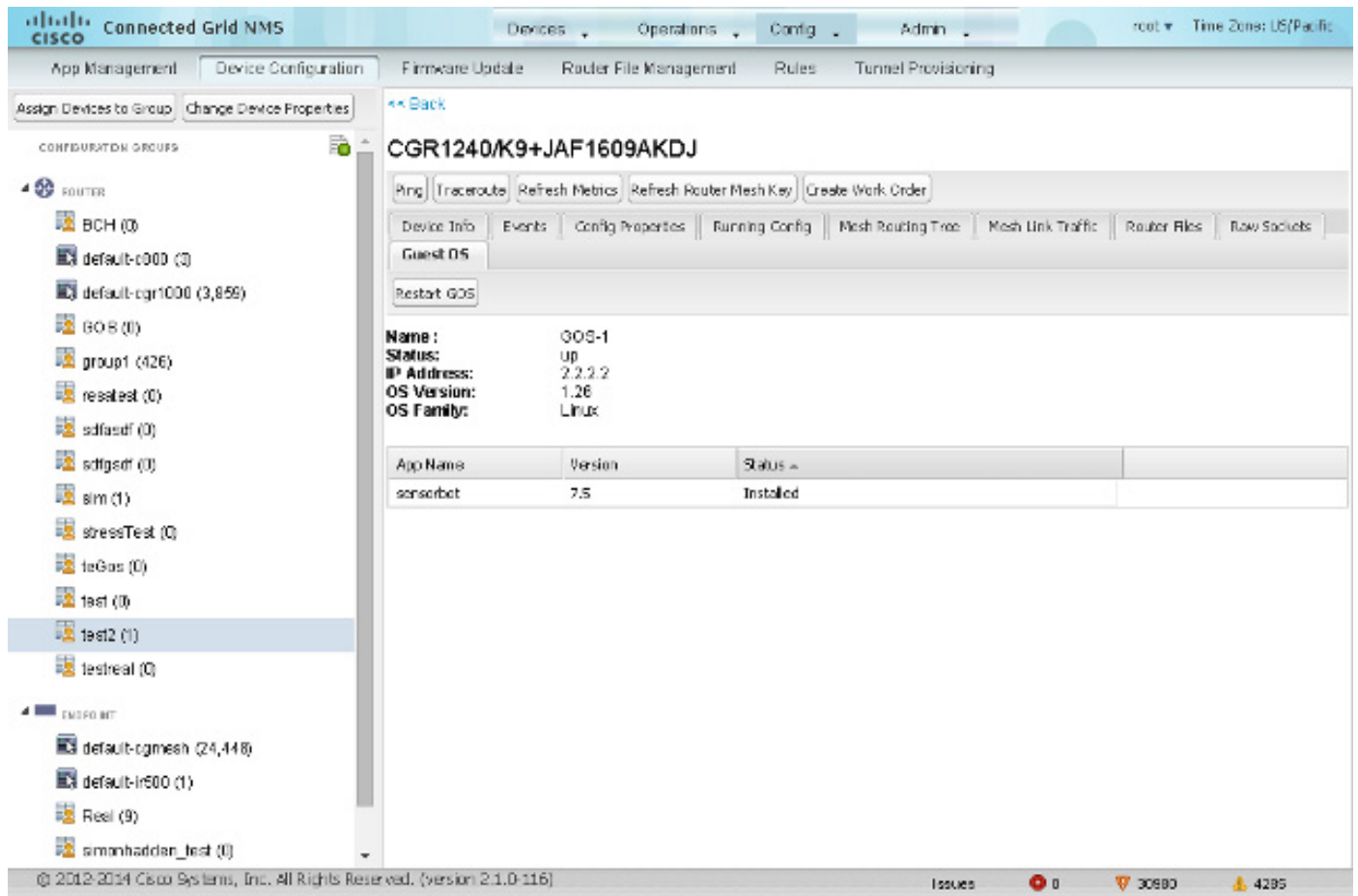
This section includes the following topics:

■ Installing a GOS

■ Managing GOS Applications

■ Restarting a Guest OS

Installing a GOS

Depending on CGR factory configuration, a GOS may be present in the VM instance. The GOS installs with the Cisco IOS firmware bundle (see "FAR Firmware Updates" section on page –219). The GOS, Hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

After any Cisco IOS install or upgrade, when CG-NMS discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest OS. See the *Cisco 1000 Series Connected Grid Routers Configuration Guides* web portal for information on configuring the CGR.

Note: If CG-NMS detects a non-Cisco OS is installed on the VM, the firmware bundle will not upload and the Cisco reference GOS will not install.

181

Managing GOS Applications

Applications (apps) run on the VM instance, but are not included in the Cisco IOS firmware bundle. You distribute GOS apps as standard *app-<appname>-ver-<version>*.zip files, and use the **Config > App Management** page to upload, install, start and stop, and uninstall GOS apps. The CG-NMS internal backup and restore mechanism preserves existing apps during upgrades.

Note: For CG-NMS GOS communications such as application uploads to the GOS using ssh, the gosPassword must be the CGR properties file. You upload the properties file in a CSV/XML upload. Without the gosPassword property, CG-NMS cannot upload apps to a GOS.

Users with the GOS Application Management role enabled can upload, install, and deploy apps on Cisco IOS CGRs within your network.

Figure 5   Config > Apps Management Page–Last Job Status

Managing GOS App Activities

You can manage app activities (jobs) on the Config > App Management **Activity Status** tab. The top pane (above the device list) displays job-related info for the last activity performed, which includes:

- The start and stop time of the last activity.

- The app name.

- The status of the activity.

- The number of devices with successful results and the number of devices with errored results.

Table 7 lists fields that display in the device list on the Activity Status tab.

Table 7   Activity Status Tab

Field	Description
Device Name	Name of the selected device.
GOS Host Name	Name of the GOS host.
App Name	Name of the app.
App Version	Version assigned to the app.
Start Time	The start for the selected activity.
Last Status Time	The last status update time.
Activity	The selected activity: Upload, Set to Run, Install, Start, Stop, Uninstall, and Delete Remote Package.
Activity Status	The status of the selected activity.
Progress	How much of the activity completed.
Message	Notes generated by the activity.
Error Details	Details on errors encountered during the activity.

On the **Activity Status** tab, you can also:

- Click the **Cancel Current Activity** button to cancel any activity. Any activity in progress can be canceled.

- Click the **Refresh Status** button to update activity status.

Uploading GOS Apps

After GOS apps are imported to CG-NMS, you can upload them for deployment on the GOS on Cisco IOS CGRs, using the **Config > Apps Management** page **Upload** tab (Figure 6). Apps are OS specific. If the GOS is Linux, any apps you upload must run on Linux.

Figure 6   Upload Tab
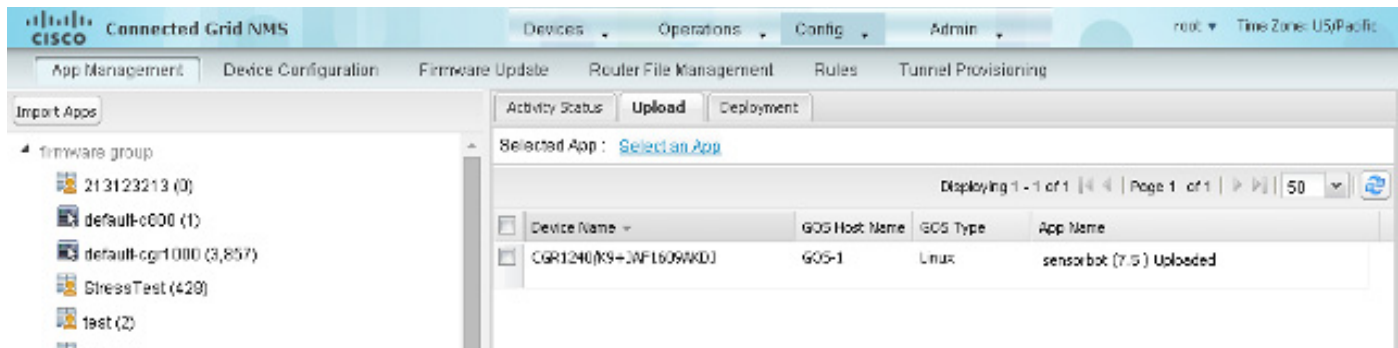
To upload apps to CG-NMS to deploy on Cisco IOS CGRs, on the **Config > Apps Management** page:

1. Select a firmware or configuration group in the left pane.

2. Click the **Upload** tab.

3. Click **Select an App** or click the **Import Apps** button in the left pane.

   The Import Apps dialog box displays apps already uploaded to the NMS server.
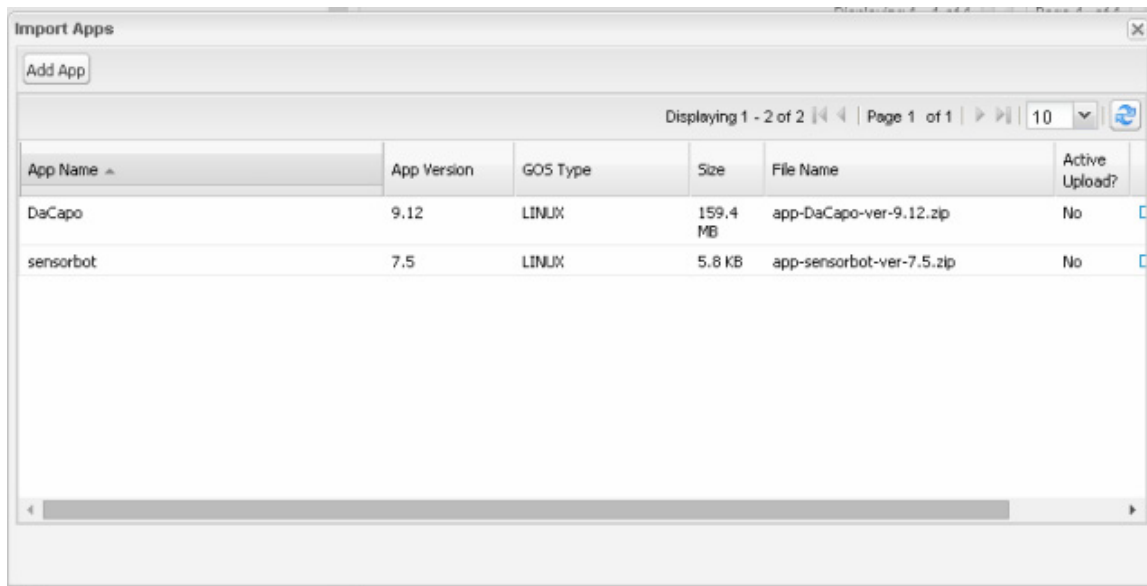
4. In the Import Apps dialog box, click **Add App**.

5. In the Add App dialog box, click **Browse** to navigate to the directory containing your app.

   Note: Apps must be in the standard *<appname>-<version>*.zip file format.

6. In the Open dialog box, select the app file, and click **Open**.

7. Click **Add File**.

   Note: Only one app may be uploaded at a time.

   The app file uploads to the NMS server and displays in the App Name list.

8. In the Add App dialog box, click the desired app to upload to CGRs, click **Add to Upload**, and click **OK**.

The app filename displays in the App Name list.

9. In the App Name list, select the desired app to upload.

   The app filename displays on the Upload tab as a link in the Selected App field, which is sensorbot 7.5 in the following example.
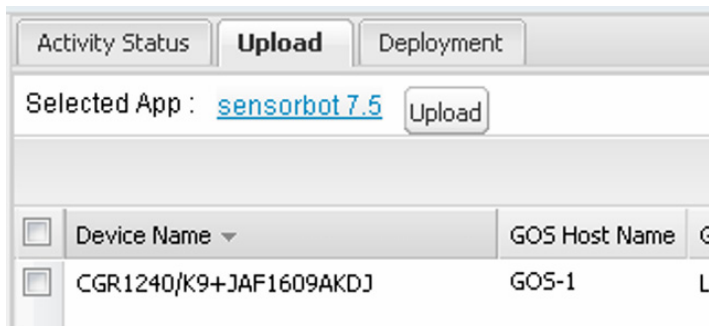
10. Click the **Upload** button to upload the file to CG-NMS.

The activity status (UPLOAD_OP_COMPLETE or UPLOAD_OP_WAITING) displays on the Upload tab.

Deploying GOS Apps

The **Config > App Management Deployment** tab allows you to perform the following activities on selected CGRs:

- Set to Run – A combination of install and start operations.

- Install – Installs the remote package and extracts the app.

- Start and Stop – Starts or stops the app.

- Uninstall – Uninstalls the app.

- Delete Remote Package – Deletes the previous upload package from the repository.

To deploy GOS apps on selected CGRs:

1. On the **Config > Apps Management** page, select a firmware or configuration group in the left pane.

2. Click the **Deployment** tab.

3. In the **Select an Action** drop-down menu, choose the desired action to perform on the selected group.
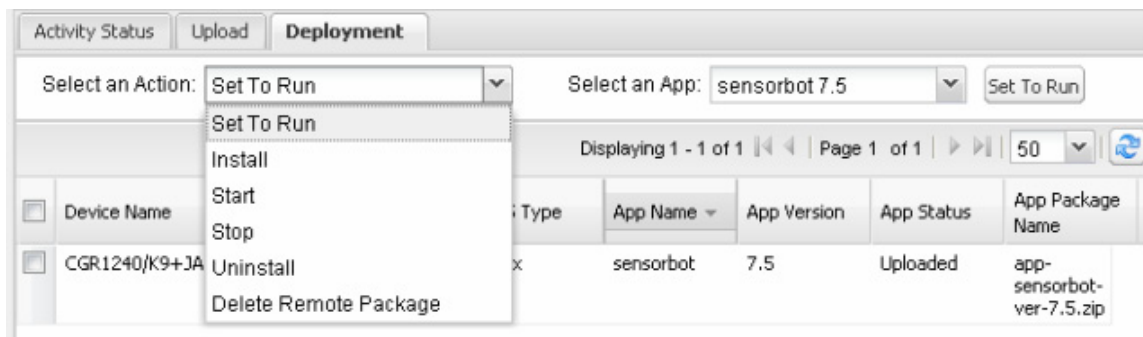
The action button at the right reflects your selected action (that is, if you select Install as the action, the action button label is "Install."

185

    4. In the **Select an App** drop-down menu, choose an app or select all apps.

    5. Click the action button.

The activity begins. You can monitor activity progress on the Activity Status tab.

Deleting GOS Apps

To delete an app from the NMS server, on the **Config > Apps Management** page:

    1. Select a firmware or configuration group in the left pane.

    2. Click the **Upload** tab.

    3. Click **Select an App** or click the **Import Apps** button in the left pane.

        The Import Apps dialog box displays apps already uploaded to the NMS server.

    4. In the **App Name** list, scroll to the right and click the **Delete** link in the row with the app to delete from the NMS server.

App Name ▲	App Version	GOS Type	Size	File Name	Active Upload?	
DaCapo	9.12	LINUX	159.4 MB	app-DaCapo-ver-9.12.zip	No	Delete
sensorbot	7.5	LINUX	5.8 KB	app-sensorbot-ver-7.5.zip	No	Delete

Import Apps — Add App — Displaying 1 - 2 of 2 — Page 1 of 1 — 10 — App to Upload
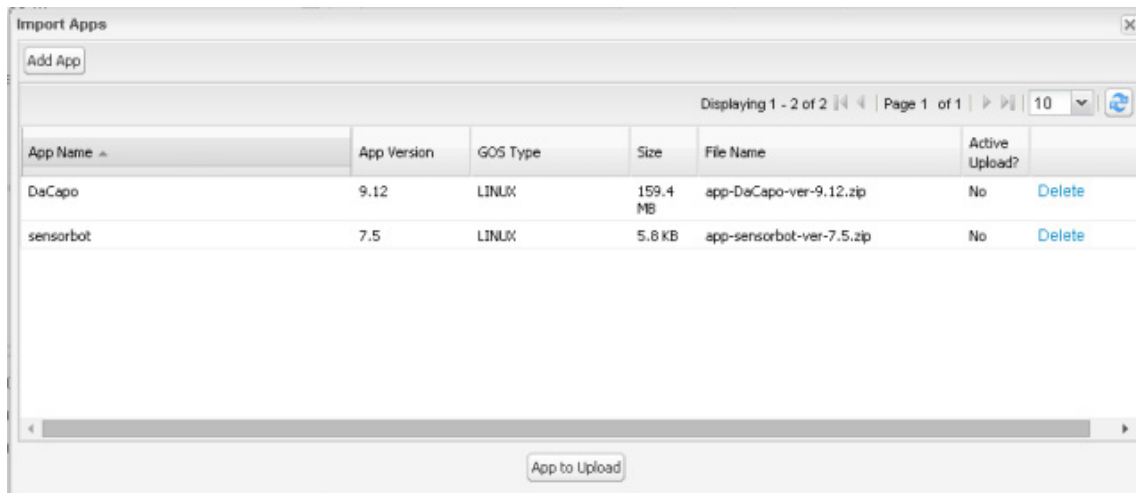
    5. Click **OK** in the confirmation dialog box.

Restarting a Guest OS

To restart a GOS, on the **Config > Device Configuration** page:

    1. In the **CONFIGURATION GROUPS** pane, select the device with the GOS to restart.

    2. Click the **Guest OS** tab.

    3. Click the Restart button ().

Managing a Guest OS

Figure 7   Config > Device Configuration Page – Guest OS Tab Restart Button
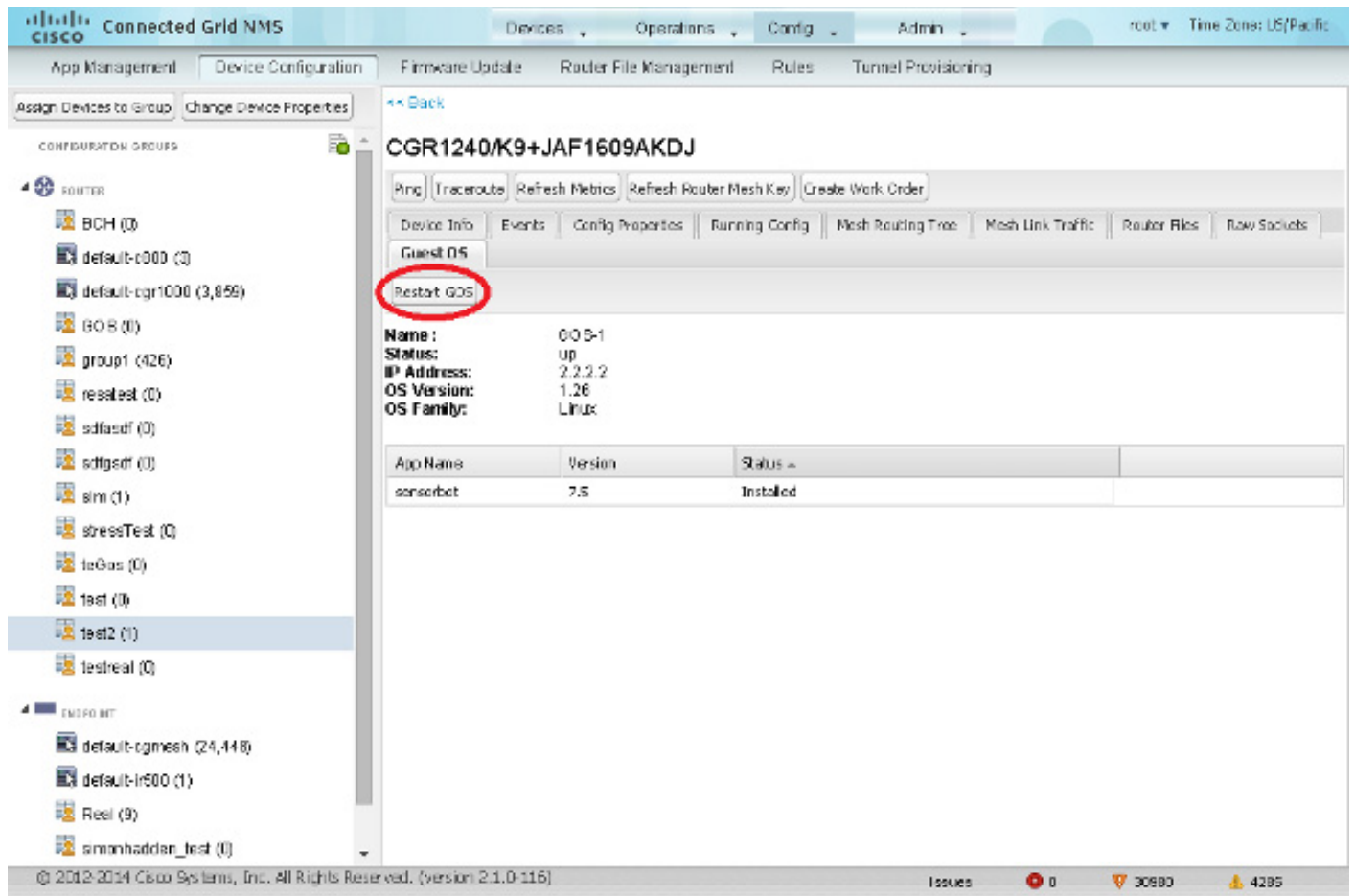
Pushing GOS Configurations

You can push the GOS configuration to the CGR using the CG-NMS config template. This is the only way to configure the DHCP pool.

...

Managing Files

Use the **Config > Router File Management** page to transfer and execute dual backhaul and Embedded Event Manager (EEM) scripts on the FAR. The Template module performs file validation. This section includes the following topics:

- File Types and Attributes

- Adding a File to CG-NMS

- Transferring Files

- Viewing Files

- Monitoring Files

- Monitoring Actions

- Deleting Files

Note: File management is role-dependent and may not be available to all users. See Managing Roles.

File Types and Attributes

Two types of EEM scripts are used on the FAR: an embedded applet, and Tool Command Language (TCL) scripts that execute on the FAR individually. You can upload and run new EEM TCL scripts on the FAR without doing a firmware upgrade. EEM files upload to the *eem* directory in FAR flash memory. These scripts display in the **Import File** page File Type column as *eem script*. You must edit the configuration template file to activate the EEM TCL scripts (see Editing the ROUTER Configuration Template). This feature works with all FAR OS versions currently supported by CG-NMS.

You can also transfer other file types to the FAR for better file management capability. You must first import the files to CG-NMS to upload files to the FAR. CG-NMS processes the file and stores it in the CG-NMS database with the following attributes:

- Filename

- Description

- Import Date/Time

- Size

- Sha1 Checksum

- MD5 Checksum

- File Content

Adding a File to CG-NMS

To add a file to CG-NMS:

1. On the **Config > Router File Management** page, click **Import Files** or **Upload** to open the Select File from List dialog box.

Managing Files
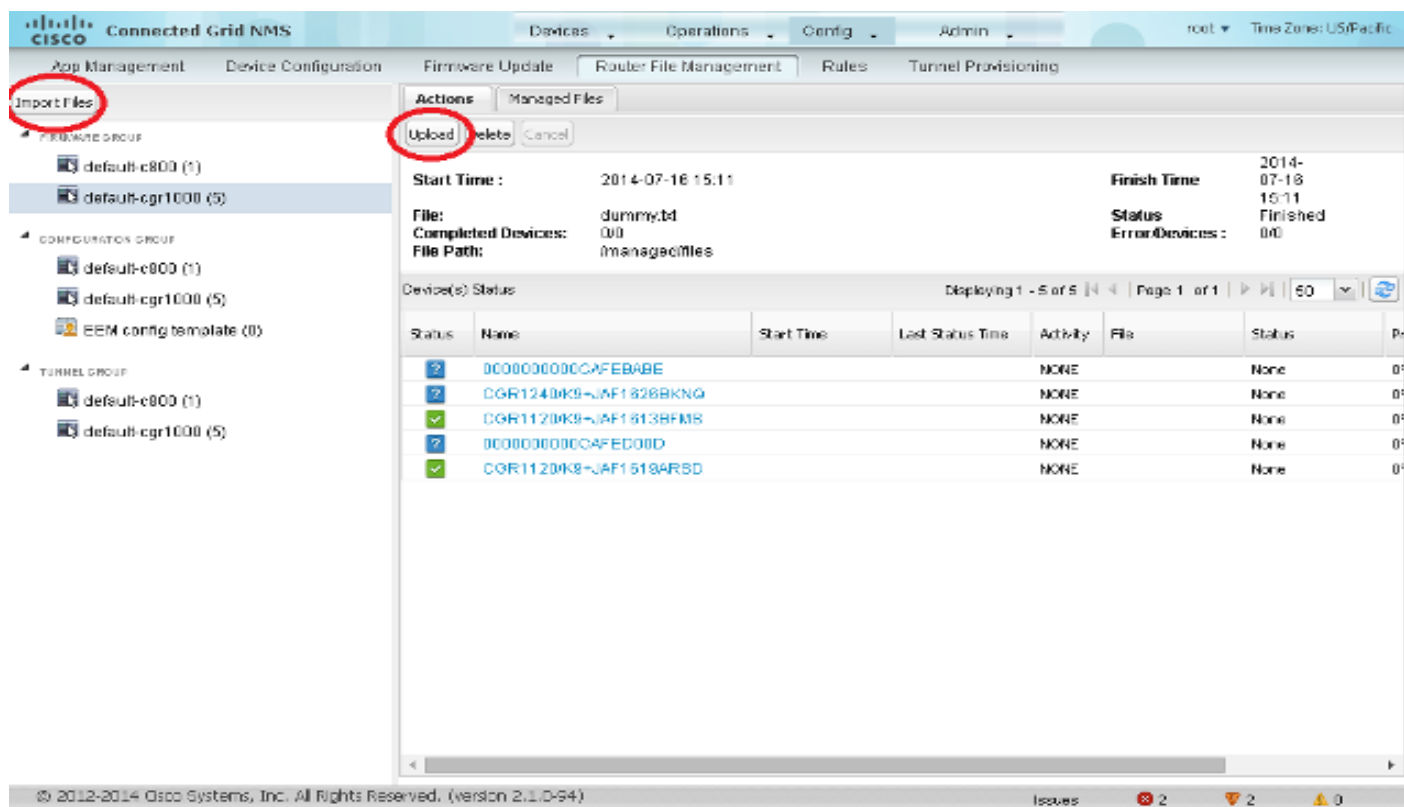
2. Click **Add File** and browse to the file location.

   Note: The maximum import file size is 200 MB.
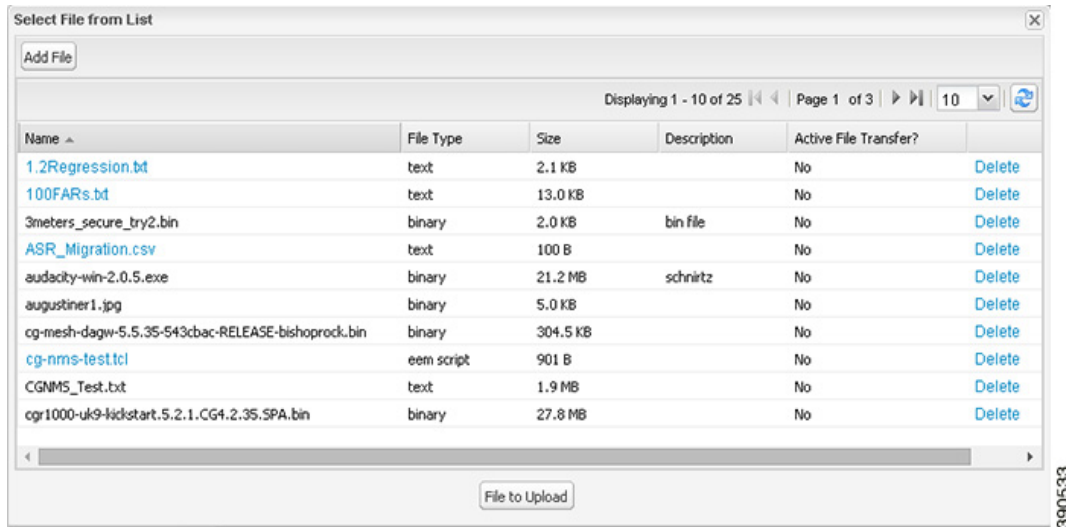
Note: In the **Select File from List** dialog box, you can also delete imported files from the CG-NMS database if the file is not in an active file transfer. This only removes the file from the CG-NMS database, not from any FARs that contain the file. Click the Name hyperlink to view uploaded text files (file size must be less than 100KB).

3. (Optional) Type a description for the file.
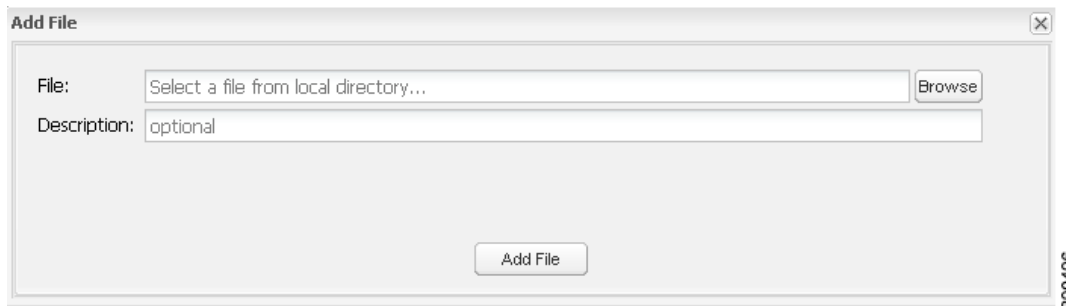
4. Click **Add File**.

When the upload completes, the file name displays in the Select File From List dialog box.

5. Repeat steps 2 through 4 to add another file, or see Transferring Files to upload the file to the selected device or group, or close the Select File From List dialog box.

Transferring Files

You can transfer files from the NMS database to any firmware, configuration or tunnel provisioning group, or to individual FARs. The maximum import file size is 200 MB.

To perform a file transfer:

1. On the **Config > Router File Management** page, select the group to transfer the file to in the **Browse Devices** pane.

2. Click **Import Files** or **Upload** on the **Actions** tab.

Managing Files
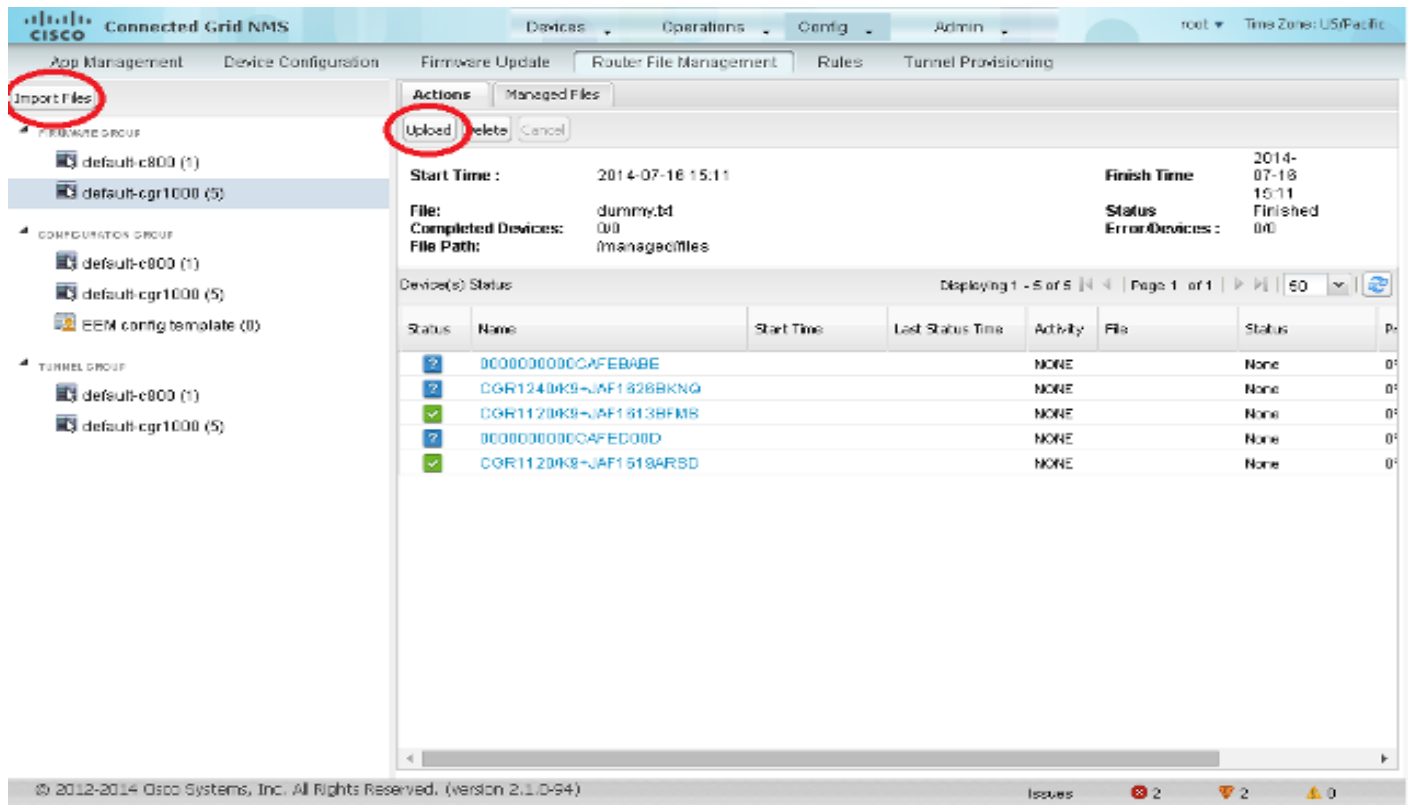
The **Select File from List** dialog box displays.
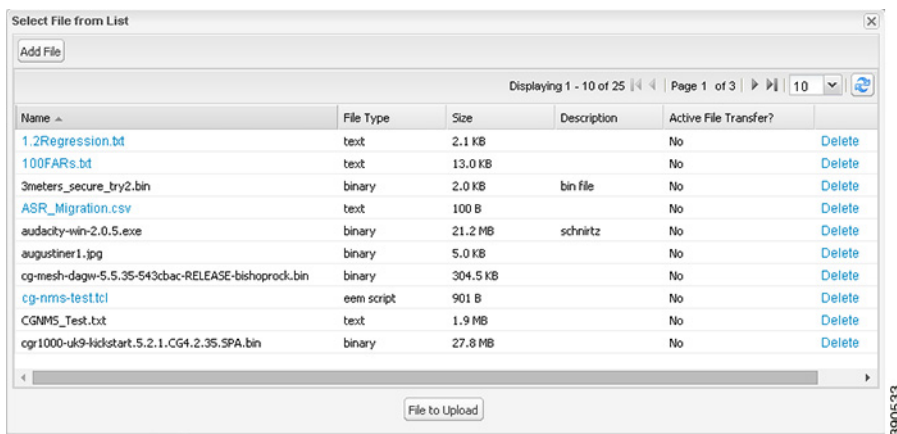
3. Select the file to transfer to the FARs in the selected group.

4. Click **File to Upload**.

The **Upload File to Routers** dialog box displays.

Managing Files
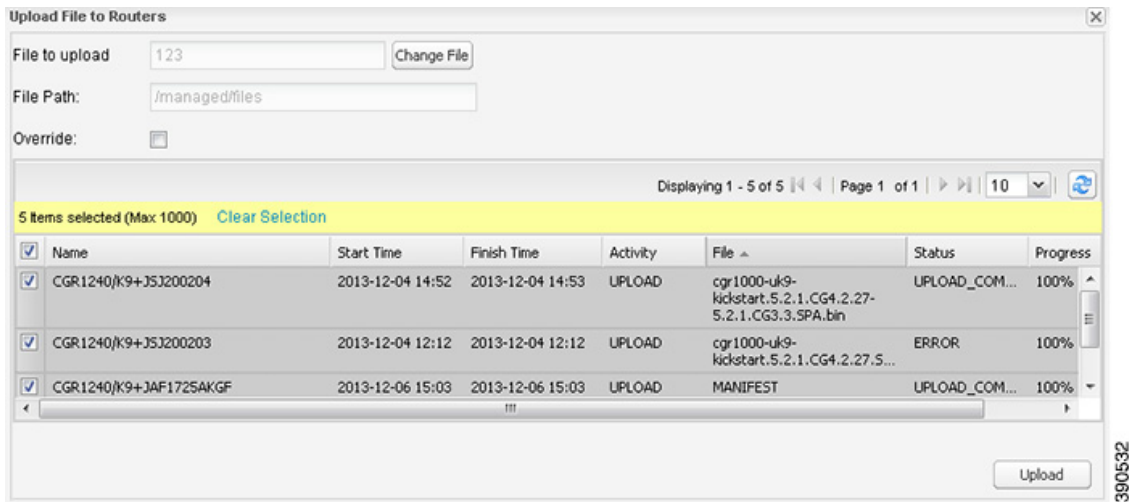
5. Check the check boxes of the FARs to which you want to transfer the file.

6. Click **Upload**.

If there is no file transfer or deletion, configuration push, firmware upload, or install or reprovision operations in progress for the group, the upload starts.

You can choose to transfer files to all FARs in the selected group or select only a subset of the FARs in the group. You can also select another group and file to perform a separate file transfer or deletion simultaneously.

All files transferred from CG-NMS reside on the FAR in flash:/managed/files/ for Cisco IOS CGRs, and bootflash:/managed/files/ for CG-OS CGRs.

The status of the last file transfer is saved with the group, as well as the operation (firmware update, configuration push, and so on) and status of the group.

Viewing Files

To view imported text file content:

1. Click the EID link to display the Device Info pane.

2. Click the **Router Files** tab.

Managing Files
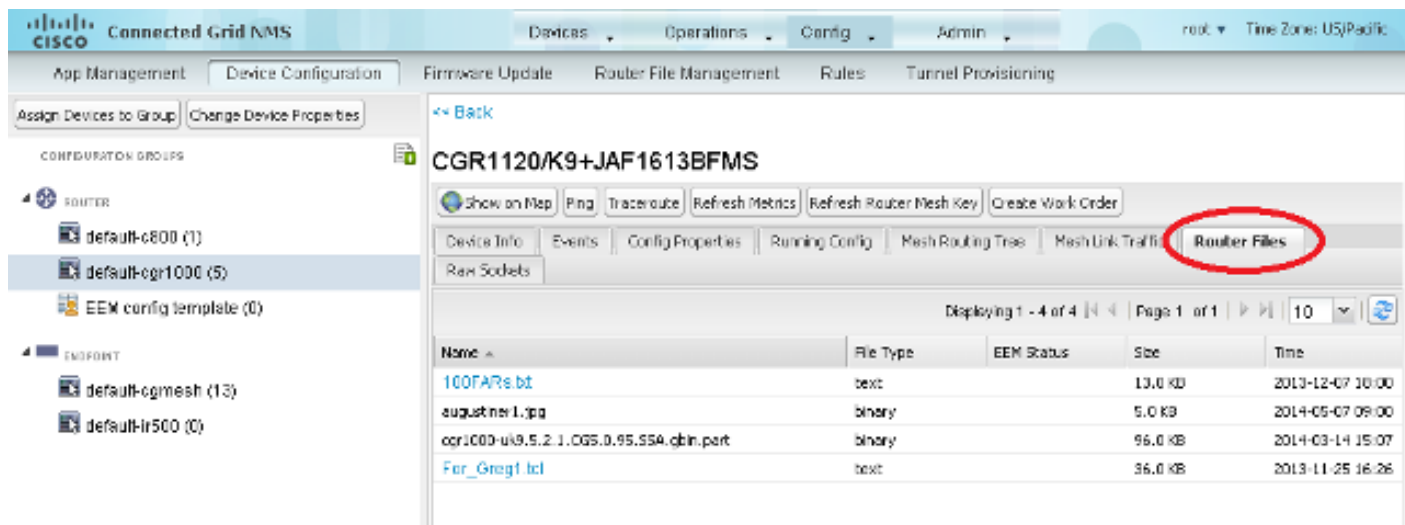
3. Click the file name link to view the content in a new window.

   Note: CG-NMS only displays files saved as plain text that are under 100 KB are viewable. You cannot view larger text files or binary files of any size. Those file types do not have a hyperlink.
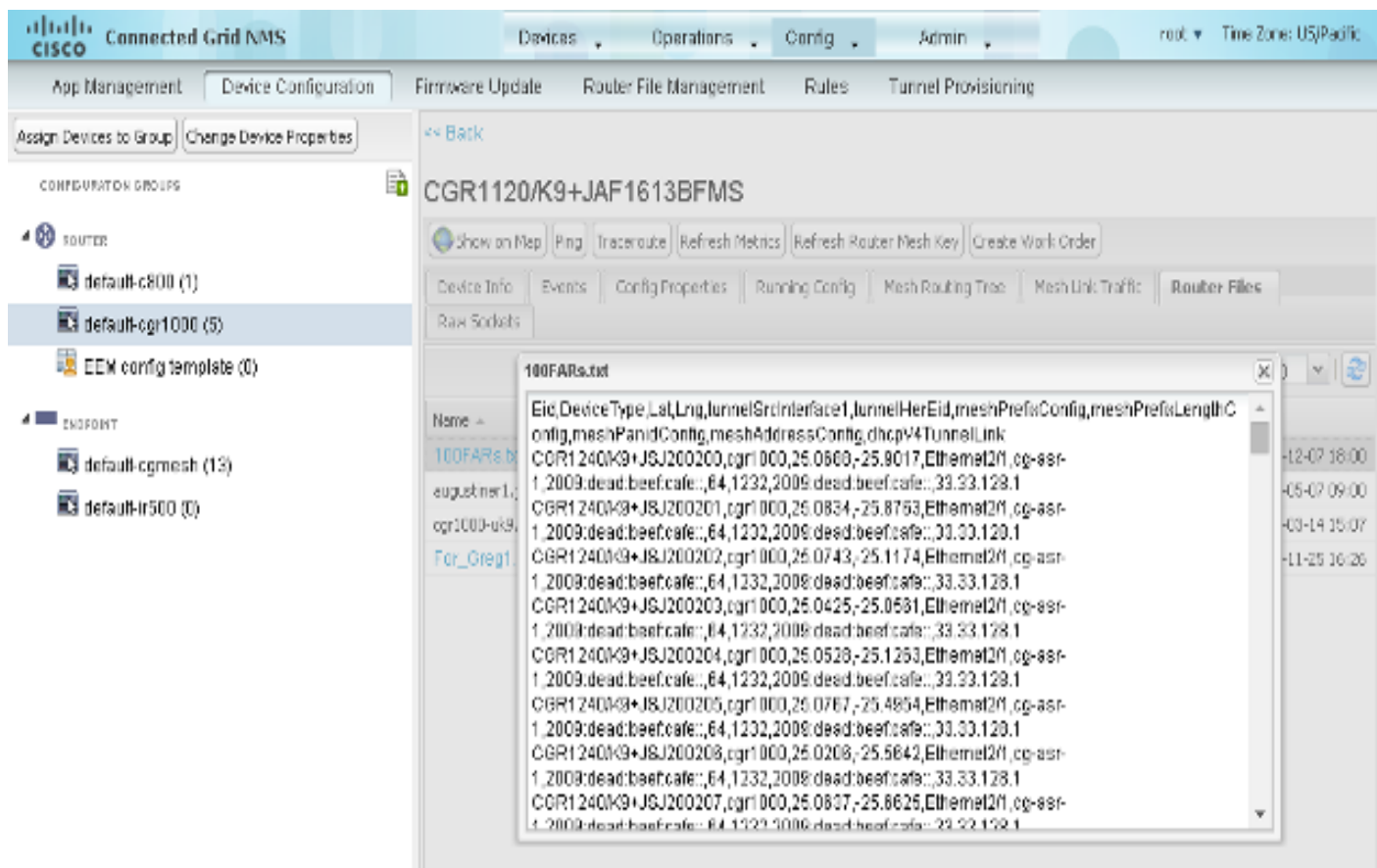
Monitoring Files

On the **Config > Router File Management** page, click the **Managed Files** tab to view a list of FARs and the files uploaded to their .../managed/files/ directories. Devices listed in the main pane are members of the selected group.

Figure 8   Managed Files Tab

The following information is included in this list:

- EID link to the Device Info page

- Number of files stored on the device

- Uploaded file names

You can use the **Filter By File Name** drop-down menu to only view devices that contain a particular file. Select **All** to include all devices in the group. Click the refresh button to update the list during file transfer or deletion processes.

Monitoring Actions

On the **Config > Router File Management** page, click the **Actions** tab to view the status of the last file transfer or last file deleted for FARs in the selected group. You can click the Cancel button to terminate any active file operation.

Figure 9   Actions Tab
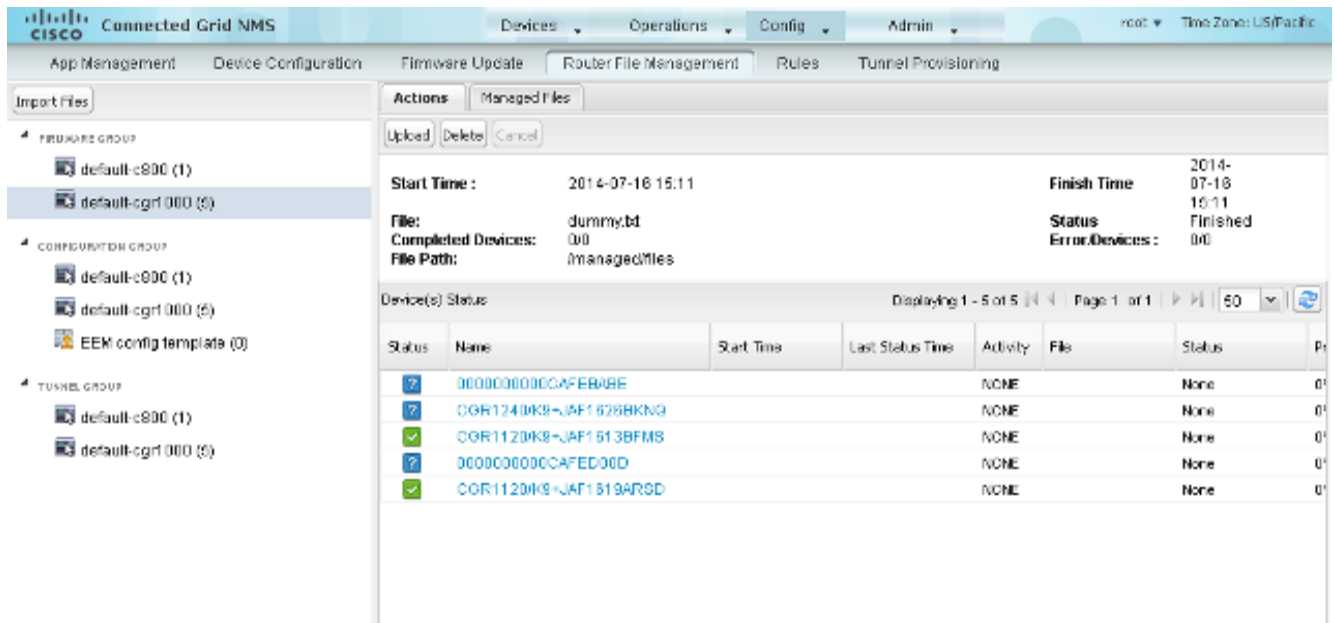
The Actions tab lists the following attributes:

■ Start date and time of the last transfer

■ End date and time of the last transfer

■ File name

■ Status of the process: UNKNOWN, AWAITING_DELETE, DELETE_IN_PROGRESS, DELETE_COMPLETE, CANCELLED, NOTSTARTED, UPLOAD_IN_PROGRESS, UPLOAD_COMPLETE, STOPPING, STOPPED

■ Number of devices with upload complete and total number of target devices

■ Number of errors and errored device count

■ File path

■ EID link to Device Info page

■ Activity performed: UPLOAD, DELETE, NONE

■ Progress percentage

■ Messages regarding any issues discovered during the process

■ Error details

Deleting Files

To delete files from FARs:

1. On the **Config > Router File Management** page, select the group to transfer the file to in the **Browse Devices** pane.

2. On the **Actions** tab, click **Delete**.

3. In the **Delete file from List** dialog, select a file to delete.

195
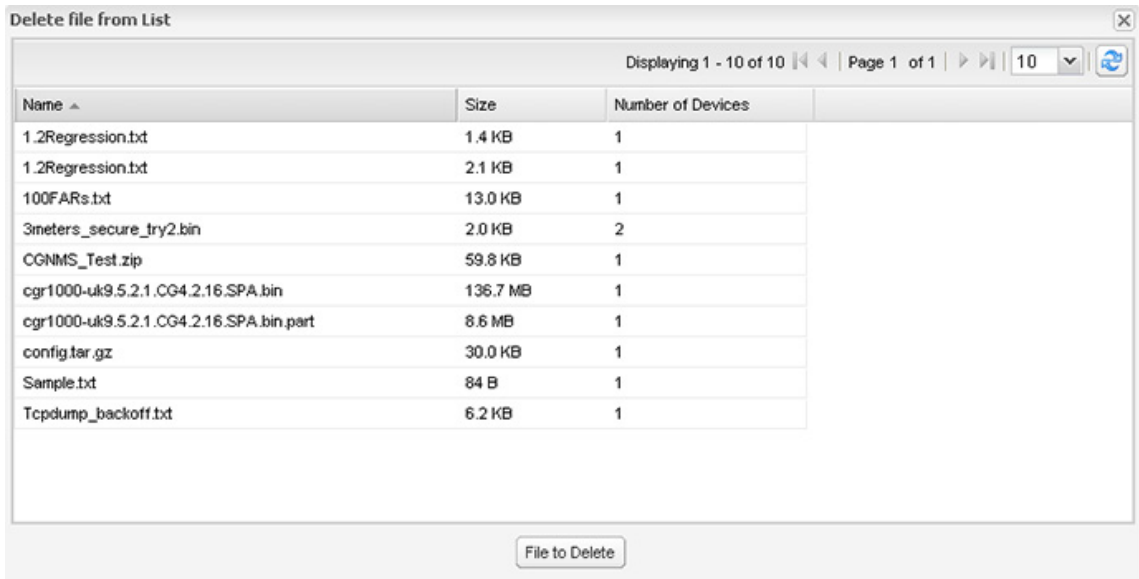
You can delete the file from all FARs in the selected group or any subset of FARs in the group.

4. Click **File to Delete**.

The **Delete File from Routers** dialog box displays.
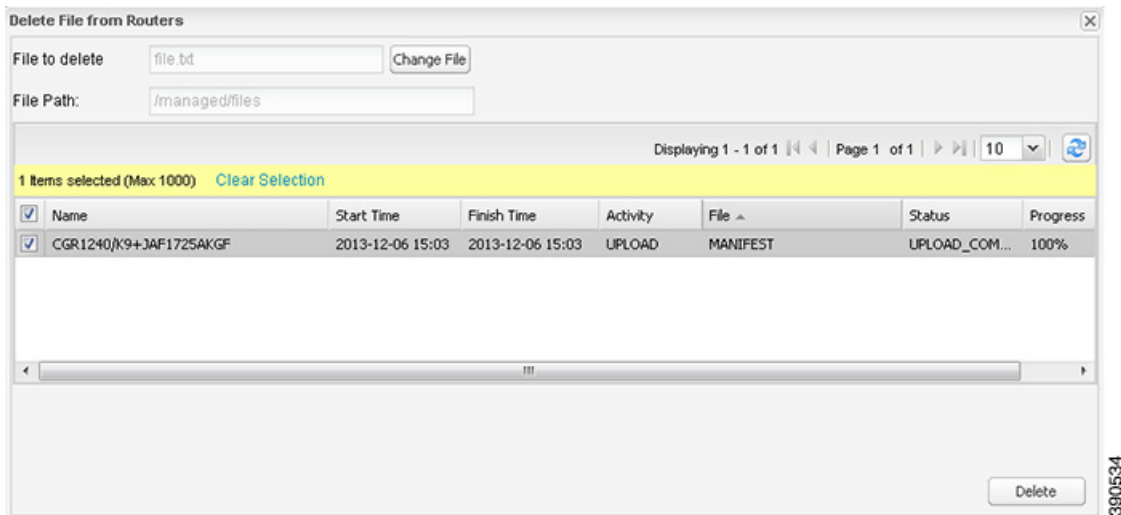
5. Check the check boxes of the FARs from which you want to delete the file.

- You can click Change File to select a different file to delete from the selected FARs.

- You can select multiple FARs.

- Only one file can be deleted at a time.

6. Click **Delete**.

If there are no file transfer or deletion, configuration push, firmware upload, or install or reprovision operations in progress for the group, the delete operation begins. CG-NMS searches the .../managed/files/ directory on the devices for the specified file name.

Note: On deletion, all file content is purged from the selected devices, but not from the CG-NMS database. File clean-up status displays for the selected group.

You can select another group and file to perform a separate file deletion while file transfer or deletion processes are in progress for this group. When you cancel file deletion processes before they complete, the currently running file deletion process completes and all waiting file deletion processes are canceled.

Managing Work Orders

- Viewing Work Orders

- Creating User Accounts for Device Manager (CGDM) Users

- Creating Work Orders

- Editing Work Orders

- Deleting Work Orders

Note: The Work Orders feature works with Release 3.0 or later of CGDM. For integration instructions, see *"Accessing Work Authorizations"* in the *Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1*, or *"Managing Work Orders"* in the *Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1*.

Note: If you are using CGDM Release 3.1, you must enable SSLv3 for CGDM-CG-NMS connection authentication:

1. Stop CG-NMS:

   ```
   service cgms stop
   ```

2. Replace **protocol="TLSv1"** attribute with the **protocol="TLSv1,SSLv3"** attribute in the following files:

   - /opt/cgms/standalone/configuration/standalone.xml
   - /opt/cgms/standalone/configuration/standalone-cluster.xml

3. Start CG-NMS:

   ```
   service cgms start
   ```

Viewing Work Orders

To view work orders in CG-NMS, choose **Operations > Work Orders**.

Table 8 lists fields that display on the Work Orders page.

Table 8   Work Orders Page Fields

Field	Description
Work Order Number	Unique identifier of the work order.
Work Order Name	Name of the work order.
Role	(CG-OS only) Role of the user assigned to the work order: tech, admin, or viewer.
FAR Name	EID of the FAR associated with the work order.
Technician User Name	User name of the assigned technician.
Time Zone	The time zone where the FAR is located–*not* the user's time zone. This value is deployment dependent, and can match the user's time zone.
Start Date	Project start and end date allotted to the field technician.
End Date	
Last Update	Time of last work order status update.
Status	Work order status. Valid status values are: New, Assigned, InService, Completed, Incomplete, or Expired.

Searching Work Orders

To refine your search, use the following syntax in the Search Work Order field (**Operations > Work Orders**):

Parameter	Description
workOrderNumber	Unique identifier of the work order.
role	(CG-OS only) Role of the user assigned to the work order. Valid roles are: tech, admin, or viewer.
technicianUserName	User name of the technician assigned to the work order.
workOrderStatus	Status of the work order. Valid status labels are: New, Assigned, InService, Completed, Incomplete, or Expired.
eid	EID of the FAR associated with the work order.

For example, to search for completed work orders that have a user with an admin role assigned to them, use this syntax:

role:admin workOrderStatus:Completed

To search work orders in CG-NMS:

1. Choose **Operations > Work Orders**.

2. In the Search Work Order field, enter the search syntax and click **Search Work Orders**.

Creating User Accounts for Device Manager (CGDM) Users

Before creating work orders, you must create user accounts for the field technicians who use CGDM to download work orders from CG-NMS.

To create a Device Manager user account:

1. If not defined, create a Device Manager User role:

    a. Choose **Admin > Access Management > Roles**.

        b. Click **Add**.

        c. (CG-OS only)) In the Role Name field, enter a name for the role.

        d. Check the check box for **Device Manager User**, and then click **Save**.

    2. Create the user account:

        a. Choose **Admin > Access Management > Users**, and then click **Add**.

        b. Configure the user name, password, and time zone information.

        c. Check the check boxes for **Monitor Only** and the Device Manager User role you created in Step 1.

        d. Click **Save**.

Creating Work Orders

If you need a technician to inspect a deployed FAR in the field, create a work order. A work order includes the WiFi credentials required for the technician to connect to the router.

BEFORE YOU BEGIN

- Your user account must have the Work Order Management permissions enabled.

- To provide a signed work order to CGDM on request, you must import CGDM certificates to cgms_keystore using the alias cgms.

- Create the user account for the field technician. (See Creating User Accounts for Device Manager (CGDM) Users)

Note: You can only create work orders for CGRs.

DETAILED STEPS

To create a work order for FARs:

    1. Choose **Operations > Work Orders**.

    2. Click **Add Work Order**.

3. In the **Work Order Name** field, enter the name of the work order.

4. In **the Field Device Names/EIDs** field, enter a comma-separated list of FAR names or EIDs.

   For every FAR in the list, CG-NMS creates a work order (one work order per FAR).

5. In the **Device User Name** field, enter the CGDM name of the technician.

6. In the **Device Type** field, select **Router** or **Endpoint**.

7. Click the radio button of the operating system type for the CGR: **CG-OS** or **IOS**.

8. This step is OS-specific:

CG-OS CGRs

    a. In the **Role** field, click the radio button for the user role required to access the work order:

      – **Admin**—Uses CGDM to view and download work orders from CG-NMS, and change the FAR configuration.

      – **Tech**—Uses CGDM to view and download work orders from CG-NMS and bring up/down FAR network interfaces, but cannot change the FAR configuration.

      – **Viewer**—Only uses CGDM to view work orders.

    b. Complete the **Technician User Name** field.

Cisco IOS CGRs

    a. In the **Device User Name** field, enter the user name the technician uses to access the device.

9. From the **Technician User Name** drop-down menu, choose their CG-NMS user name.

   This menu only lists users with CGDM User permissions enabled.

10. From the **Status** drop-down menu, choose the status of the work order (**New**, **Assigned**, **In Service**, **Completed**, or **InComplete**).

Note: For a CGDM user to retrieve a work order, the work order must be in the *Assigned* state in CG-NMS for that user. If the work order is in any other state, CGDM cannot retrieve the signed work order.

Note: After the work order has been successfully requested by the CGDM user, the state of work order changes to In Service.

11. In the **Start Date** and **End Date** fields, specify the starting and ending dates for which the work order is valid.

   If the work order is not valid, the technician cannot access the router.

12. In the **Device Time Zone** field, choose the time zone of the device from the drop-down menu.

13. Click **Save**.

14. Click **OK**.

You can also create work orders on the Field Devices page (**Devices > Field Devices**), as described in Creating Work Orders, and on the Device Info page.

Downloading Work Orders

To download the work orders created by CG-NMS, field technicians use Cisco CGDM, a Windows-based application that field technicians use to manage a single Cisco CGR 1000 router. The technician can download all work orders in the *Assigned* state.

Field technicians use CGDM to update work order status, which is sent to CG-NMS.

Note: Certificates are not included in the work order and are preinstalled on the CGDM field laptop prior to downloading work orders from CG-NMS.

For more information about CGDM, see the *Cisco Connected Grid Device Manager User Guide*.

Editing Work Orders

To edit work order details:

1. Choose **Operations > Work Orders**.

2. Select the work order to edit, and then click **Edit Work Order**.

   Alternatively, click the work order number to open the page displaying the work order details.

3. Click **Save**.

Deleting Work Orders

To delete work orders:

1. Choose **Operations > Work Orders**.

2. Check the check box of the work orders to delete.

3. Click **Delete Work Order**.

4. Click **Yes**.

Device Properties

This section describes the device properties that you can view in CG-NMS. Some of these properties are configurable; others are not.

- Types of Device Properties

- Device Properties by Category

Types of Device Properties

CG-NMS stores two types of device properties in its database:

- Actual device properties—These are the properties defined by the device, such as IP Address, Transmit Speed, and SSID.

- CG-NMS device properties—These are properties defined by CG-NMS for devices, such Latitude and Longitude properties, which CG-NMS uses to display device locations on its GIS map.

  Note: The Key column provides the version of the property name in the CG-NMS database that you can use in filters. For example, to search for the device with an IP address of 10.33.0.30, enter **ip:10.33.0.30** in the Search Devices field.

Device Properties by Category

This section presents CG-NMS device properties by category:

- Cellular Link Settings

- Cellular Link Metrics

- DA Gateway Properties

- Dual PHY WPAN Properties

- Ethernet Link Metrics

- Guest OS Properties

- Head-End Routers > Netconf Config

- Head-End Routers > Tunnel 1 Config

- Head-End Routers > Tunnel 2 Config

- Inventory

- Mesh Device Health

- Mesh Link Keys

- Mesh Link Settings

- Mesh Link Metrics

- PLC Mesh Info

- Raw Sockets Metrics and Sessions

- Router Battery

- Router Config

Device Properties

- **Router Credentials**

- **Router DHCP Proxy Config**

- **Router Health**

- **Router Tunnel Config**

- **Router Tunnel 1 Config**

- **Router Tunnel 2 Config**

- **SCADA Metrics**

- **WiMAX Link Metrics**

- **WiMAX Link Settings**

Every device in CG-NMS presents a list of fields, which are used for device searches. The available fields for a device are defined in the **Device Type** field. Fields are either configurable or discovered. Configurable fields are set using XML and CSV files; the device EID is the lookup key. Discovered fields are presented from the device. Fields are also accessible in the device configuration templates for FARs.

Cellular Link Settings

Table 9 lists the fields in the Cellular Link area of the Device Info view.

Table 9   Cellular Link Settings Area Fields

Field	Key	Configurable?	Description
Cellular Network Type	N/A	Yes	Defines the type of cellular network for example, GSM or CDMA.
Module Status	cellularStatus	No	Displays whether the cellular interface module is active in the network. There is also an unknown state for the module.
Network Name	–	Yes	Defines the service provider name for example, AT&T or Verizon.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cell ID	cellularID	No	Displays the cell ID for the cellular interface. This value must exist to activate the interface.
Cellular SID	cellularSID	No	Displays the System Identification Number for the CDMA cellular area.
Cellular NID	cellularNID	No	Displays the Network Identification Number, for the CDMA cellular area.
Cellular Roaming Status	cellularRoamingStatus	No	Indicates whether the modem is in the home network or roaming.
Cellular Modem Serial Number	cellularModemSerialNumber	No	Displays the serial number of the connected modem.

Table 9   Cellular Link Settings Area Fields (continued)

Field	Key	Configurable?	Description
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the Cellular module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: ■ Packet switched ■ Circuit switched
Location Area Code	locationAreaCode	No	Displays the Location Area Code (LAC) given by the base station.
Routing Area Code	routingAreaCode	No	Displays the routing area code given by the base station.
IMSI	cellularIMSI	No	The International Mobile Subscriber Identity (IMSI) identifies an individual network user as a 10-digit decimal value within a GSM and CDMA network. Possible values are: ■ 10-digit decimal value ■ Unknown
IMEI	cellularIMEI	No	Displays the International Mobile Equipment Identity (IMEI) for the cellular interface within a GSM network only. The IMEI value is a unique number for the cellular interface.

Cellular Link Metrics

Table 10 describes the fields in the Cellular Link Metrics area of the Device Info view.

Table 10 Cellular Link Metrics Area Fields

Field	Key	Description
Transmit Speed	cellularTxSpeed	Displays the average speed (bits/sec) of data transmitted by the cellular interface over the cellular uplink for a defined period (such as an hour).
Receive Speed	cellularRxSpeed	Displays the average speed (bits/sec) of data received by the cellular interface from the cellular uplink for a defined period (such as an hour).
RSSI	cellularRssi	Indicates the radio frequency (RF) signal strength of the cellular uplink. Valid values are 0 to -100. The LED states on the cellular interface and corresponding RSSI values are: ■ Off: RSSI < = -110 ■ Solid amber: -100 < RSSI <= -90 ■ Fast green blink: -90 < RSSI <= -75 ■ Slow green blink: -75 < RSSI <= -60 ■ Solid green: RSSI > -60
Bandwidth Usage (Current Billing Cycle)	CellBwPerCycle (bytes)	Displays current bandwidth usage (in bytes) of a particular route for the current billing cycle.

DA Gateway Properties

Table 11 describes the fields in the DA Gateway area of the Device Info view.

Table 11 DA Gateway Metrics Area Fields

Field	Key	Description
SSID	–	The mesh SSID.
PANID	–	The subnet PAN ID.
Transmit Power	–	The mesh transmit power.
Security Mode	–	Mesh Security mode: ■ 0 indicates no security mode set ■ 1 indicates 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK

Table 11   DA Gateway Metrics Area Fields (continued)

Field	Key	Description
Mesh Tone Map Reverse Modulation	–	Mesh tone map reverse modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	–	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	–	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	–	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	–	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	–	IPv6 address for Map-T settings.
Map-T IPv4 Address	–	IPv4 address for Map-T settings.
Map-T PSID	–	Map-T PSID.
Active Link Type	–	Link type of the physical link over which device communicates with other devices including CG-NMS.

Dual PHY WPAN Properties

Table 12 describes the fields in the Dual PHY area of the Device Info view.

Table 12   Dual PHY Metrics Area Fields

Field	Key	Description
SSID	ssid	The mesh SSID.
PANID	panid	The subnet PAN ID.
Transmit Power	txpower	The mesh transmit power.
Security Mode	–	Mesh Security mode: ■ 0 = No security mode set ■ 1 = 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK

Table 12   Dual PHY Metrics Area Fields (continued)

Field	Key	Description
Mesh Tone Map Reverse Modulation	–	Mesh tone map reverse modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	–	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	–	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	–	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	–	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	–	IPv6 address for Map-T settings.
Map-T IPv4 Address	–	IPv4 address for Map-T settings.
Map-T PSID	–	Map-T PSID.
Active Link Type	–	Link type of the physical link over which device communicates with other devices including CG-NMS.

Ethernet Link Metrics

Table 13 describes the fields in the Ethernet link traffic area of the Device Info view.

Table 13   Ethernet Link Metrics Area Fields

Field	Key	Description
Transmit Speed	ethernetTxSpeed	Indicates the average speed (bits/sec) of traffic transmitted on the Ethernet interface for a defined period of time.
Receive Speed	ethernetRxSpeed	Indicates the average speed (bits/sec) of traffic received on the Ethernet interface for a defined period of time.
Transmit Packet Drops	ethernetTxDrops	Indicates the number of packets dropped (drops/sec) when the transmit queue is full.

Guest OS Properties

Table 14 describes the fields in the Guest OS Properties area of the Config Properties page.

Table 14   Guest OS Properties Fields

Field	Key	Description
GOS Password	–	Password to access the GOS.
DHCPv4 Link for Guest OS Gateway	–	The DHCPc4 gateway address.

Table 14   Guest OS Properties Fields

Field	Key	Description
Guest OS IPv4 Subnet mask	–	The IPv4 subnet mask address.
Guest OS Gateway IPv6 Address	–	The IPv6 gateway address.
Guest OS IPv6 Subnet Prefix Length	–	The IPv6 subnet prefix length.

Head-End Routers > Netconf Config

Table 15 describes the fields in the Netconf Client area of the **Head-End Routers > Config Properties** page.

Table 15   Head-End Routers > Netconf Config Client Fields

Field	Key	Configurable?	Description
Netconf Username	netconfUsername	Yes	Identifies the username to enter when establishing a Netconf SSH session on the HER.
Netconf Password	netconfPassword	Yes	Identifies the password to enter when establishing a Netconf SSH session on the HER.

Head-End Routers > Tunnel 1 Config

Table 16 describes the fields in the Tunnel 1 Config area of the **Head-End Routers > Config Properties** page.

Table 16   Head-End Routers > Tunnel 1 Config Fields

Field	Key	Configurable?	Description
IPsec Tunnel Source 1	ipsecTunnelSrc1	Yes	Identifies the source interface or IP address of IPsec tunnel 1.
IPsec Tunnel Dest Addr 1	ipsecTunnelDestAddr1	Yes	Identifies the destination interface or IP address of IPsec tunnel 1.
GRE Tunnel Source 1	greTunnelSrc1	Yes	Identifies the source interface or IP address of GRE tunnel 1.
GRE Tunnel Dest Addr 1	greTunnelDestAddr1	Yes	Identifies the destination interface or IP address of GRE tunnel 1.

Head-End Routers > Tunnel 2 Config

Table 17 describes the fields in the Tunnel 2 Config area of the **Head-End Routers > Config Properties** page.

Table 17   Head-End Routers > Tunnel 2 Config Device Fields

Field	Key	Configurable?	Description
IPsec Tunnel Source 2	ipsecTunnelSrc2	Yes	Identifies the source interface or IP address of IPsec tunnel 2.
IPsec Tunnel Dest Addr 2	ipsecTunnelDestAddr2	Yes	Identifies the destination interface or IP address of IPsec tunnel 2.
GRE Tunnel Source 2	greTunnelSrc2	Yes	Identifies the source interface or IP address of GRE tunnel 2.
GRE Tunnel Dest Addr 2	greTunnelDestAddr2	Yes	Identifies the destination interface or IP address of GRE tunnel 2.

Device Properties

Inventory

Table 18 describes the fields in the Inventory area of the Device Info page.

Table 18   Inventory Fields

Field	Key	Configurable?	Description
Config Group	configGroup	Yes	The name of the configuration group to which the device belongs.
Device Category	deviceCategory	No	This field lists the type of device.
Device Type	deviceType	No	This field determines all other fields, as well as how the device is communicated with how it displays in CG-NMS.
Domain Name	domainName	Yes	The domain name configured for this device.
EID	eid	No	The primary element ID of the device, which is used as the primary unique key for device queries.
Firmware Group	firmwareGroup	Yes	The name of the firmware group to which the device belongs.
Firmware Version	runningFirmwareVersion	No	The firmware version running on the device.
Hardware Version	vid	No	The hardware version of the device.
Hypervisor Version	hypervisor	No	(Cisco IOS CGRs running Guest OS only) The version of the Hypervisor.
Hostname	hostname	No	The hostname of the device
IP Address	ip	Yes	The IP address of the device. Use this address for the CG-NMS connection through a tunnel.
Labels	label	Yes	Custom label assigned to the device. A device can have multiple labels. Labels are assigned through the UI or API, but not through a XML or CSV file.
Last Heard	lastHeard	No	The last date and time the device contacted CG-NMS.
Last Metric Heard	N/A	No	The time of last polling (periodic notification).
Last Property Heard	N/A	No	The time of last property update for the FAR.
Last RPL Tree Update	N/A	No	The time of last RPL tree poll update (periodic notification).
Location	N/A	No	The latitude and longitude of the device.
Manufacturer	–	No	The manufacturer of the endpoint device.
Mesh Function	cgmesh	No	Function of the mesh device. Valid values are Range Extender and Meter.
Meter Certificate	meterCert	No	The global or unique certificate reported by the meter.
Meter ID	meterId	No	ME meter ID.
Model Number	pid	No	The product ID of the device.
Name	name	Yes	The unique name assigned to the device.
SD Card Password Lock	–	Yes	(CGRs only) The state of the SD card password lock (on/off).

Table 18   Inventory Fields (continued)

Field	Key	Configurable?	Description
Serial Number	sn	No	The serial number of the device.
Status	status	No	The device status.
Tunnel Group	tunnelGroup	Yes	The name of the tunnel group to which the device belongs.

Mesh Link Config

Table 19 describes the fields in the Mesh Link Config area of the **Routers > Config Properties** page.

Table 19   Mesh Link Config Fields

Field	Key	Configurable?	Description
Mesh Prefix Config	meshPrefixConfig	Yes	The subnet prefix address.
Mesh Prefix Length Config	meshPrefixLengthConfig	Yes	The subnet prefix address length.
Mesh PAN ID Config	meshPanidConfig	Yes	The subnet PAN ID.
Mesh Address Config	meshAddressConfig	Yes	The IP address of the mesh link.
Master WPAN Interface	masterWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is master.
Slave WPAN Interface	slaveWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is slave.

Mesh Device Health

Table 20 describes the fields in the Mesh Device Health area of the Device Info view.

Table 20   Mesh Device Health Fields

Field	Key	Description
Uptime	uptime	The amount of time, in seconds, that the element has been running since last boot.

Mesh Link Keys

Table 21 describes the fields in the Mesh Link Keys area of the Device Info view.

Table 21   Mesh Link Keys Fields

Field	Key	Configurable?	Description
Key Refresh Time	meshKeyRefresh	No	The last date the mesh link keys were uploaded.
Key Expiration Time	meshKeyExpire	Yes	The date the mesh link keys expire.

Mesh Link Settings

Table 22 describes the fields in the Mesh Link Settings area of the Device Info view.

Table 22   Mesh Link Settings Fields

Field	Key	Description
Firmware Version	meshFirmwareVersion	The ME firmware version.
Mesh Interface Active	meshActive	The status of the ME.
Mesh SSID	meshSsid	The ME network ID.

Table 22   Mesh Link Settings Fields (continued)

Field	Key	Description
PANID	meshPanid	The subnet PAN ID.
Transmit Power	meshTxPower	The ME transmission power (dBm).
Security Mode	meshSecMode	The ME security mode.
RPL DIO Min	meshRplDioMin	An unsigned integer used to configure the Imin of the DODAG Information Object (DIO) Trickle timer.
RPL DIO Double	meshRplDioDbl	An unsigned integer used to configure the Imax of the DIO Trickle timer.
RPL DODAG Lifetime	meshRplDodagLifetime	An an unsigned integer used to configure the default lifetime (in minutes) for all downward routes display as Directed Acyclic Graphs (DAGs).
RPL Version Incr. Time	meshRplVersionIncrementTime	An unsigned integer used to specify the duration (in minutes) between incrementing the RPL version.

Mesh Link Metrics

Table 23 describes the fields in the Mesh Link Metrics area of the Device Info page.

Table 23   Mesh Link Metrics Fields

Field	Key	Description
Meter ID	meterId	The ME meter ID.
PANID	meshPanid	The ME PANID.
Mesh Endpoints	meshEndpointCount	Number of MEs.
Mesh Link Transmit Speed	meshTxSpeed	The current speed of data transmission over the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Receive Speed	meshRxSpeed	The rate of data received by the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Transmit Packet Drops	–	The number of data packets dropped in the uplink.
Mesh Route RPL Hops	meshHops	The number of hops that the element is from the root of its RPL routing tree.
Mesh Route RPL Link Cost	linkCost	The RPL cost value for the link between the element and its uplink neighbor.
Mesh Route RPL Path Cost	pathCost	The RPL path cost value between the element and the root of the routing tree.
Mesh Route RSSI	meshRssi	The measured RSSI value of the primary mesh RF uplink (dBm).
Mesh Route Reverse RSSI	meshReverseRssi	The RSSI value measured by the mesh uplink neighbor (dBm) of the element.

NAT44 Metrics

Table 24 describes the fields in the NAT44 area of the Device Info page.

Table 24   NAT44 Metrics Fields

Field	Key	Description
NAT44 Internal Address	nat44InternalAddress0	The internal address of the NAT 44 configured device.
NAT 44 Internal Port	nat44InternalPort0	The internal port number of the NAT 44 configured device.
NAT 44 External Port	nat44ExternalPort0	The external port number of the NAT 44 configured device.

PLC Mesh Info

Table 25 describes the fields in the PLC Mesh Info area of the Device Info view.

Table 25   PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information, used in conjunction with RSSI, combine to determine viable channels.
Mesh Absolute Phase of Power	–	Mesh absolute phase of power is basically relative position of current and voltage waveforms for a PLC node.
LMAC Version	–	Version of LMAC firmware in use by the PLC module DSP processor, which provides lower media access functionality for PLC communications compliant with the IEEE P1901.2 PHY standard.

Raw Sockets Metrics and Sessions

Table 26 describes the fields in the TCP Raw Sockets area of the **Field Devices > Config Properties** page.

Table 26   Raw Sockets Metrics and Sessions View

Field	Key	Description
Metrics		
Tx Speed (bps)	rawSocketTxSpeedS[portNo]	The transmit speed of packetized streams of serial data in bits per second.
Rx Speed (bps)	rawSocketRxSpeedS[portNo]	The receive speed of packetized streams of serial data in bits per second.
Tx Speed (fps)	rawSocketTxFramesS[portNo]	The transmit speed of packetized streams of serial data in frames per second.
Rx Speed (fps)	rawSocketRxFramesS[portNo]	The receive speed of packetized streams of serial data in frames per second.
Sessions		
Interface Name	–	The name of the serial interface configured for raw socket encapsulation.
TTY	–	The asynchronous serial line on the router associated with the serial interface.
VRF Name	–	Virtual Routing and Forwarding instance name.
Socket	–	The number identifying one of 32 connections.
Socket Mode	–	Client or server. The mode in which the asynchronous line interface is set up.
Local IP Address	–	The IP address that either the server listens for connections on (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Local Port	–	The port that either the server listens to for connections (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Dest. IP Address	–	The destination IP address of the remote TCP Raw Socket server.
Dest. Port	–	Destination port number to use for the connection to the remote server.
Up Time	–	The length of time that the connection has been up.
Idle Time	–	The length of time that no packets were sent.
Time Out	–	The currently configured session idle timeout, in minutes.

Router Battery

Table 27 describes the fields in the Router Battery area of the Device Info page.

Table 27   Router Battery Device View

Field	Key	Configurable?	Description
Battery 0 Charge	battery0Charge	No	The percentage of charge remaining in battery 0.
Battery 0 Level (%)	battery0Level	No	The percentage of charge remaining in battery 0.
Battery 0 Remaining Time	battery0Runtime	No	How long battery 0 has been up and running since its installation or its last reset.
Battery 0 State	battery0State	No	The current battery 0 state of the device.

Table 27   Router Battery Device View (continued)

Field	Key	Configurable?	Description
Battery 1 Level (%)	battery1Level	No	The percentage of charge remaining in battery 1.
Battery 1 Remaining Time	battery1Runtime	No	How long battery 1 has been up and running since its installation or its last reset.
Battery 1 State	battery1State	No	The current battery 0 state of the device.
Battery 2 Level (%)	battery2Level	No	The percentage of charge remaining in battery 2.
Battery 2 Remaining Time	battery2Runtime	No	How long battery 2 has been up and running since its installation or its last reset.
Battery 2 State	battery2State	No	The current battery 0 state of the device.
Battery Total Remaining Time	batteryRuntime	No	The total aggregate charge time remaining for all batteries.
Number of BBU	numBBU	No	The number of battery backup units (BBUs) installed in the router. The router can accept up to three BBUs (battery 0, battery 1, battery 2).
Power Source	powerSource	No	The router power source: AC or BBU.

Router Config

Table 28 describes the fields in the Router Config area of the **Field Devices > Config Properties** page.

Table 28   Router Config Device View

Field	Key	Configurable?	Description
Use GPS Location	useGPSLocationConfig	Yes	The internal GPS module provides the router location (longitude and latitude).

Router Credentials

Table 29 describes the fields in the Router Credentials area of the **Field Devices > Config Properties** page.

Table 29   Router Credentials Fields

Field	Key	Configurable?	Description
Administrator Username	–	Yes	The user name used for root authentication.
Administrator Password	–	Yes	The password used for root authentication.
Master key	–	Yes	The master key used for device authentication.
SD Card Password	–	No	SD card password protection status.
Token Encryption Key	–	Yes	The token encryption key.
CGR Username	–	Yes	The username set for the CGR.
CGR Password	–	Yes	The password set on the CGR for the associated username.

Router DHCP Info

Table 30 describes the fields in the DHCP Info area of the Device Info page.

Table 30   Router DHCP Fields

Field	Key	Description
DHCP Unique ID (DUID)	–	A DHCP DUID in hex string format (for example, 0xHHHH).

Router DHCP Proxy Config

Table 31 describes the fields in the DHCP Proxy Config area of the **Field Devices > Config Properties** page.

Table 31   DHCP Proxy Config Fields

Field	Key	Configurable?	Description
DHCPv4 Link for Loopback Interfaces	dhcpV4LoopbackLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for loopback interfaces.
DHCPv4 Link for Tunnel Interfaces	dhcpV4TunnelLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for tunnel interfaces.
DHCPv6 Link for Loopback Interfaces	dhcpV6LoopbackLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for loopback interfaces.
DHCPv6 Link for Tunnel Interfaces	dhcpV6TunnelLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for tunnel interfaces.

Router Health

Table 32 describes the Router Health fields in the Device Info view.

Table 32   Router Health Device View

Field	Key	Configurable?	Description
Uptime	uptime	No	Indicates the length of time (in seconds) that the router has been up and operating since its last reset.
Door Status	doorStatus	No	Options for this field are: ■ "Open" when the door of the router is open ■ "Closed" after the door is closed
Chassis Temperature	chassisTemp	No	Displays the operating temperature of the router. You can configure alerts to indicate when the operating temperature falls outside of the customer-defined temperature range.

Router Tunnel Config

Table 33 describes the fields in the Router Tunnel Config area of the **Field Devices > Config Properties** page.

Table 33   Router Tunnel Config Device View

Field	Key	Configurable?	Description
Tunnel Config	tunnelHerEid	Yes	Displays the EID number of the HER that the FAR connects with through secure tunnels.

Router Tunnel 1 Config

Table 34 describes the fields in the Router Tunnel 1 Config area of the **Field Devices > Config Properties** page.

Table 34   Router Tunnel 1 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 1	tunnelSrcInterface1	Yes	Defines the interface over which the first tunnel is built to provide WAN redundancy.
OSPF Area 1	ospfArea1	Yes	Defines the OSPFv2 Area 1 in which the router (running IPv4) is a member.
OSPFv3 Area 1	ospfV3Area1	Yes	Defines OSPFv3 Area 1 in which the router (running IPv6) is a member.
OSPF Area 2	ospfArea1	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfV3Area1	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 1	ipsecTunnelDestAddr1	Yes	Defines the destination IP address for IPsec tunnel 1.
GRE Dest Addr 1	greTunnelDestAddr1	Yes	Defines the destination IP address for GRE tunnel 1.

Router Tunnel 2 Config

Table 34 describes the fields in the Router Tunnel 2 Config area of the **Field Devices > Config Properties** page.

Table 35   Router Tunnel 2 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 2	tunne2SrcInterface1	Yes	Defines the interface over which the second tunnel is built to provide WAN redundancy.
OSPF Area 2	ospfArea2	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfV3Area2	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 2	ipsecTunnelDestAddr2	Yes	Defines the destination IP address for IPsec tunnel 2.
GRE Dest Addr 2	greTunnelDestAddr2	Yes	Defines the destination IP address for GRE tunnel 2.

SCADA Metrics

Table 36 describes the fields on the SCADA tab of the Device Info page.

Table 36   SCADA Metrics View

Field	Key	Configurable?	Description
Channel Name	channel_name	No	Identifies the channel on which the serial port of the FAR communicates to the RTU.
Protocol Type	protocol	No	Identifies the Protocol Translation type.
Messages Sent	–	No	The number of messages sent by the FAR.
Messages Received	–	No	The number of messages received by the FAR.
Timeouts	–	No	Displays the timeout value for connection establishment.
Aborts	–	No	Displays the number of aborted connection attempts.
Rejections	–	No	Displays the number of connection attempts rejected by CG-NMS.

Table 36   SCADA Metrics View (continued)

Field	Key	Configurable?	Description
Protocol Errors	–	No	Displays the number of protocol errors generated by the FAR.
Link Errors	–	No	Displays the number of link errors generated by the FAR.
Address Errors	–	No	Displays the number of address errors generated by the FAR.
Local IP	–	No	Displays the local IP address of the FAR.
Local Port	–	No	Displays the local port of the FAR.
Remote IP	–	No	Displays the remote IP address of the FAR.
Data Socket	–	No	Displays the Raw Socket server configured for the FAR.

WiFi Interface Config

Table 37 describes the fields in the WiFi Interface Config area of the **Field Devices > Config Properties** page.

Table 37   WiFi Interface Config Fields

Field	Key	Configurable?	Description
SSID	wifiSsid	No	The service set identifier (SSID) assigned to the WiFi interface on the FAR.
Pre-Shared Key	type6PasswordMasterKey	No	The key used to encrypt other pre-shared keys stored on the FAR.

WiMAX Link Metrics

Table 38 describes the fields in the WiMAX Link Health area of the Device Info page.

Table 38   WiMAX Link Health Fields

Field	Key	Description
Transmit Speed	wimaxTxSpeed	The current speed of data transmission over the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
Receive Speed	wimaxRxSpeed	The rate of data that has been received by the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
RSSI	wimaxRssi	The measured RSSI value of the WiMAX RF uplink (dBm).
CINR	wimaxCinr	The measured CINR value of the WiMAX RF uplink (dB).

WiMAX Link Settings

Table 39 describes the fields in the WiMAX Link Settings area of the Device Info page.

Table 39   WiMAX Link Settings Fields

Field	Key	Description
BSID	wimaxBsid	The ID of the base station connected to the WiMAX device.
Hardware Address	wimaxHardwareAddress	The hardware address of the WiMAX device.
Hardware Version	wimaxHardwareVersion	The hardware version of the WiMAX device.
Microcode Version	wimaxMicrocodeVersion	The microcode version of the WiMAX device.

Table 39   WiMAX Link Settings Fields (continued)

Field	Key	Description
Firmware Version	wimaxFirmwareVersion	The firmware version of the WiMAX device.
Device Name	wimaxDeviceName	The name of the WiMAX device.
Link State	wimaxLinkState	The link state of the WiMAX device.
Frequency	wimaxFrequency	The frequency of the WiMAX device.
Bandwidth	wimaxBandwidth	The bandwidth the WiMAX device is using.

Managing Firmware Upgrades

This chapter describes managing firmware upgrade settings in CG-NMS, and includes the following sections:

- FAR Firmware Updates

- FAR Firmware Updates

- Mesh Endpoint Firmware Updates

- Configuring Firmware Group Settings

- Working with FAR Firmware Images

- Working with Mesh Endpoint Firmware Images

Overview

Use CG-NMS to upgrade the firmware running on FARs (CGRs and C800s) and MEs (CGEs and range extenders). CG-NMS stores the firmware binaries in its database for later transfer to FARs in a firmware group through a CGDM file transfer, and to MEs using CG-NMS.

Cisco provides the firmware bundles as a zip file. CG-NMS automatically unzips the kickstart and system images included in the bundle. Firmware system images are large (approximately 130 MB); kickstart images are approximately 30 MB. Every firmware bundle includes a manifest file with metadata about the images in the bundle. You can pause, stop, or resume the upload process.

FAR Firmware Updates

CG-NMS updates FAR firmware in two steps:

1. Uploads the firmware image from CG-NMS to the devices.

   Because of their large size, firmware-image uploads to FARs takes approximately 30 minutes, depending on interface speeds.

2. Installs the firmware on the device and reloads it.

Note: You must initiate the installation process. CG-NMS does not start it automatically after the image upload.

Note that when a FAR contacts CG-NMS for the first time to register and request tunnel provisioning, CG-NMS rolls the FAR back to the default factory configuration (ps-start-config) before uploading and installing the new firmware image.

Note: This rollback requires a second reload to update the boot parameters in ps-start-config and apply the latest configuration. This second reload adds an additional 10–15 minutes to the installation and reloading operation.

Upgrading Guest OS Images

Depending on CGR factory configuration, a Guest OS (GOS) may be present in the VM instance. You can install or upgrade Cisco IOS on the **Config > Firmware Update** page (see FAR Firmware Updates). The GOS, hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

After after any Cisco IOS install or upgrade, when CG-NMS discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and GigabitEthernet 0/1 interface configured to provide an IP address and act as the gateway for the GOS. The new GOS image overwrites existing configurations. CG-NMS has an internal backup and restore mechanism that ports existing apps to the upgraded Guest OS (see Managing a Guest OS).

See the *Cisco 1000 Series Connected Grid Routers Configuration Guides* documentation page for information on configuring the CGR.

Note: If CG-NMS detects a non-Cisco OS installed on the VM, the firmware bundle will not upload and the Cisco reference GOS will not install.

Changing the CGR Timer

You can use the cgnms_preferences.sh script to set or retrieve the FAR timer expiration value in the CG-NMS database:

```
/opt/cgms
/bin/cgnms_preferences setCgrActionExpirationTimeout 50
```

Valid options are:

- set*<pkg>actionExpirationTimeoutMins<value>*

  where,

  - *<pkg>* is the preference package (required for *set* and *get* operations).

  - *actionExpirationTimeoutMins* is the preference key (required for *set* and *get* operations).

  - *<value>* is the prefered value, in minutes (required for *set* and *setCgrActionExpirationTimeout* operations).

- setCgrActionExpirationTimeout *<value>*

- get*<pkg>actionExpirationTimeoutMins*

- *getCgrActionExpirationTimeout*

Example

In the following example, CGR timer value is retrieved, set, the current value retrieved again, the value removed, and a null value retrieved:

```
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:42,004:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
5
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh setCgrActionExpirationTimeout 50
2013-08-12 22:38:51,907:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:58,591:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:12,921:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh set com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins 15
2013-08-12 22:39:23,594:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:29,231:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
15
```

Mesh Endpoint Firmware Updates

When you instruct CG-NMS to upload a firmware image to the members of an ME firmware group, CG-NMS pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

Configuring Firmware Group Settings

This section describes how to add, delete, and configure firmware groups, and includes the following topics:

- Adding Firmware Groups

- Assigning Devices to a Firmware Group

- Renaming a Firmware Group

- Deleting Firmware Groups

Note: Upload operations only begin when you click the Resume button.

When you add FARs or MEs to CG-NMS, the application sorts the devices into the corresponding default firmware group: default-*<router>* or default-cgmesh. Use these groups to upload and install firmware images on member devices. Add firmware groups to manage custom sets of devices. You can assign devices to firmware groups manually or in bulk. Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

Note: When creating firmware groups note the following caveats:

- CGRs and C800s can coexist on a network; however, for firmware management, they cannot belong to the same firmware group.

- IR500s and other mesh endpoint devices can coexist on a network; however, for firmware management, they cannot belong to the same group.

The Groups tab on the **Config > Firmware Update** page displays various device metrics.

CG-NMS displays this information about the image on the FARs in the selected firmware group:

Field	Description
Selected Firmware Image	The name of the current image zip archive or the image being uploaded to group members.
Current Action	The name of the firmware action being performed.
Current Status	The status of the image uploading (Running or Finished).
Written/Devices	Specifies how many devices received or installed the image out of the total number of devices in the group. For example, 1/3 means that one device received the firmware image out of 3 devices in the group.
Error/Devices	Specifies how many devices failed to receive or install the image out of the total number of devices in the group. For example, 2/3 means that two out of the three devices in the group failed to install the image. **Tip:** Click the Error/Devices link (1 in Figure 1) to view the devices that are in the errored state.

For every FAR in the group, CG-NMS displays this information:

Field	Description
Status	Device status of the (for example, Up, Down, or Unheard).
Name	EID of the device.
IP Address	IP address of the device.
Firmware Version	Version of the firmware image installed on the device.
Activity	Device activity.
Update Progress	Firmware image updating progress. A progress of 100% indicates that the image uploading is complete.
Last Firmware Status Heard	The last time the firmware status was heard.
Error Message	Error message if image upload failed.
Error Details	Displays error details for the selected device.

Tip: Click the Error/Devices link (1) to apply a filter (3). Click the Clear (2) button to revert to an unfiltered view of the selected device group.

Figure 1   Firmware Update Page – Errored Devices
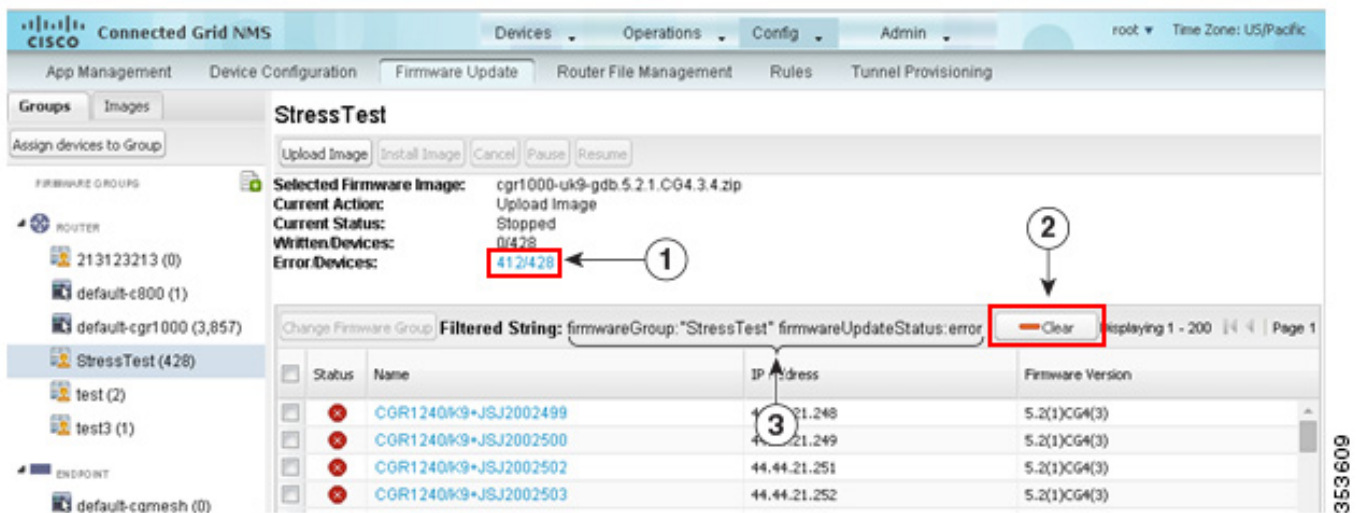
Adding Firmware Groups

To add a firmware group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

Configuring Firmware Group Settings
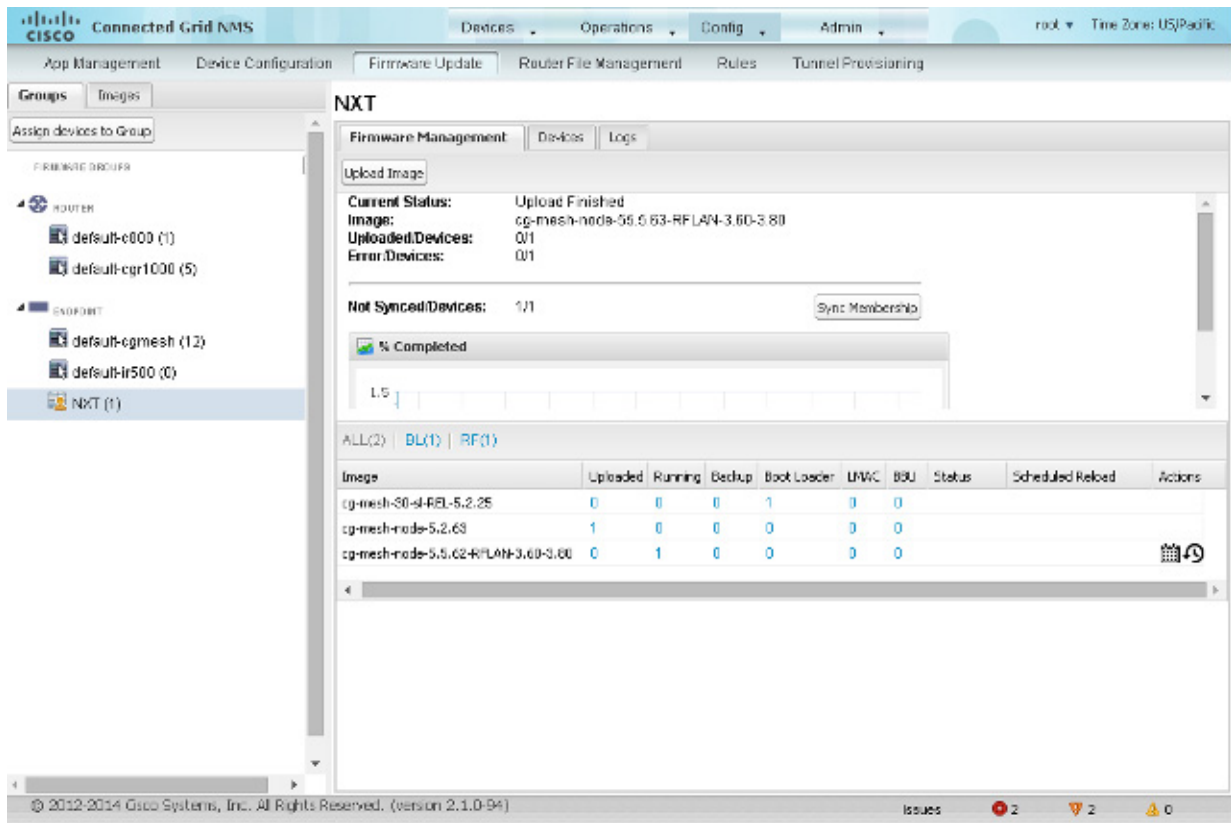
3. In the FIRMWARE GROUPS pane, select **default-cgr1000**, **default-c800**, or **default-cgmesh**, or **default-ir500**.

4. Click **Add Group** (📄) at the top-right of the FIRMWARE GROUPS pane.

5. In the **Add Group** dialog box, enter the name of the firmware group. Device Category is dependent on the device type you select in 3..
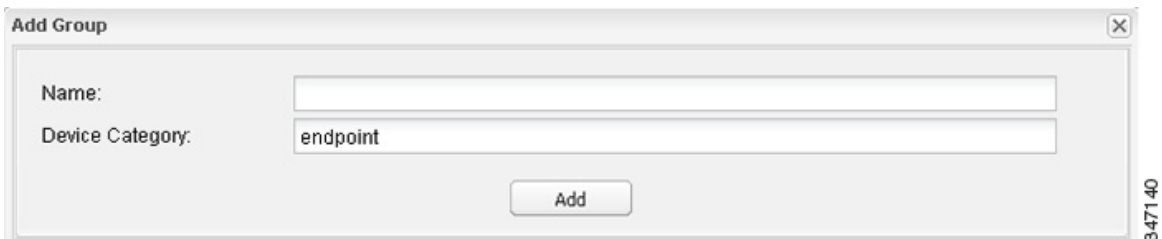
6. Click **Add**.

The new group label appears under the corresponding device type in the FIRMWARE GROUPS pane.

To assign devices to the new group, see Assigning Devices to a Firmware Group.

Assigning Devices to a Firmware Group

This section describes moving devices, and includes the following topics:

■ Moving Devices to Another Group Manually

■ Moving Devices to Another Group In Bulk

223

Configuring Firmware Group Settings

Moving Devices to Another Group Manually

To manually move devices to a group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the desired firmware group based on device type.

> **Note:** If this is an ENDPOINT firmware group, click the **Devices** tab above the main pane.
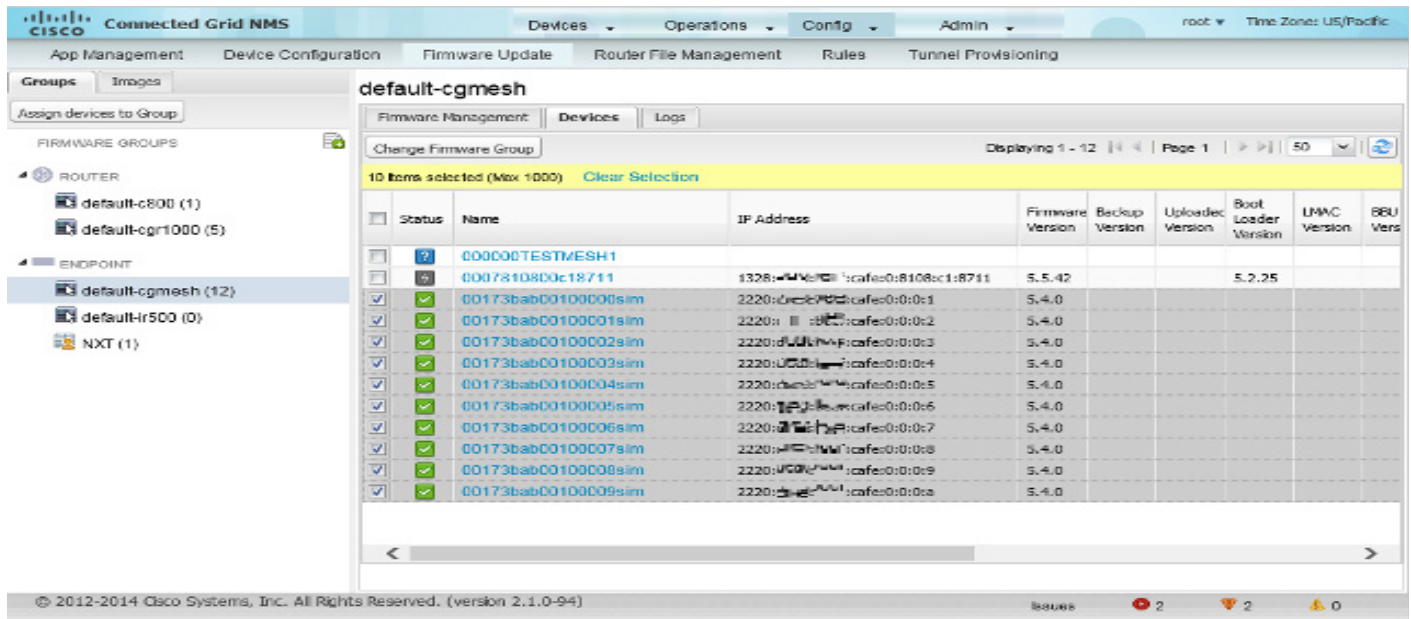
4. Check the check boxes of the devices that you want to move.

5. Click **Change Firmware Group**.
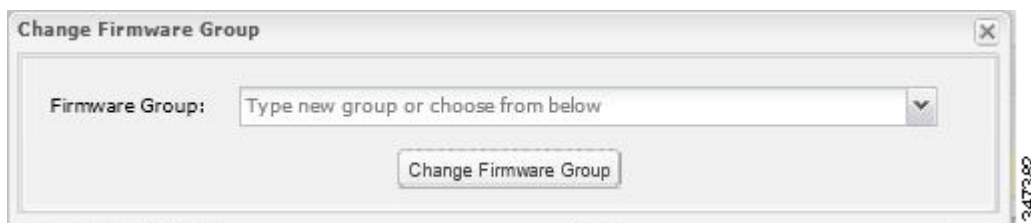
6. From the **Firmware Group** drop-down menu, choose the firmware group to which you want to move the devices or enter a new group name.

7. Click **Change Firmware Group**.

8. Click **Close**.

Moving Devices to Another Group In Bulk

To move devices from one group to another in bulk:

1. Create a CSV or XML file listing devices that you want to move using the format shown in the following examples:

DeviceType/EID for CGRs:	*EID* only for MEs:
``` eid CGR1120/k9+JS1 CGR1120/k9+JS2 CGR1120/k9+JS3 ```	``` eid 00078108003c1e07 00078108003C210b ```

EID only for C800s:	*EID* only for IR500s:
``` eid C819HGW-S-A-K9+FTX174685V0 C819HGW-S-A-K9+FTX174686V0 C819HGW-S-A-K9+FTX174687V0 ```	``` eid da1 da2 da3 ```

Note: Each file can only list one device type.

2. Choose **Config > Firmware Update**.

3. Click the **Groups** tab.

4. Click **Assign Devices to Group**.
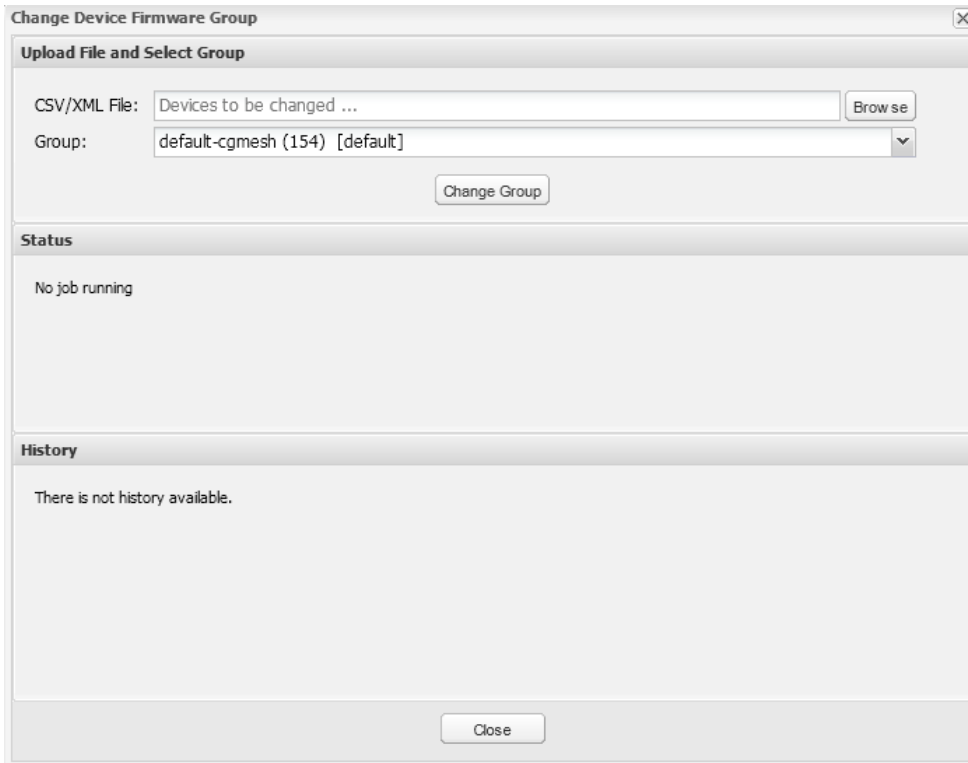
5. Click **Browse** and locate the device list CSV or XML file.

6. From the **Group** drop-down menu, choose the destination group.

7. Click **Change Group**.

   CG-NMS moves the devices listed in the file from their current group to the destination group.

8. Click **Close**.

Renaming a Firmware Group

To rename a firmware group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group to rename.

4. Move the cursor over the group and click the **Edit Group Name** pencil icon.
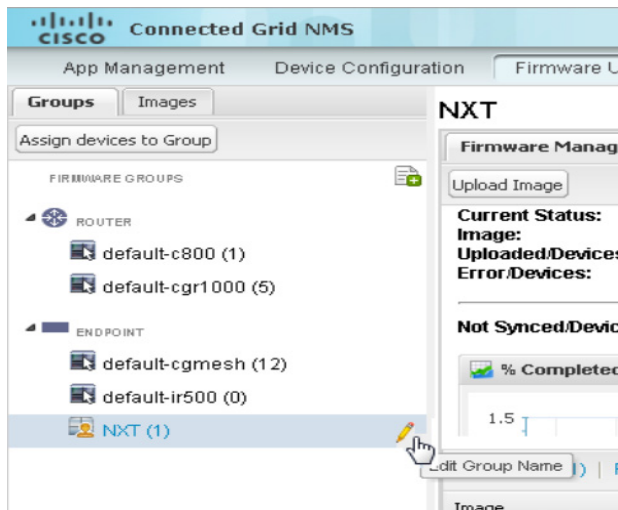
5. In the **Rename Group** window, enter the new name and then click **OK**.
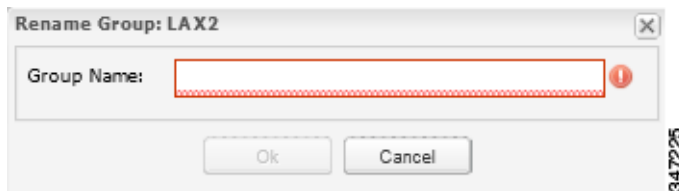
> **Note:** As shown above, when you enter an invalid character entry (such as, @, #, !, or +) within a field, CG-NMS displays a red alert icon, highlights the field in red, and disables the **OK** button.

Deleting Firmware Groups

> **Note:** Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

To delete a firmware group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group to delete.

4. Move the cursor over the group and click **Delete Group** (━).
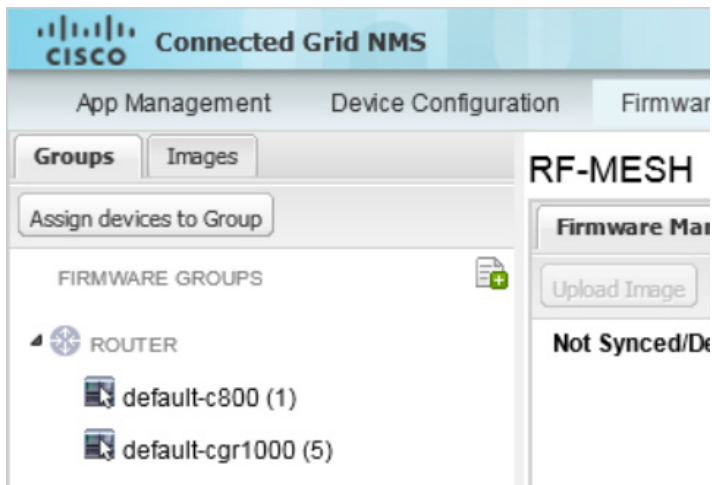
5. To confirm deletion, click **Yes**.

6. Click **OK**.

Working with FAR Firmware Images

This section describes how to add FAR firmware images to CG-NMS and how to upload and install the images on FARs, and includes the following topics:

- Viewing Firmware Image Files in CG-NMS

- Adding a Firmware Image to CG-NMS

- Uploading a Firmware Image to a FAR Group

- Canceling FAR Firmware Image Upload

- Pausing and Resuming FAR Firmware Image Uploads

- Installing a Firmware Image

- Stopping Firmware Image Installation

- Pausing and Resuming FAR Firmware Image Installation

Viewing Firmware Image Files in CG-NMS

You can display firmware image information from the **Images** pane in the **Config > Firmware Update** page. Select ROUTER or ENDPOINT to display all firmware images for those devices in the CG-NMS database. Select the firmware image type to refine the display. For example, Figure 2 shows that selecting ENDPOINT > BBU displays the available BBU firmware image file name and version, and supported Hardware ID.

Figure 2   Config > Firmware Update Images Pane
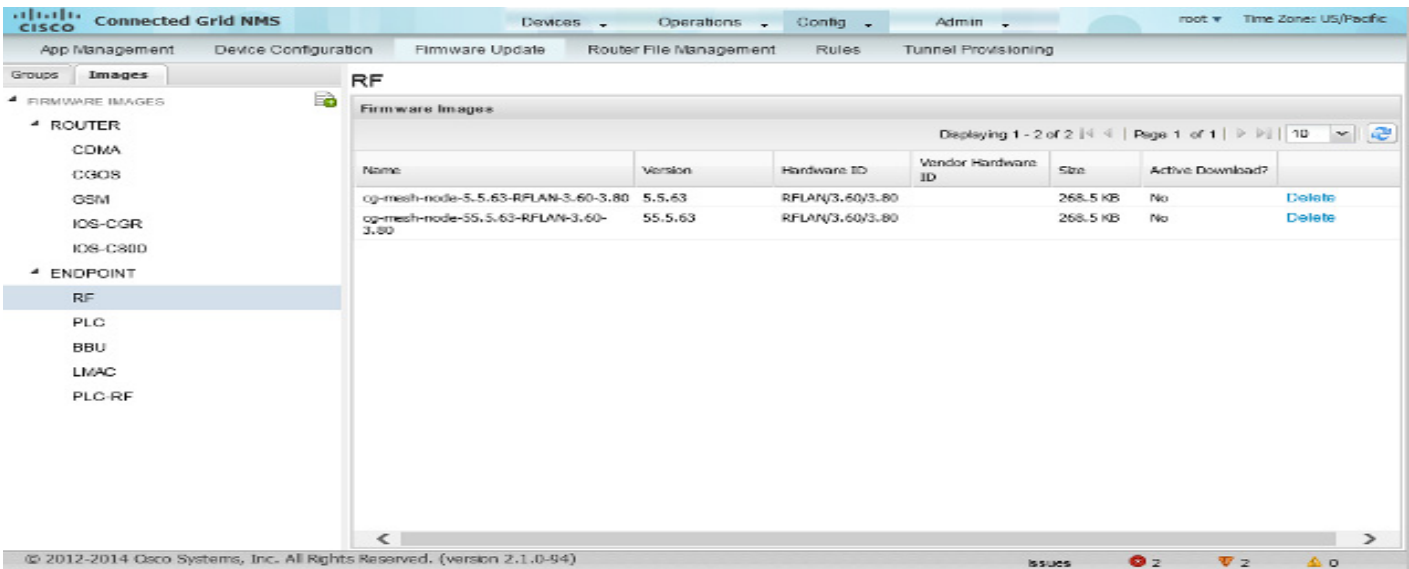
For every image in the list, CG-NMS provides this information:

Field	Description
Name	The filename of the firmware image bundle.
Version	The version of the firmware bundle.
Hardware ID	The hardware family to which you can download this image.
Size	The size of the firmware bundle.
Active Download	The active firmware using the firmware image.

Adding a Firmware Image to CG-NMS

Before you can upload and install a firmware image on a device, add the image file (as a zip archive) to CG-NMS. CG-NMS stores the image in its database.

Note: Do not unzip the image file. CG-NMS unzips the file.

To add a firmware image to CG-NMS:

1. Choose **Config > Firmware Update**.

2. Click the **Images** tab (Figure 2).

3. In the Firmware Images pane, select **ROUTER** or **ENDPOINT**, and the type of device group.

4. Click **Add Image** ( ).

5. Click **Browse** to locate the firmware image. Select the image, then click **Choose**.

6. Click **Upload**.

    The image appears in the Firmware Images pane.

- To delete an image, click its **Delete** link. Click **Yes** to confirm.

  Firmware images with a download in progress (with Yes in the Active Download? column) cannot be deleted.

- To upload the firmware image to devices in a group, select the group and then click **Upload Image.** See Uploading a Firmware Image to a FAR Group.

Uploading a Firmware Image to a FAR Group

When you upload a firmware image to FAR firmware group members, CG-NMS pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

On FARs, firmware image upload and installation requires 200 MB of free disk space. CG-NMS stores image files in the .../managed/images directory on the FAR.

Note: If there is not enough disk space on the FAR for the firmware image, the CG-NMS initiates disk cleanup process on the FAR and removes the following files, sequentially, until there is enough disk space to upload the new image:

- Unused files in the .../managed/images directory that are not currently running or referenced in the before-tunnel-config, before-registration-config, express-setup-config, and factory-config files for IOS CGRs; golden-config, ps-start-config, express-setup-config, or factory-config for CG-OS CGRs

- Unused .gbin and .bin files from the bootflash directory in CG-OS based CGRs

If there is still not enough space, you must manually delete unused files on the FAR.

To upload a firmware image to FAR group members:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group to update.

   Note: CGR groups can be mixed CG-OS and IOS-based devices. The selected firmware image type only uploads to CGRs running that firmware. Therefore, IOS firmware images only upload to selected IOS-based CGRs and to C819s; CG-OS images only upload to CG-OS based CGRs.

   CG-NMS displays the firmware image type applicable the router:

Image	Type	Applicable Router
CDMA	all	Cisco IOS CGR and C800s
GSM	all	Cisco IOS CGR and C800s
IOS_CGR	cgr1000	Cisco IOS CGR

Image	Type	Applicable Router
IOS_C800	all	C800s
CGOS	cgr1000	Cisco IOS CGR running Guest OS

4. Click **Upload Image**.

5. From the **Select Type:** drop-down menu, choose the firmware type for your device.

6. From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

7. Click **Upload Image**.

8. Click **OK**.

CG-NMS starts the upload process. After the image uploads, install the image as described in Installing a Firmware Image.

Canceling FAR Firmware Image Upload

You can stop the image upload process to firmware router groups at any time. Stopping the upload can take a few minutes. When you cancel the image upload, the image upload process immediately stops currently running tasks, and blocks all queued tasks.

Note: Running tasks do not complete, leaving partial files on the disk and sets the firmware group status to CANCELING until you complete the upload operation.

To stop firmware image uploading to a group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group.

4. Click **Cancel**.

5. Click **Yes**.

Pausing and Resuming FAR Firmware Image Uploads

You can pause the image upload process to FAR firmware groups at any time, and resume it later.

Note: The image upload process does not immediately pause; all queued (but not running) operations pause, but currently running tasks complete. The status changes to PAUSING until the active operations complete.

To pause firmware image upload:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group.

4. Click **Pause**.

   The Status column displays PAUSING until the active upload operations complete. No new upload operations start until you click the Resume button.

5. Click **Yes**.

To resume the upload process, click **Resume**.

Note: If a CG-NMS server goes down while the firmware image is being uploaded to devices, the server resumes the upload process for the scheduled devices after the server comes up. For CG-NMS server clusters, if one server goes down during the upload process, another server in the cluster resumes the process.

Installing a Firmware Image

To install an image on devices in a router firmware group:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group.

   Note: CG-NMS recognizes devices as firmware-specific, and uploads the proper image to selected devices. Select a device subgroup in the Images pane to refine the display to those device types.

4. Click **Install Image**.

   CG-NMS sends commands to the FARs in the group to install the uploaded image and reload the FAR to ensure that the new image is operational.

5. Click **Yes**.

   CG-NMS starts the installation or reloading process.

Note: If you restart CG-NMS during the image installation process, CG-NMS restarts the firmware installation operations that were running prior to CG-NMS going offline.

You can pause or stop the installation operation as described in:

■ Stopping Firmware Image Installation

■ Pausing and Resuming FAR Firmware Image Installation.

Note: The firmware installation operation can time out on some routers. If routers are not heard from for more than an hour, CG-NMS logs error messages.

Stopping Firmware Image Installation

You can stop firmware image installation at any time. When you stop image installation, the running version of the firmware remains in place.

Note: Stopping the installation cancels all queued tasks. Currently running tasks complete.

To stop firmware image installation to devices in a firmware group:

1. Choose **Config > Firmware Update**.

2. Click **Groups**.

3. In the FIRMWARE GROUPS pane, select the firmware group.

4. Click **Cancel**.

5. Click **Yes**.

Pausing and Resuming FAR Firmware Image Installation

You can pause the firmware image installation process at any time.

Note: Pausing the installation pauses all queued tasks. Currently running tasks complete.

To pause firmware image installation to devices in a firmware group:

1. Choose **Config > Firmware Update**.

2. In the FIRMWARE GROUPS pane, select the firmware group.

3. Click **Pause**.

4. Click **Yes**.

You can resume the installation process by clicking **Resume**.

Working with Mesh Endpoint Firmware Images

This section describes how to add ME firmware images to CG-NMS, and how to upload and install the images on FARs, and includes the following topics:

■ Uploading a Firmware Image to a Mesh Endpoint Group

■ Viewing Mesh Device Firmware Image Upload Logs

■ Viewing Mesh Device Firmware Information

Note: IR500s and other mesh endpoint devices can coexist on a network; however, for firmware management they cannot belong to the same group.

Note: ENDPOINT devices can report BL/Boot Loader image types to CG-NMS, but CG-NMS cannot upload boot loader images to devices.

Uploading a Firmware Image to a Mesh Endpoint Group

To upload a firmware image to ME group members:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the firmware group to update.

4. Click **Firmware Management**.

5. Click **Upload Image**.

6. From the **Select Type:** drop-down menu, choose the firmware type for your device.

    CG-NMS can upload these image types to ENDPOINT devices.

Image Type	Description
RF	RFLAN connected devices.
PLC	Power line communication devices.
BBU	Devices with battery back up.

Working with Mesh Endpoint Firmware Images

Image Type	Description
IOS_C800	C800 connected devices.
LMAC	Local MAC connected devices.

7. From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

8. Click **Upload Image**.

9. Click **OK**.

CG-NMS adds the image to the list of images in the Firmware Management pane and starts the upload process in the background.
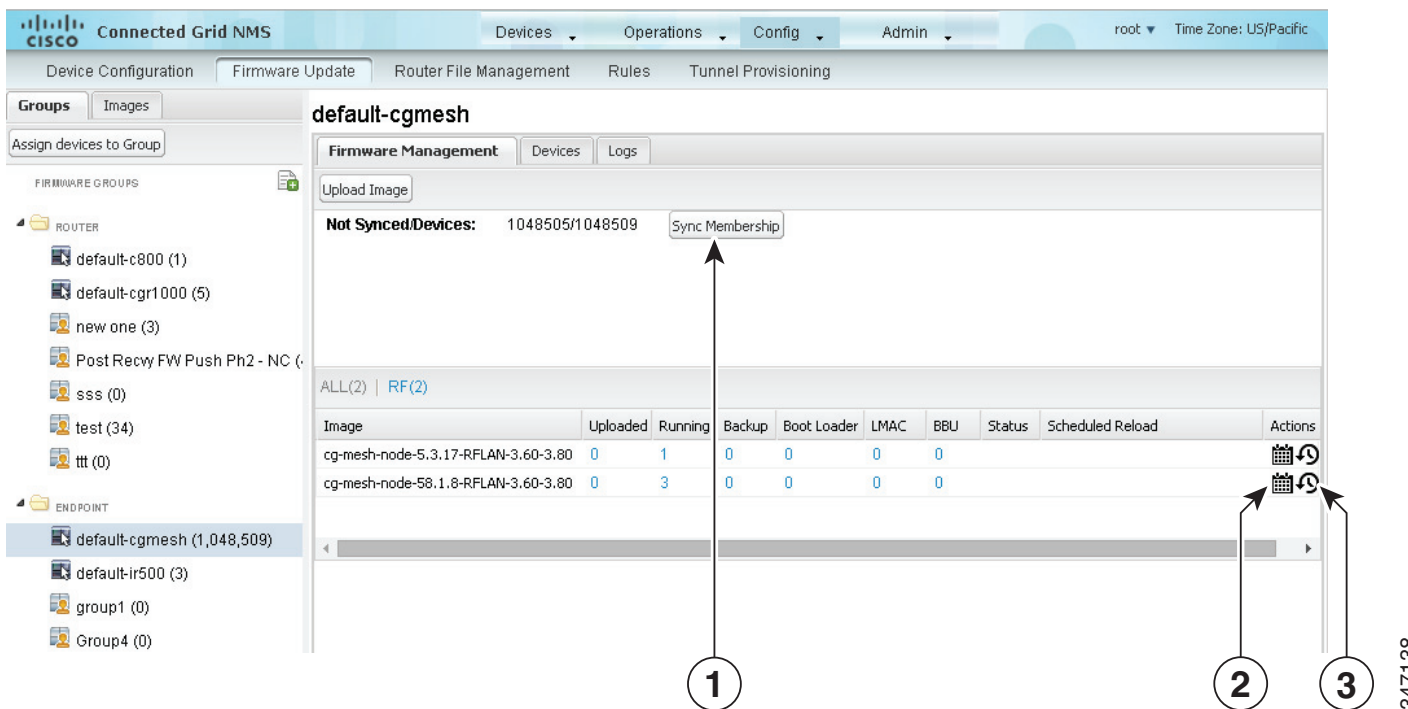
1	Sync membership button
2	Schedule Install and Reload button
3	Set as Backup button

For every image in the list, CG-NMS displays the following information:

Column	Description
Image	Image name.
Uploaded	Specifies the number of devices that uploaded the image. Click the number to display a list of these devices.
Running	Specifies the number of devices running this image. Click the number to display a list of these devices.
Backup	Specifies the number of devices using this image as a backup. Click the number to display a list of these devices.

Column	Description
Boot Loader	Specifies the boot loader image version.
LMAC	Specifies the LMAC image version.
BBU	Specifies the BBU image version.
Status	Specifies the status of the upload process.
Scheduled Reload	Specifies the scheduled reload time.
Actions	Provides two actions:

- Schedule Install and Reload—Schedule the installation of the loaded image and the rebooting of the ME.

- Set as Backup—Set the image as the backup image.

Setting the Installation Schedule

To set the installation schedule:

1. Click the **Schedule Install and Reload** button (2).

2. Specify the date and time for the installation of the image and the rebooting of the device.
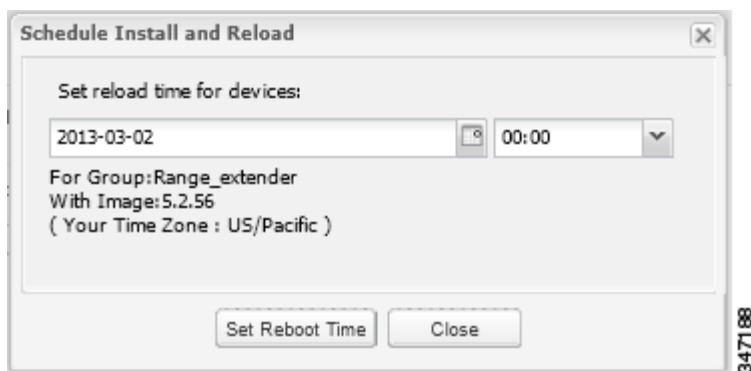
3. Click **Set Reboot Time**.

- To set the selected image as the firmware image backup, click the **Set as Backup** button (3).

4. Click **Yes**.

- To sync the group members in the same firmware group, click **Sync Membership** (1).
- To view member devices, click the **Devices** tab.
- To view log files for the group, click the **Logs** tab.

Viewing Mesh Device Firmware Image Upload Logs

To view the firmware image upload logs for mesh devices:

1. Choose **Config > Firmware Update**.

2. Click the **Groups** tab.

3. In the FIRMWARE GROUPS pane, select the mesh device firmware group.

234

   4. Click the **Logs** tab.

Viewing Mesh Device Firmware Information

   To view the firmware information for mesh devices:

   1. Choose **Config > Firmware Update**.

   2. Click the **Groups** tab.

   3. In the FIRMWARE GROUPS pane, select a MESH DEVICES group.

   4. Click the **Devices** tab.

   For every device in the group, CG-NMS displays this information:

Field	Description
Status	Status of the device (for example, Up, Down, or Unheard).
Name	EID of the device.
IP Address	IP address of the device.
Firmware Version	Version of the firmware image running on the device.
Backup Version	Version of the firmware image used as a backup.
Uploaded Version	Version of the firmware image loaded on the device.
Member Synced?	Whether the device is in sync with the rest of the group.
Activity	Firmware image upload activity.
Update Progress	Firmware image upload progress. An update progress of 100% indicates that the upload is complete.
Last Firmware Status Heard	Last time the firmware status was heard.
Scheduled Reload Time	The time set for upload image reloads.
Error Message	Error message if image upload failed.

Managing Tunnel Provisioning

This chapter describes how to configure CG-NMS for tunnel provisioning, and how to manage and monitor tunnels connecting FARs (CGRs and C800s) and HERs, and includes the following topics.

- Overview

- Configuring Tunnel Provisioning

- Monitoring Tunnel Status

- Reprovisioning CGRs

Overview

CG-NMS sends the commands generated from processing the tunnel provisioning templates to FARs and HERs to provision secure tunnels between them. The default CG-NMS templates contain CLI commands to set up and configure GRE and IPsec tunnels.

Figure 1   Tunnels Connect FARs and their Corresponding HERs
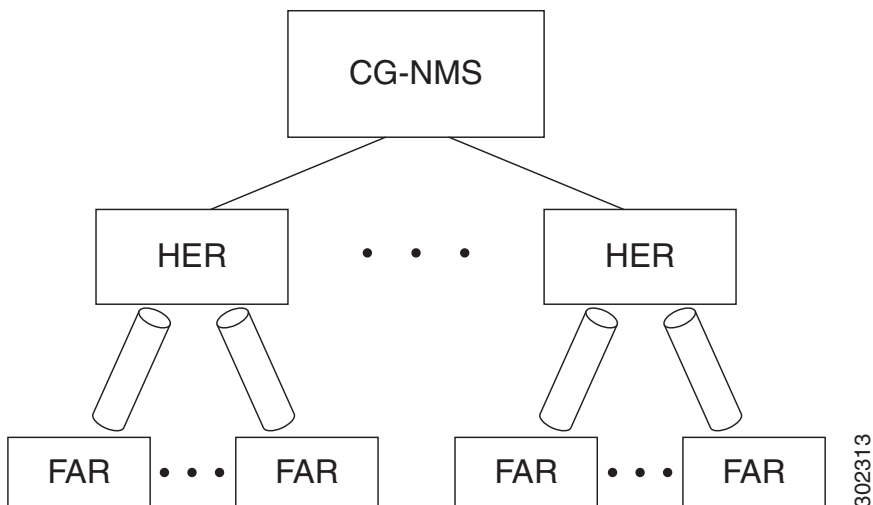
To provision tunnels between HERs and FARs, CG-NMS executes CLI tunnel configuration commands on these devices. By default, CG-NMS provides basic tunnel configuration templates containing the CLI tunnel configuration commands. You can also use your own templates. Although the tunnel provisioning process is automatic, you must first complete the configuration steps outlined in Tunnel Provisioning Configuration Process. After that, whenever a FAR comes online, CG-NMS automatically provisions it with a tunnel. Before you configure CG-NMS for tunnel provisioning, ensure that the CG-NMS TPS Proxy is installed and running.

Tunnel Provisioning Configuration Process

You must generate the keystore files on the CG-NMS and TPS Proxy before configuring tunnel provisioning. Then, you configure CG-NMS and the TPS Proxy to talk to one another (Setting Up the TPS Proxy and Configuring CG-NMS to Use the TPS Proxy).

To configure CG-NMS for tunnel provisioning:

Notes

1. (CG-OS CGRs) Configure the DHCP servers.

   Configuring the DHCP Server for Tunnel Provisioning.

   Configure DHCP servers to provide unique IP addresses to CG-NMS. The default CG-NMS tunnel provisioning templates configure a loopback interface and the IP addresses required to create the tunnels.

   Cisco IOS CGRs use FlexVPN. Ensure that the template only contains addresses for the loopback interface.

2. Configure the tunnel settings.

   Configuring Provisioning Settings.

   Configure the NMS URL and the DHCP proxy client settings on the Provisioning Settings page in CG-NMS (**Admin > System Management > Provisioning Settings**).

3. (CG-OS CGRs) Configure CG-NMS to accept FAR registration requests on first contact (*call home*) to request tunnel provisioning.

   Cisco IOS CGRs use the CGNA service.

4. Configure HER management.

   Configuring HERs Before Adding them to CG-NMS.

   Configure HERs to allow management by CG-NMS using NETCONF over SSH.

5. Add HERs to CG-NMS.

   Adding HERs to CG-NMS.

6. Review the CG-NMS tunnel provisioning templates to ensure that they create the correct type of tunnel.

7. (Optional) If you plan to use your own templates for tunnel provisioning, create one or more tunnel provisioning groups and modify the default tunnel provisioning templates.

   Configuring Tunnel Provisioning Templates.

8. (CG-OS CGRs) Configure FARs to call home.

   This step is typically performed at the factory where the FARs are configured to contact the TPS Proxy.

   Configure FARs to contact CG-NMS over HTTPS through the CG-NMS TPS proxy.

9. Add FARs to CG-NMS.

   Adding FARs to CG-NMS.

   Import the FARs in to CG-NMS using the Notice-of-Shipment XML file.

10. Map FARs to their corresponding HER.

    Mapping FARs to HERs.

After completing the previous steps, deploy the FARs and power them on. Tunnel provisioning happens automatically.

This is the sequence of events after a FAR is turned on:

1. Upon joining the uplink network after being turned on, the FAR sends a request for certificate enrollment.

2. The FAR then requests tunnel provisioning to CG-NMS through the CG-NMS TPS Proxy.

3. CG-NMS looks up the FAR record in the CG-NMS database and determines which tunnel provisioning templates to use. CG-NMS also looks up which HERs to which to establish a tunnel.

4. For Cisco IOS CGRs, the default templates configure the CGR to use FlexVPN. The FlexVPN client is configured on the CGR that will contact the HER and ask for a FlexVPN tunnel to be dynamically constructed. This is how the HER dynamically adds a new tunnel endpoint interface for the CGR.

5. Before processing FAR templates, CG-NMS processes the HER Tunnel Deletion template and sends the resulting commands to the HERs. This is done for each HER to remove existing tunnel configuration that may be associated with the FAR.

6. CG-NMS uses the FreeMarker template engine to process the FAR Tunnel Addition template. The engine converts the templates to text, which CG-NMS assumes to be CLI configuration commands (CG-OS or Cisco IOS, per the CGR). CG-NMS uses these commands to configure and bring up one end of the tunnel on the FAR.

7. CG-NMS uses the FreeMarker template engine to process the HER Tunnel Addition template. The engine converts the templates to text, which CG-NMS assumes to be commands for configuring the tunnel on the HERs.

8. This step is OS-specific:

   ■ For Cisco IOS CGRs, if no errors occurred applying the commands generated by the templates to the FAR and HERs, CG-NMS configures a new active CGNA profile "cg-nms-register," and deactivates the cg-nms-tunnel profile. That cg-nms-register profile uses the CG-NMS URL.

   ■ For CG-OS CGRs, CG-NMS re-configures the call home URL to the CG-NMS URL specified in the Provisioning Settings page (**Admin > System Management > Provisioning Settings**).
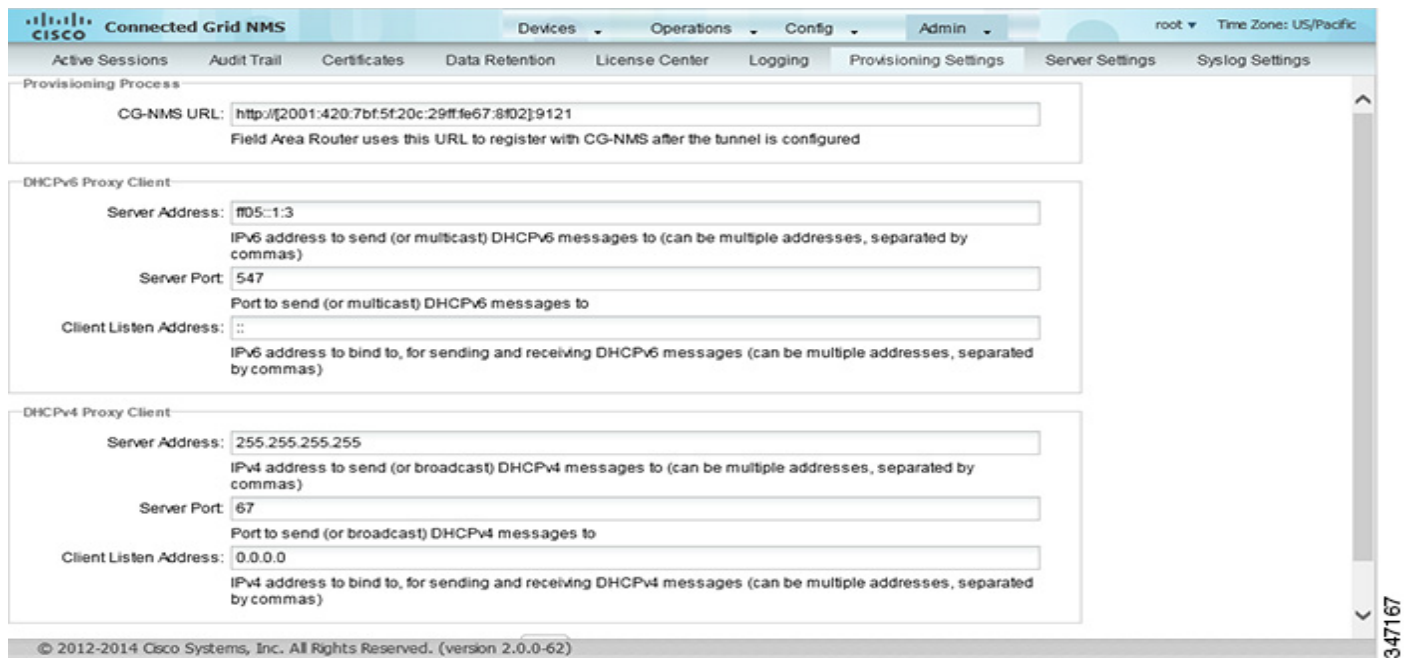
The specified URL uses the CG-NMS registration port (default 9121) instead of the tunnel provisioning port. The Fully Qualified Domain Name (FQDN) in that URL is different and resolves to an IP address that is only reachable through the tunnels.

Configuring Tunnel Provisioning

This section describes how to configure CG-NMS for tunnel provisioning.

■ Configuring the DHCP Server for Tunnel Provisioning

■ Configuring DHCP for Tunnel Provisioning Using CNR

Configuring the DHCP Server for Tunnel Provisioning

For tunnel provisioning to succeed, configure the DHCP server used by CG-NMS to supply addresses to create tunnels between the FARs and HERs. For example, configure the DHCP server to provide IP addresses for tunnel provisioning on a permanent-lease basis.

CG-NMS makes the DHCP requests based on the settings defined in the tunnel provisioning templates. During tunnel provisioning, the CG-NMS templates can make two kinds of DHCP requests:

- Request an IP address, and then make it available to the template.

- Request a subnet with two IP addresses, and then make both addresses available to the template.

CG-NMS can make these requests for IPv4 addresses and IPv6 addresses.

The ability to request DHCP addresses from the template gives you maximum flexibility when defining tunnel configurations because you allocate the exact address needed for each FAR and corresponding interface on the HER. The default tunnel provisioning templates provided address the most common use case: one IPsec tunnel between the FAR and its corresponding HER. Each end of this IPsec tunnel gets a dynamically allocated IPv4 address:

- If your DHCP server supports subnet allocation, use it to obtain two addresses that belong to the same subnet.

- If your DHCP server only supports address allocation, configure it so that the two DHCP address requests return addresses that can be used as ends of an IPsec tunnel.

- If your routing plan calls for allocating unique IPv4 addresses for each FAR and assigning it to a loopback interface above the IPsec tunnel, allocate this address using the CG-NMS template.

If you choose to build IPv6 GRE tunnels, allocate the IPv6 addresses for each end of the tunnel using DHCP prefix delegation or individual address requests.

This section describes example DHCP settings for tunnel provisioning. How you configure these settings depends on your installation. This section provides general guidelines for configuring the DHCP server for tunnel provisioning using the Cisco Network Registrar (CNR).

Configuring DHCP for Tunnel Provisioning Using CNR

The CNR CLI script in the following example configures the CNR DHCP server to service requests made by the default tunnel provisioning templates in CG-NMS. When using this script, ensure that the subnets are appropriate for your DHCP server environment.

Example CNR DHCP Server Tunnel Provisioning Script

```
# These commented out commands support re-applying the configuration by first
# removing any previously applied configuration, in reverse order. This should
# not be done in a production environment, but may be useful when initially
# developing and testing a configuration.

# scope v4address-perm delete
# dhcp-address-block v4subnet-perm delete
# prefix v6subnet-perm delete
# prefix v6address-perm delete
# policy permanent delete

# Configure the server to automatically map any IPv4 or IPv6 user class
# option values to selection tags. By default CG-NMS includes a value of
# "CG-NMS" for the user class in its requests. The tag is used to insure
# prefixes and scopes configured to satisfy requests from CG-NMS are only
# used for that purpose.

dhcp set map-user-class-id=append-to-tags
```

```
# Since CG-NMS uses the leased addresses and subnets in router
# configuration the addresses and subnets must be permanently allocated
# for that purpose. Create a policy that instructs the DHCP server to
# offer a permanent lease.

policy permanent create
policy permanent set permanent-leases=enabled

# Configure DHCPv6.

# The default CG-NMS tunnel template will request IPv6 addresses for
# use with CGR loopback interfaces.

prefix v6address-perm create 2001:DB8:0:0:1::/80 dhcp-type=dhcp
prefix v6address-perm set description="Pool for leasing addresses for loopback interfaces."
prefix v6address-perm set policy=permanent
prefix v6address-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv6 prefixes for
# use with GRE tunnels. Force use of a /127 prefix.

prefix v6subnet-perm create 2001:DB8:0:0:2::/80 dhcp-type=prefix-delegation
prefix v6subnet-perm set description="Pool for leasing prefixes for GRE tunnels."
prefix v6subnet-perm set policy=permanent
prefix v6subnet-perm set selection-tags=CG-NMS
prefix-policy v6subnet-perm set default-prefix-length=127
prefix-policy v6subnet-perm set shortest-prefix-length=127

# Configure DHCPv4.

# The default CG-NMS tunnel template will request IPv4 subnets for
# use with IPsec tunnels. Note that currently address pools for
# IPv4 subnet allocation can only be configured using the CLI as the
# CNR Web UI does not currently support them.

# If CNR allowed you to set a description on DHCP address blocks it would be:
# "Pool for leasing subnets for IPsec tunnels."

dhcp-address-block v4subnet-perm create 192.0.2.0/24
dhcp-address-block v4subnet-perm set default-subnet-size=31
dhcp-address-block v4subnet-perm set policy=permanent
dhcp-address-block v4subnet-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv4 addresses for
# use with loopback interfaces.

scope v4address-perm create 198.51.100.0 255.255.255.0
scope v4address-perm set description="Pool for leasing addresses for loopback interfaces."
scope v4address-perm set policy=permanent
scope v4address-perm addRange 198.51.100.2 198.51.100.254
scope v4address-perm set selection-tag-list=CG-NMS

# Configure detailed logging of incoming and outgoing packets. This is useful when
# debugging issues involving DHCP, however this level of logging will lower the
# performance of the DHCP server. If this is a production server under heavy load
# it may be necessary to forgo detailed packet logging.

dhcp set
log-settings=missing-options,incoming-packet-detail,outgoing-packet-detail,unknown-criteria,client-deta
il,client-criteria-processing,dropped-waiting-packets,v6-lease-detail

# Save the changes and reload the server to have them take effect.
save
```

241

Configuring Tunnel Provisioning

```
dhcp reload

# List the current configuration.

policy list
prefix list
dhcp-address-block list
scope list
dhcp show
```

Configuring Tunnel Group Settings

You use groups in CG-NMS to bulk configure tunnel provisioning for FARs. By default, all FARs added to CG-NMS (see Adding Devices in Bulk) the appropriate default group: **default-cgr1000** or **default-c800**. Default groups contain the three templates CG-NMS uses for tunnel provisioning.

Topics in this section include the following:

- Creating Tunnel Groups

- Deleting Tunnel Groups

- Viewing Tunnel Groups

- Moving FARs to Another Group

- Renaming a Tunnel Group

Creating Tunnel Groups

If you plan to use one set of templates for all FARs, whether using the default templates, modified default templates or custom templates, do not create additional groups. To define multiple sets of templates, create groups and customize the templates for these groups.

Note: CGRs and C800s can be in the same tunnel provisioning group if your custom templates are applicable to both router types.

To create a tunnel group:

1. Choose **Config > Tunnel Provisioning**.

2. Click **Add Group** ( ).
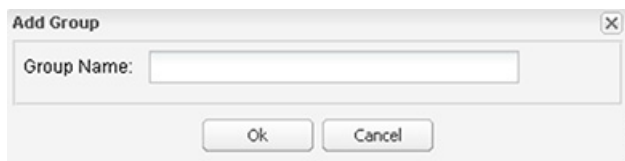
3. Enter a name of the new group, and then click **OK**.

    The group appears in the TUNNEL GROUPS pane.

After creating a tunnel group, the next step is to move FARs from other groups to it, as described in Moving FARs to Another Group.

Configuring Tunnel Provisioning

Deleting Tunnel Groups

Only empty groups can be deleted. Before you can delete a tunnel group, you must move the devices it contains to another group.

To delete an empty tunnel group:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select the tunnel group to delete.

3. Click **Delete Group** (**—**).

4. Click **Yes**.

Viewing Tunnel Groups

The Tunnel Provisioning page lists information about existing tunnel groups.

Follow these steps to view the tunnel groups defined in CG-NMS:

1. Choose **Config > Tunnel Provisioning**.

2. Click **Group Members**.

3. In the TUNNEL GROUPS pane, select a group.

CG-NMS displays a list of all FARs in the group. Use the list navigation buttons to scroll through the list. Table 1 describes the list fields.

Table 1   Tunnel Group Fields

Field	Description
Name	FAR EID (device identifier)
Status	Status of the FAR: ■ Unheard—The FAR has not contacted CG-NMS yet. ■ Unsupported—The FAR is not supported by CG-NMS. **Note:** Only CGR 1000 Series routers are supported. ■ Up—The FAR is in operation. ■ Down—The FAR is turned off.
Last Heard	Last time the router contacted or sent metrics to CG-NMS. If the router never contacted CG-NMS, **never** appears in this field. Otherwise, CG-NMS displays the date and time of the last contact, for example, **4/10 19:06**.
Tunnel Source Interface 1 Tunnel Source Interface 2	FAR interface used by the tunnel
OSPF Area 1 OSPF Area 2	Open shortest path first (OSPF) areas 1 and 2
OSPFv3 Area 1	OSPFv3 area 1
IPsec Dest Addr 1 IPsec Dest Addr 2	IPv4 destination address of the tunnel
GRE Tunnel Dest Addr 1 GRE Tunnel Dest Addr 2	IPv6 destination address of the tunnel

Renaming a Tunnel Group

You can rename a tunnel group at any time. Cisco recommends using short, meaningful names. Names cannot be more than 250 characters long.

To rename a tunnel group:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, roll over the tunnel group to rename and click the **Edit** pencil icon (✏).
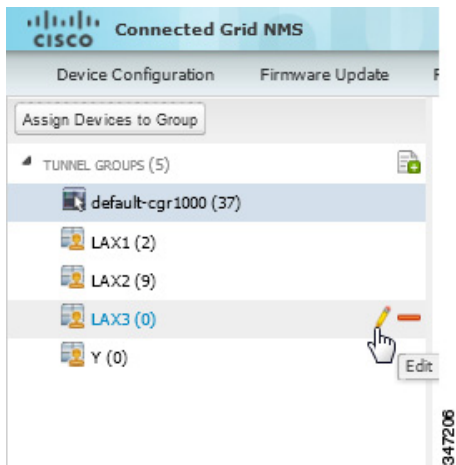
3. Enter the new name, and then click **OK**.
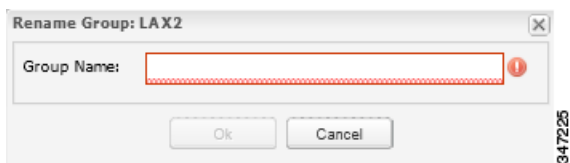
> **Note:** As shown above, when you enter an invalid character entry (such as, @, #, !, or +) within a field, highlights the field in red, and disables the **OK** button.

Moving FARs to Another Group

You can move FARs to another group in two ways:

- Moving FARs to Another Group Manually
- Moving FARs to Another Group in Bulk

Moving FARs to Another Group Manually

To move FARs to another group manually:

1. Choose **Config > Tunnel Provisioning**.

2. Click the **Group Members** tab.

3. In the TUNNEL GROUPS pane, select the tunnel group with the routers to move.

4. Choose the device type from the **Select a device type** drop-down menu.

5. Check the check boxes of the FARs to move.

   To select all FARs in a group, click the check box at the top of the column. When you select devices, a yellow bar displays that maintains a count of selected devices and has the Clear Selection and Select All commands. The maximum number of devices you can select is 1000.

6. Click the **Change Tunnel Group** button.

7. From the drop-down menu, choose the tunnel group to which you want to move the FARs.

8. Click **Change Tunnel Group**.

9. Click **OK** to close the dialog box.

Moving FARs to Another Group in Bulk

You can move FARs in bulk to another group by importing a CSV or XML file containing the names of the FARs to move. Ensure that the file contains entries in the format shown the following example:

```
eid
CGR1120/k9+JSM1
CGR1120/k9+JSM2
CGR1120/k9+JSM3
CGR1120/k9+JSM4
C819HGW-S-A-K9+FTX174685V0
```

The first line is the header, which tells CG-NMS to expect FAR EIDs in the remaining lines (one FAR EID per line).

To move FARs to another group in bulk:

1. Create a CSV or XML file with the EIDs of the devices to move to a different group.

2. Choose **Config > Tunnel Provisioning**.

3. Click **Assign Devices to Group**.
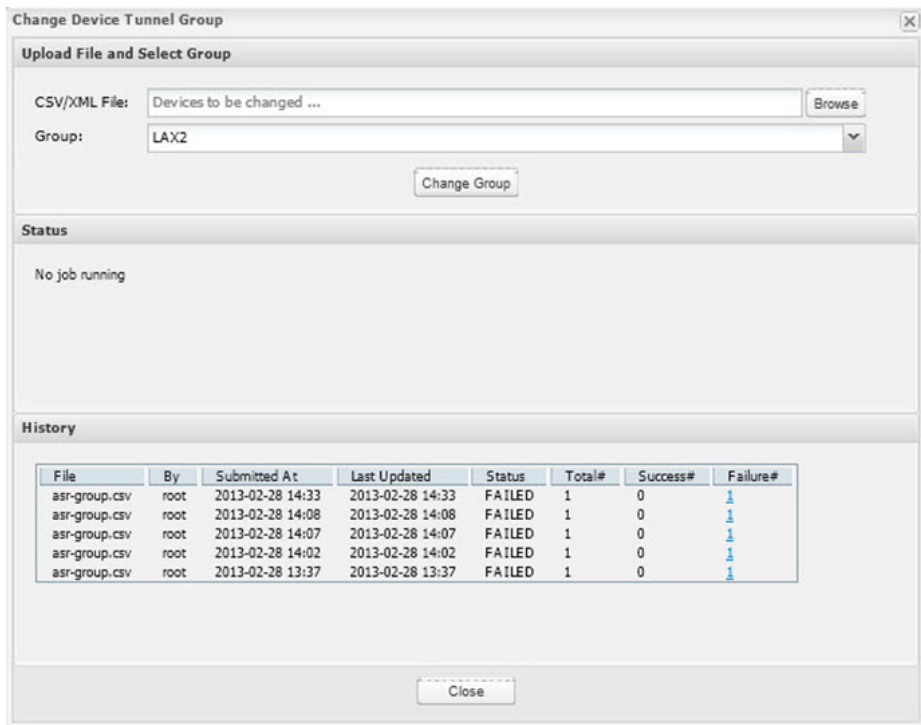
4. Click **Browse** and locate the file that contains the FARs that you want to move.

5. From the **Group** drop-down menu, choose the destination tunnel group.

6. Click **Change Group**.

7. Click **Close**.

Configuring Tunnel Provisioning Templates

CG-NMS has three default tunnel provisioning templates:

■ Field Area Router Tunnel Addition–CG-NMS uses this template to generate the CLI configuration commands for creating one end of an IPsec tunnel on the FAR.

■ Head-End Router Tunnel Addition–CG-NMS uses this template to generate the CLI configuration commands for creating the other end of the IPsec tunnel on the HER.

■ Head-End Router Tunnel Deletion–CG-NMS uses this template to generate the CLI configuration commands for deleting any existing tunnel to the FAR at the other end of the tunnel.

Tunnel Provisioning Template Syntax

The CG-NMS tunnel provisioning templates are expressed with the FreeMarker syntax. FreeMarker is an open-source Java-based engine for processing templates and is built into CG-NMS. As shown in Figure 2, FreeMarker takes as input the tunnel provisioning template and data supplied by CG-NMS, and generates CLI commands that CG-NMS runs on the FARs and HERs in the "configure terminal" context.

Figure 2   CLI Command Generation from Templates in CG-NMS
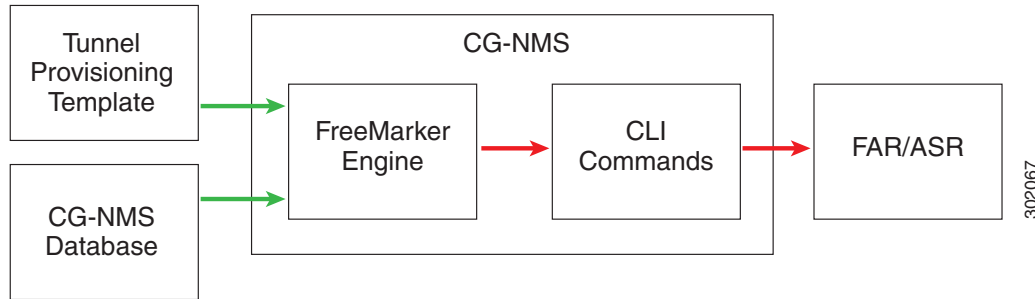
In CG-NMS, the tunnel provisioning templates consist of router CLI commands and FreeMarker variables and directives. The use of FreeMarker syntax allows CG-NMS to define one template to provision multiple routers.

This section describes the basic FreeMarker syntax in the tunnel provisioning templates. For information about FreeMarker visit http://freemarker.sourceforge.net/.

- Template Syntax

- Data Model

Template Syntax

Table 2 describes the syntax in the default tunnel provisioning templates.

Table 2   Tunnel Provisioning Template Syntax

Component	Description
Text	Unmarked text is carried through as CG-OS CLI configuration commands for FARs and Cisco IOS CLI commands for HERs.
Interpolations	${variable} FreeMarker replaces this construct with the value of a string variable that CG-NMS supplies. In this example, CG-NMS provides the EID of the FAR: `description IPsec tunnel to ${`**`far.eid`**`}`
Default Values	${variable!" Default" } FreeMarker replaces this construct with the value of a string variable. If the variable is not set, FreeMarker replaces this construct with **Default**.

Conditionals	<#if condition> output1 <#else> output2 </#if>
	
	FreeMarker uses this construct to determine the text to use in the output. For example:
	
	`<#if far.ipsecTunnelDestAddr1??>`
	`    <#assign destinationAddress=far.ipsecTunnelDestAddr1>`
	`  <#else>`
	`    <#assign destinationAddress=`
	`  her.interfaces("GigabitEthernet0/0/0")[0].v4.addresses[0].address>`
	`</#if>`

Iteration over lists	<#list list as variable> ${variable} </#list> FreeMarker uses this construct to iterate over a list.
Comments	<#-- this is a comment --> FreeMarker allows comments, but does not retain them in the output.

248

Table 2   Tunnel Provisioning Template Syntax (continued)

Component	Description
Assign statements	<#assign name=value> This construct declares a local variable within the template and assigns a value to it. After that, use this construct to reference the variable: ${name} For example: ``` <#assign interfaceNumber=0> ... interface Tunnel${interfaceNumber} ```

Macros	These constructs are similar to function calls.
	
	<#macro name(param1,param2, ... ,paramN)>
	
	... ${param1} ...
	
	</#macro>
	
	Here is an example of a macro definition:
	
	``
	<#macro configureTunnel(interfaceNamePrefix,ospfCost)>
	  <#assign wanInterface=far.interfaces(interfaceNamePrefix)>
	  <#if (wanInterface[0].v4.addresses[0].address)??>
	    <#assign interfaceName=wanInterface[0].name>
	    interface Tunnel${her.unusedInterfaceNumber()}
	      description IPsec tunnel to ${far.eid}
	      ...
	      ip ospf cost ${ospfCost}
	      ...
	</#macro>
	``

Macro calls	To call macros in a tunnel provisioning template: <@name param1, param2 ... paramN> FreeMarker replaces the macro call with the output of the macro after resolving all variables. For example: ``` <@configureTunnel far.tunnelSrcInterface1!"Wimax", 100/> ```

Data Model

This section describes the data model in the tunnel provisioning templates. The **far** and **her** prefixes provide access to the properties of the FARs and HERs, respectively. These properties are stored in the CG-NMS database. Table 3 describes referencing the information provided by the data model in tunnel provisioning templates.

Table 3   Data Model

Property	Description
far.eid	Returns the EID of the FAR. For example: ${far.eid}
far.hostname	Returns the hostname of the FAR.
far.tunnelSrcInterface1	Returns the name of the FAR interface on which to establish the tunnel.

Table 3   Data Model (continued)

Property	Description
far.ipsecTunnelDestAddr1	Returns the name of the tunnel destination IP address on the HER.
far.ipv4Address(*clientId*, *linkAddress*, *userClass*)	Returns an IPv4 address. The IPv4 address method takes these parameters as input: ■ clientId – DCHP Client Identifier for the DHCP request ■ linkAddress – Link address for the DHCP request ■ userClass – Value for the DHCP User Class option (defaults to "CG-NMS") To establish a loopback interface and assign it an address: ``` interface Loopback0 ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32 ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128 exit ```
far.ipv4Subnet()	Returns a DHCP IPv4 subnet lease. This call takes a clientId and linkAddress as arguments. Construct the clientId from the FAR EID and interface ID number using the dhcpClientId() method provided in the template API. This method takes as input a DHCPv6 Identity Association Identifier (IAID) and a DHCP Unique Identifier (DUID) and generates the DHCPv4 client identifier, as specified in RFC 4361. This method provides consistency for how network elements are identified by the DHCP server. For example: ``` <#assign lease=far.ipv4Subnet(dhcpClientId(far.enDuid,iaId), far.dhcpV4TunnelLink)> ```
far.[any device property]	Returns the value of the specified property. For example, far.tunnelSrcInterface1 returns the value of the FAR tunnelSrcInterface1 property.
far.interfaces(interfaceNamePrefix)	Returns a list of interfaces discovered from the device that with that prefix (not case sensitive). Use square brackets to index list members for example, [0], [1], [2], and so on. Use the <#list> construct to iterate list members. For example: ``` <#assign wanInterface = far.interfaces(interfaceNamePrefix)> <#if (wanInterface[0].v4.addresses[0].address)??> ... ```

Addresses

Table 4 describes referencing addresses in the tunnel provisioning templates.

Table 4   Address References

Property	Description
address.address	Returns the address of the interface.
address.prefixLength	Returns the prefix length of the address.
address.prefix	Returns the address prefix.
address.subnetMask	Returns the subnet mask for the address.
address.wildcardMask	Returns the wildcard mask for the subnet.

Configuring the Field Area Router Tunnel Addition Template

To edit the FAR Tunnel Addition template to provide one end of an IPsec tunnel on FARs in the group:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select the tunnel group with the template to edit.

3. Click the **Field Area Router Tunnel Addition** tab.
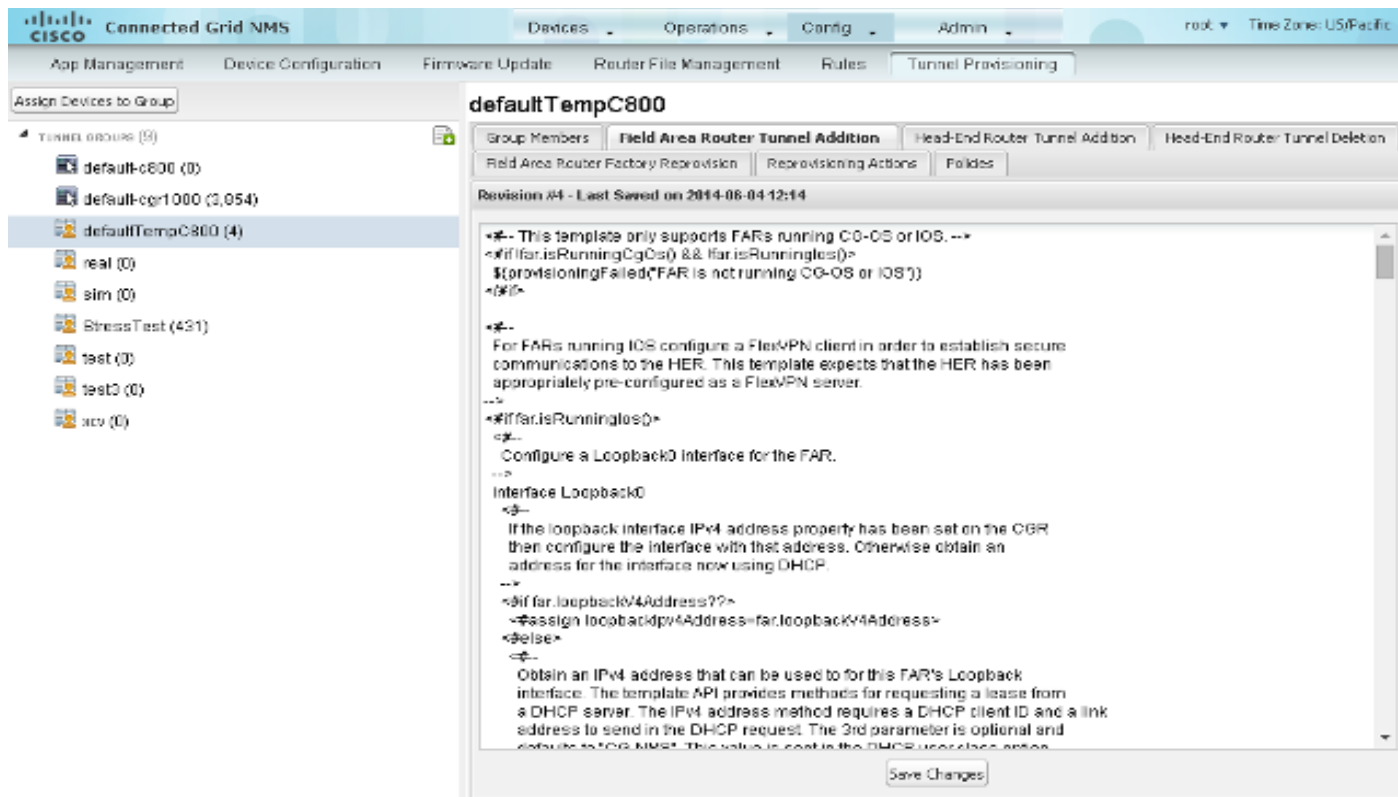
4. Modify the default template.

   Tip: Use a text editor to modify templates and copy the text into the template field in CG-NMS.

5. Click **Save Changes**.

Configuring Tunnel Provisioning

6. Click **OK** to confirm the changes.

See also, Tunnel Provisioning Template Syntax.

Configuring the Head-End Router Tunnel Addition Template

Note: To ensure that both endpoints are in a matching subnet, this template must use the same IAID as the FAR template.

To edit the HER Tunnel Addition template to create the other end of the IPsec tunnel on HERs in the group:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select a tunnel group.

3. Click the **Head-End Router Tunnel Addition** tab.

4. Modify the default HER addition template.

5. Click **Save Changes**.

6. Click **OK** to confirm the changes.

Configuring the HER Tunnel Deletion Template

To edit the HER tunnel deletion template to delete existing tunnels to FARs at the other end of the tunnel:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select the tunnel group whose template to edit.

3. Click the **Head-End Router Tunnel Deletion** tab.
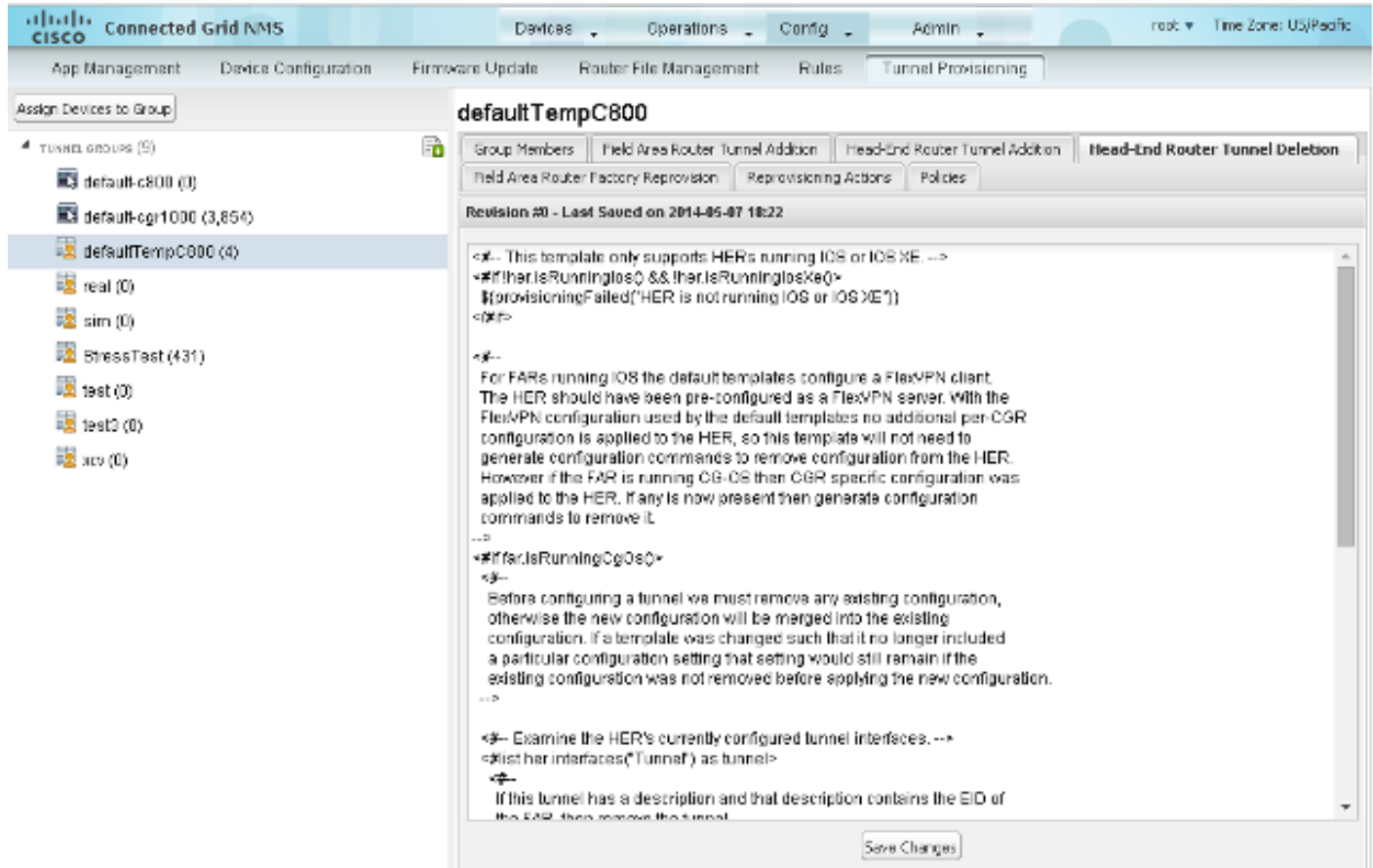
4. Modify the default HER deletion template.

5. Click **Save Changes**.

6. Click **OK** to confirm the changes.

Monitoring Tunnel Status

To view tunnel status, choose **Operations > Tunnel Status**. The Tunnel Status page lists devices and their provisioned tunnels and displays relevant information about tunnels and their status.

Monitoring Tunnel Status

Table 5 describes the tunnel status fields. To change the sort order of tunnels in the list by name, click the HER Name column heading. A small arrow next to the heading indicates the sort order.

Note: It takes time for the status of the newly created tunnel to be reflected in CG-NMS.

Table 5   Tunnel Status Fields

Field	Description
HER Name	The EID of the HER at one end of the tunnel. To view the HER details, click its EID. **Note:** Because one HER can serve up to 500 FARs, there may be multiple tunnels in the list with the same HER EID. The Network Interfaces area of the Device Info page displays a list of tunnels configured on the HER. The Config Properties and Running Config tabs also contain information about tunnels configured on this HER.
HER Interface	The name of the HER tunnel interface. These names are automatically generated when tunnels are created (Tunnel1, Tunnel2, Tunnel3, and so on).
Admin Status	The administrative status of the tunnel (up or down). This indicates if the administrator enabled or disabled the tunnel.
Oper. Status	The operational status of the tunnel (up or down). If the tunnel is down, traffic does not flow through the tunnel, which indicates a problem to troubleshoot. Ping the HER and FAR to determine if they are online, or log on to the routers over SSH to determine the cause of the problem.
Protocol	The protocol used by the tunnel (IPSEC, PIM, or GRE).
HER Tunnel IP Address	The IP address of the tunnel at the HER side. Depending on the protocol used, the IP address appears in dotted decimal (IPv4) or hexadecimal (IPv6) slash notation.
HER IP Address	The destination IP address of the tunnel on the HER side.
FAR IP Address	The destination IP address of the tunnel on the FAR side.

Table 5   Tunnel Status Fields (continued)

Field	Description
FAR Interface	The name of the interface on the FAR used by the tunnel.
FAR Tunnel IP Address	The IP address of the tunnel on the FAR side. **Note:** The IP addresses on both sides of the tunnel are on the same subnet.
FAR Name	The EID of the FAR. To view the FAR details, click its EID. The Network Interfaces area of the Device Info page displays a list of tunnels configured on the FAR. The Config Properties and Running Config tabs also contain information about tunnels configured on this FAR.

Reprovisioning CGRs

In CG-NMS, CGR reprovisioning is a process for modifying the configuration files on CGRs.

- CGR Reprovisioning Basics
- Tunnel Reprovisioning
- Factory Reprovisioning

Note: C800s do not support reprovisioning.

CGR Reprovisioning Basics

- CGR Reprovisioning Actions
- CGR Reprovisioning Sequence

CGR Reprovisioning Actions

In CG-NMS, you can perform the following two CGR reprovisioning actions in the Reprovisioning Actions pane of the Tunnel Provisioning page (**Config > Tunnel Provisioning**).

You can also activate the mesh firmware on this page.

Reprovisioning Actions	Description
Factory Reprovisioning	Change the express-setup-config file loaded on the CGR during factory configuration. This file contains a minimal set of information and is loaded on the CGR at the factory. This file provides the CGR with information to contact CG-NMS (call home) through the TPS Proxy after the CGR is deployed and powered on.
Tunnel Reprovisioning	Change the golden-config file on a CGR. This file has the tunnel configuration defined on the CGR.
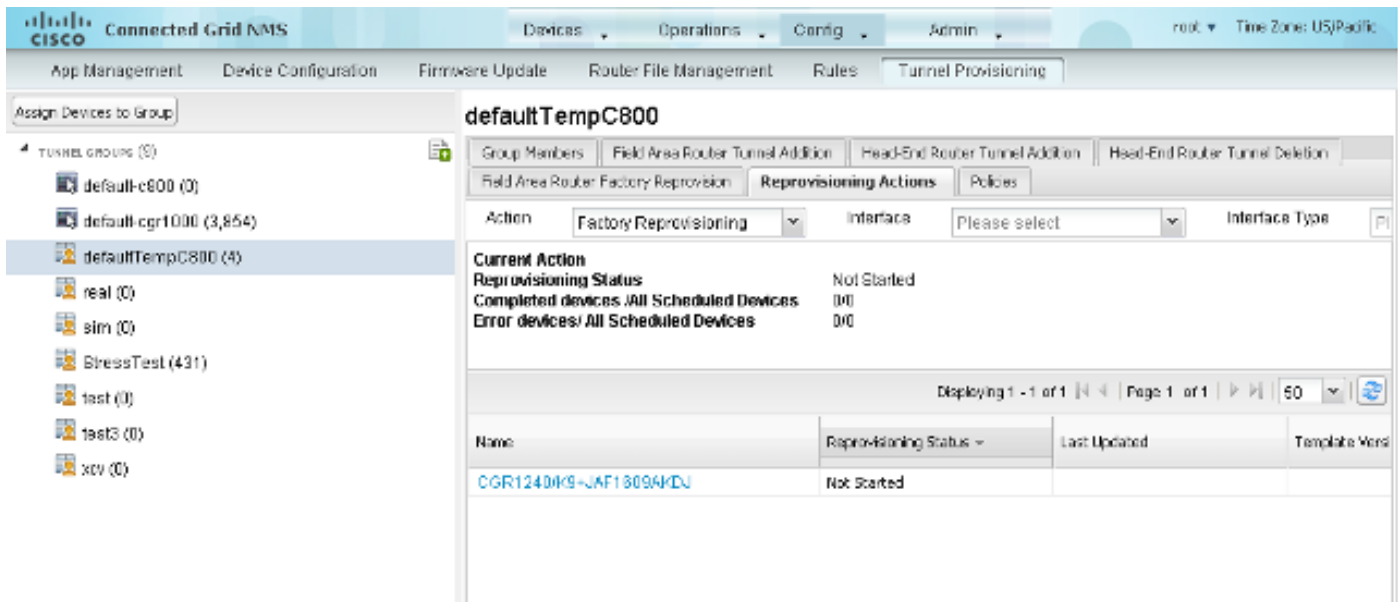
Table 6 describes the fields on the Reprovisioning Actions pane.

Table 6   Reprovisioning Actions Pane Fields

Field	Description
Current Action	The current reprovisioning action being performed.
Reprovisioning Status	The status of the reprovisioning action.
Completed devices /All Scheduled Devices	The number of CGRs that were processed relative to the number of all CGRs scheduled to be processed.
Error devices/ All Scheduled Devices	The number of CGRs that reported an error relative to the number of all CGRs scheduled to be processed.
Name	The EID of the CGR.
Reprovisioning Status	The status of the reprovisioning action for this CGR.
Last Updated	The last time the status of the reprovisioning action for this CGR was updated.
Template Version	The version of the Field Area Router Factory Reprovision template being applied.
Error Message	The error message reported by the CGR, if any.
Error Details	The error details.

CGR Reprovisioning Sequence

When you start tunnel or factory reprovisioning on a tunnel provisioning group, the reprovisioning algorithm sequentially goes through 12 CGRs at a time and reprovisions them.

After CG-NMS reprovisions a router successfully or if an error is reported, CG-NMS starts the reprovisioning process for the next router in the group. CG-NMS repeats the process until all CGRs are reprovisioned.

There is a timeout of 4 hours when reprovisioning each CGR in the group. If the CGR does not report successful reprovisioning or an error within the timeout period, then CG-NMS changes the Reprovisioning Status of the CGR to Error and displays a timeout error and any further information displays in the Error Details field.

Tunnel Reprovisioning

If you make changes to the Field Area Router Tunnel Addition template and want all CGRs already connected to CG-NMS reprovisioned with new tunnels based on the modified template, use the tunnel reprovisioning feature of CG-NMS.

Tunnel reprovisioning places the CGR in a state where no tunnels are configured, and then initiates a new tunnel provisioning request. To reprovision tunnels, CG-NMS sequentially goes through the FARs (12 at a time) in a tunnel provisioning group. For every CGR, CG-NMS rolls back the configuration of the CGR to that defined in the ps-start-config template file.

After a rollback to ps-start-config, the CGR contacts CG-NMS to request tunnel provisioning. CG-NMS processes the Field Area Router Tunnel Addition template and sends the resultant configuration commands for creating new tunnels to the CGR. As shown in Figure 3, the tunnel provisioning process includes updating the golden-config file to include the new configuration information.

Figure 3   Tunnel Reprovisioning Process
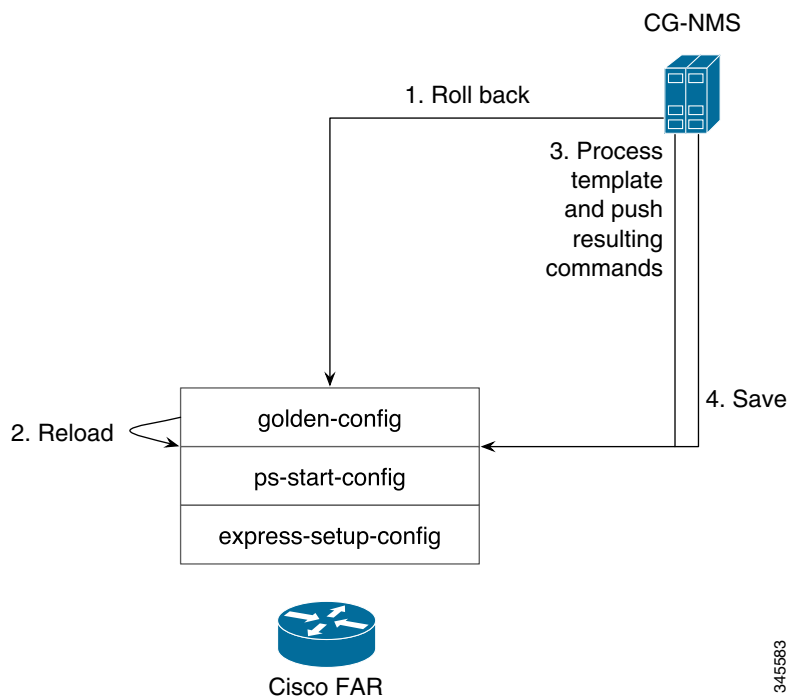
Note: For CG-OS CGRs, a rollback results in a reload of the CGR. Also, when CG-NMS rolls back a CGR, CG-NMS removes the corresponding tunnel information from the HERs to which the CGR was connected.

You perform a configuration replace for Cisco IOS based CGRs.

Note: The Field Area Router Factory Reprovision template is not used when performing tunnel reprovisioning.

To configure and trigger tunnel reprovisioning:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select the tunnel group whose template to provision.

3. Click the **Reprovisioning Actions** tab.

Reprovisioning CGRs
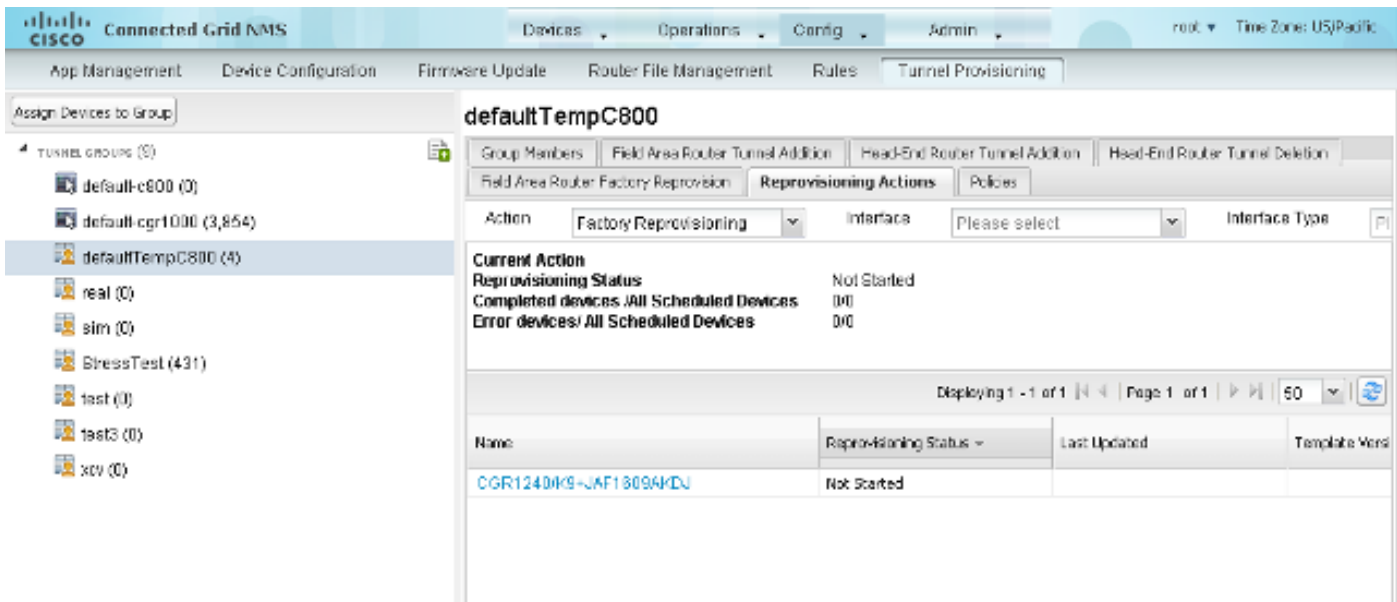
4. From the Action drop-down menu, choose **Tunnel Reprovisioning**.
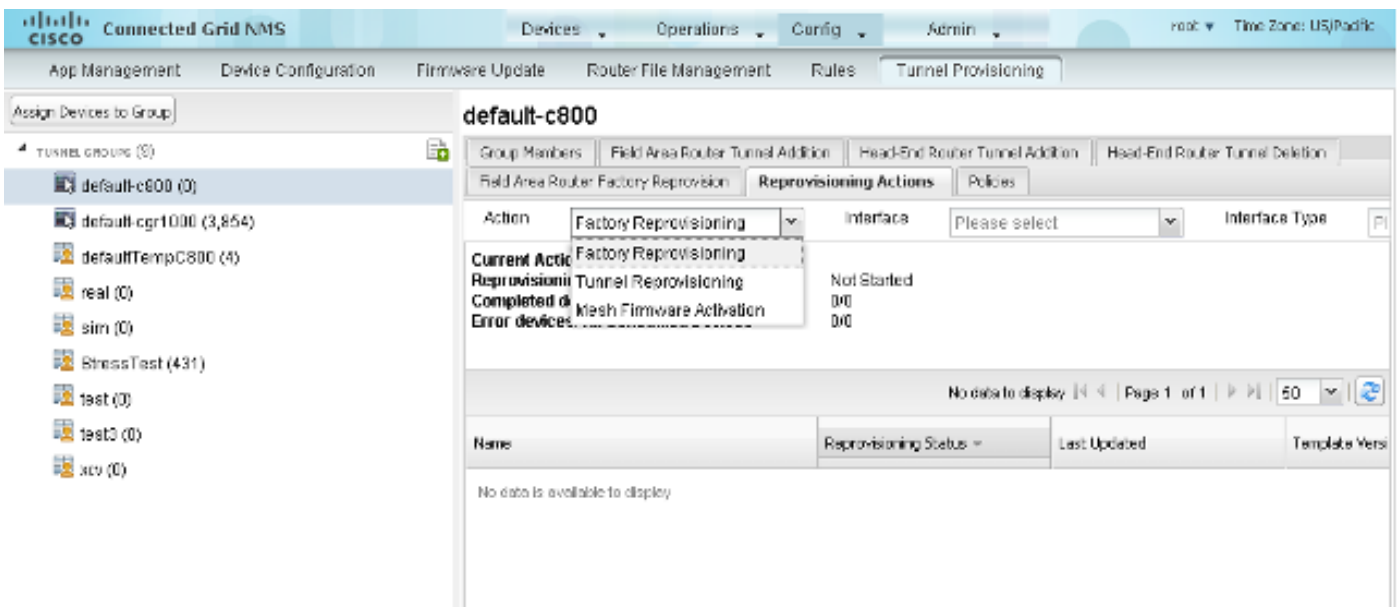
5. Click **Start**.

CG-NMS changes the Reprovisioning Status field to Initialized, and then to Running.

Note: If you click **Stop** while tunnel reprovisioning is running, CG-NMS stops the reprovisioning process only for the FARs in the queue that were not selected. However, for those CGRs in the queue that were selected for reprovisioning, the process completes (success or error) and cannot be stopped.

The reprovisioning process completes after CG-NMS finishes attempting to reprovision each CGR in the tunnel provisioning group. If a CGR cannot be reprovisioned, CG-NMS displays the error message reported by the CGR.

Factory Reprovisioning

Use the Factory Reprovisioning feature in CG-NMS to change the factory configuration of CGRs (express-setup-config).

Factory Reprovisioning involves these steps:

1. Sending the roll back command to the CGR.

2. Reloading the CGR.

3. Processing the Field Area Router Factory Reprovision template, and pushing the resultant commands to the CGR.

4. Saving the configuration in the express-setup-config file.

After these steps complete successfully, CG-NMS processes the Field Area Router Tunnel Addition, Head-End Router Tunnel Addition, and Head-End Router Tunnel Deletion templates and pushes the resultant commands to the CGR (see Tunnel Provisioning Configuration Process).

To configure and trigger factory reprovisioning:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select the tunnel group whose template you want to edit.

3. Click the **Field Area Router Factory Reprovision** tab and enter the template that contains the configuration commands to apply.

   Note: The Field Area Router Factory Reprovision template is processed twice during factory reprovisioning; once when pushing the configuration and again before saving the configuration in express-setup-config. Because of this, when making your own template, use the specific if/else condition model defined in the default template.
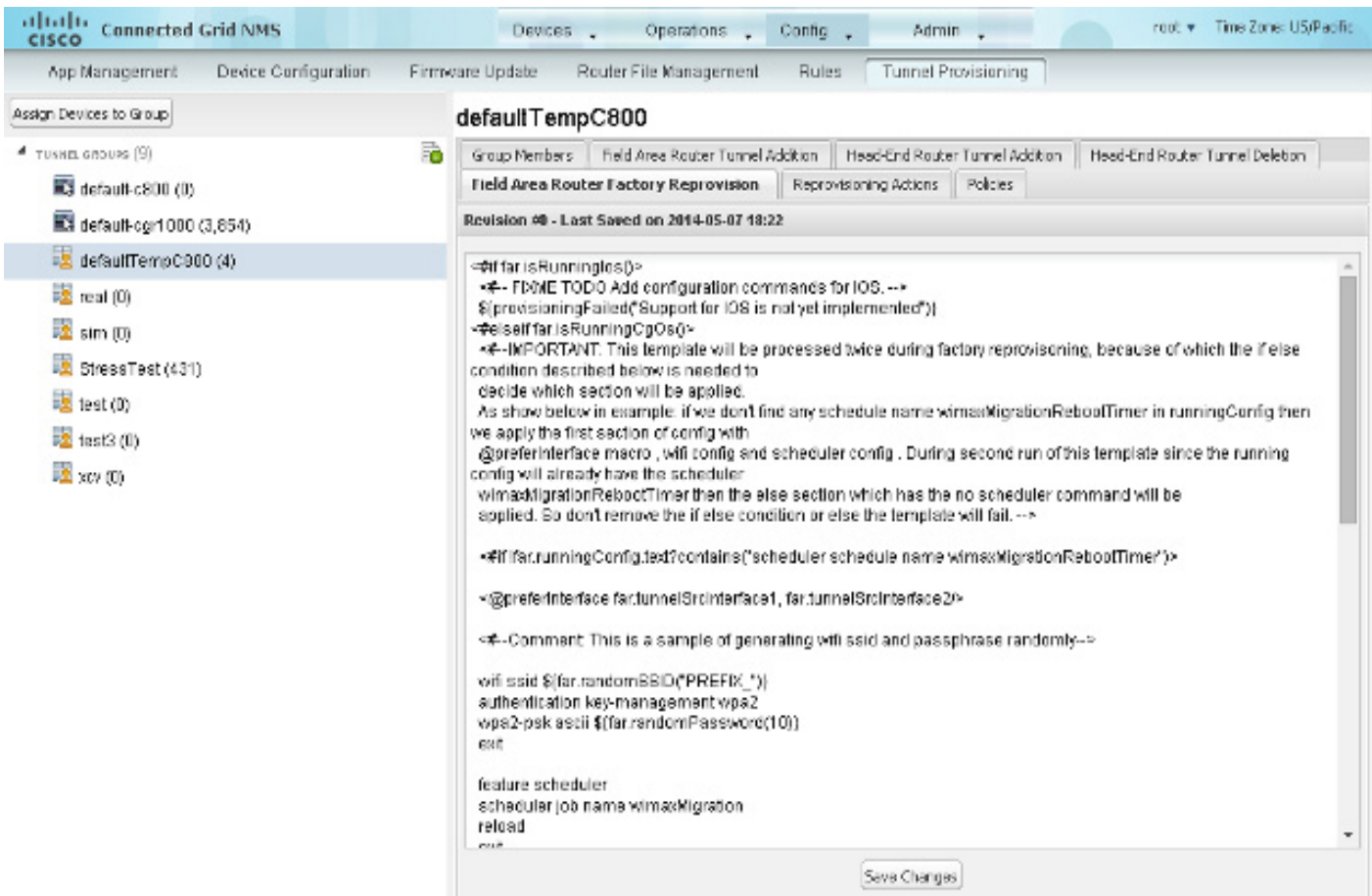
4. Click **Save Changes**.

5. If needed, make the necessary modifications to the Field Area Router Tunnel Addition, Head-End Router Tunnel Addition, and Head-End Router Tunnel Deletion templates.

6. Click the **Reprovisioning Actions** tab.

7. From the Action drop-down menu, choose **Factory Reprovisioning**.
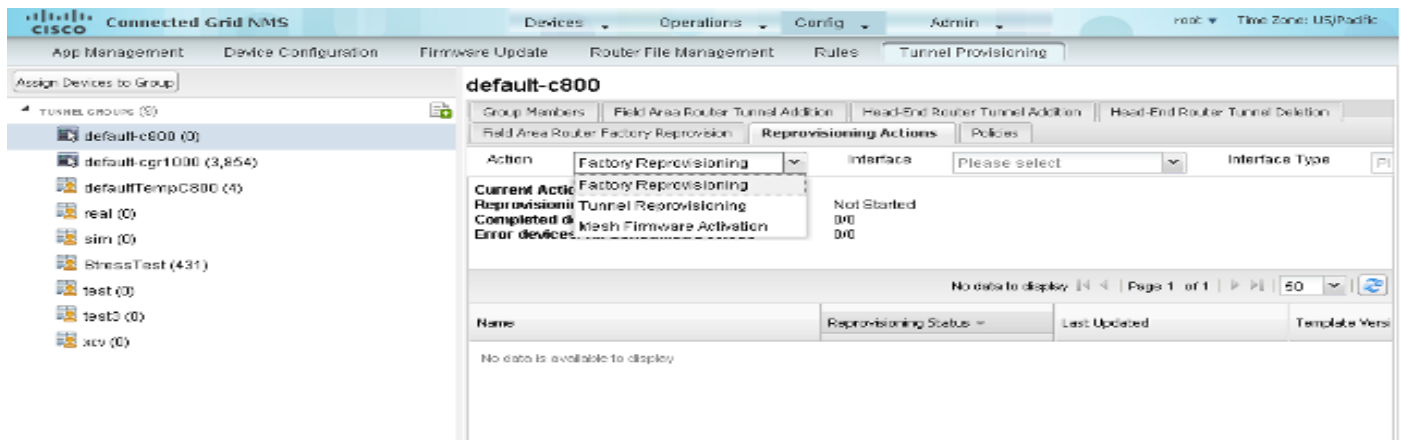
8. From the Interface drop-down menu, choose the CGR interface for CG-NMS to use to contact the FARs for reprovisioning.

Reprovisioning CGRs
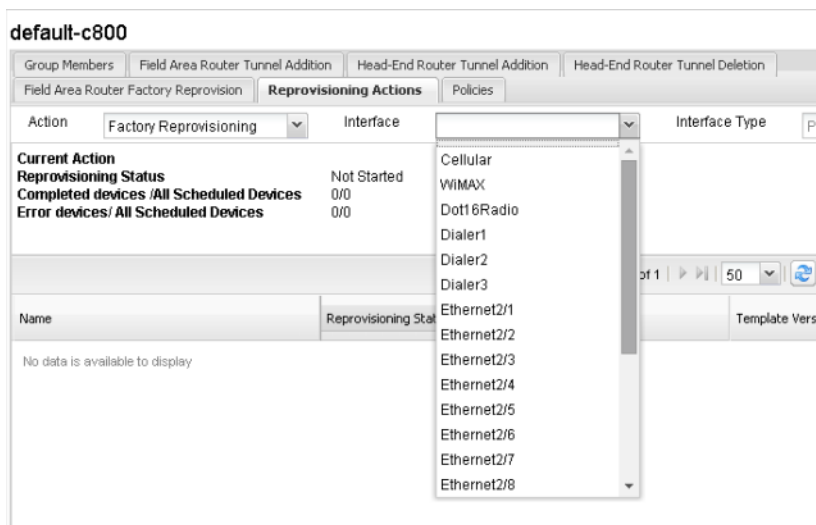
9. From the Interface Type drop-down menu, choose **IPv4** or **IPv6**.
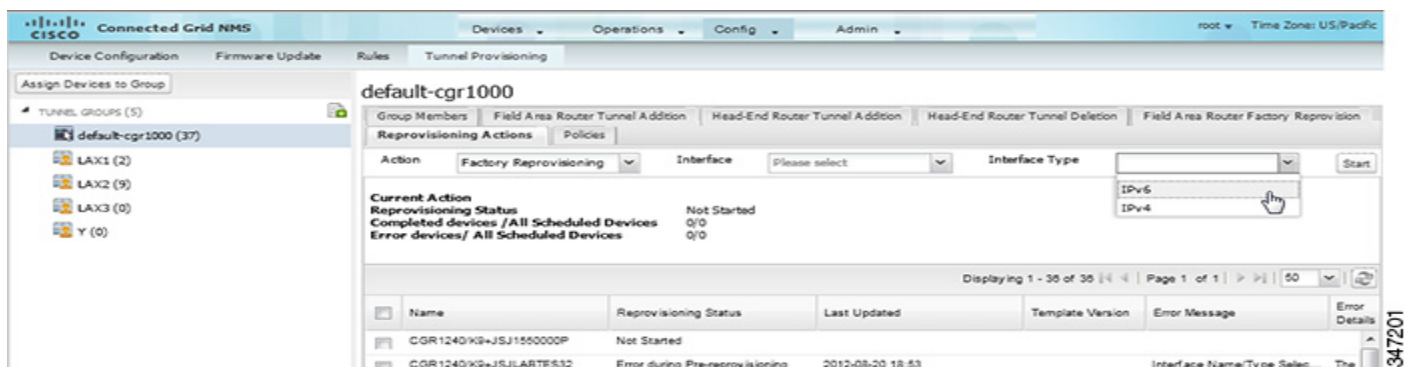
10. Click the **Start** button.

CG-NMS changes the Reprovisioning Status field to Initialized, and then to Running.

Note: If you click **Stop** while factory reprovisioning is running, CG-NMS stops the reprovisioning process only for the FARs in the queue that were not selected. However, for those CGRs in the queue that were selected for reprovisioning, the process completes and cannot be stopped.

The reprovisioning process completes after CG-NMS has finished attempting to reprovision each CGR in the tunnel provisioning group. If a CGR cannot be reprovisioned, CG-NMS displays the error message reported by the CGR.

Sample Field Area Router Factory Reprovision Template

This sample template changes the WiFi SSID and passphrase in the factory configuration.

```
<#--IMPORTANT: This template is processed twice during factory reprovisioning. The if/else condition
described below is needed to determine which part of the template is applied.
In this example, if no schedule name wimaxMigrationRebootTimer is found in runningConfig, then the if
part of the if/else section is applied. During the second pass, this template runs the commands in the
else section and the no scheduler command is applied. If modifying this template, do not remove the
if/else condition or else the template fails. -->

<#if !far.runningConfig.text?contains("scheduler schedule name wimaxMigrationRebootTimer")>

<#--Comment: This is a sample of generating wifi ssid and passphrase randomly-->

wifi ssid ${far.randomSSID("PREFIX_")}
authentication key-management wpa2
wpa2-psk ascii ${far.randomPassword(10)}
exit

feature scheduler
scheduler job name wimaxMigration
reload
exit

scheduler schedule name wimaxMigrationRebootTimer
time start +02:00
job name wimaxMigration
exit

<#else>

no scheduler job name wimaxMigration
no scheduler schedule name wimaxMigrationRebootTimer

</#if>
```

Monitoring System Activity

This chapter describes how to monitor CG-NMS system activity, including the following topics:

- Using the Dashboard

- Monitoring Events

- Monitoring Issues

- Viewing Device Charts

Using the Dashboard

The CG-NMS Dashboard (Figure 1) displays *dashlets* to provide a visual overview of important network metrics.

Figure 1   CG-NMS Dashboard
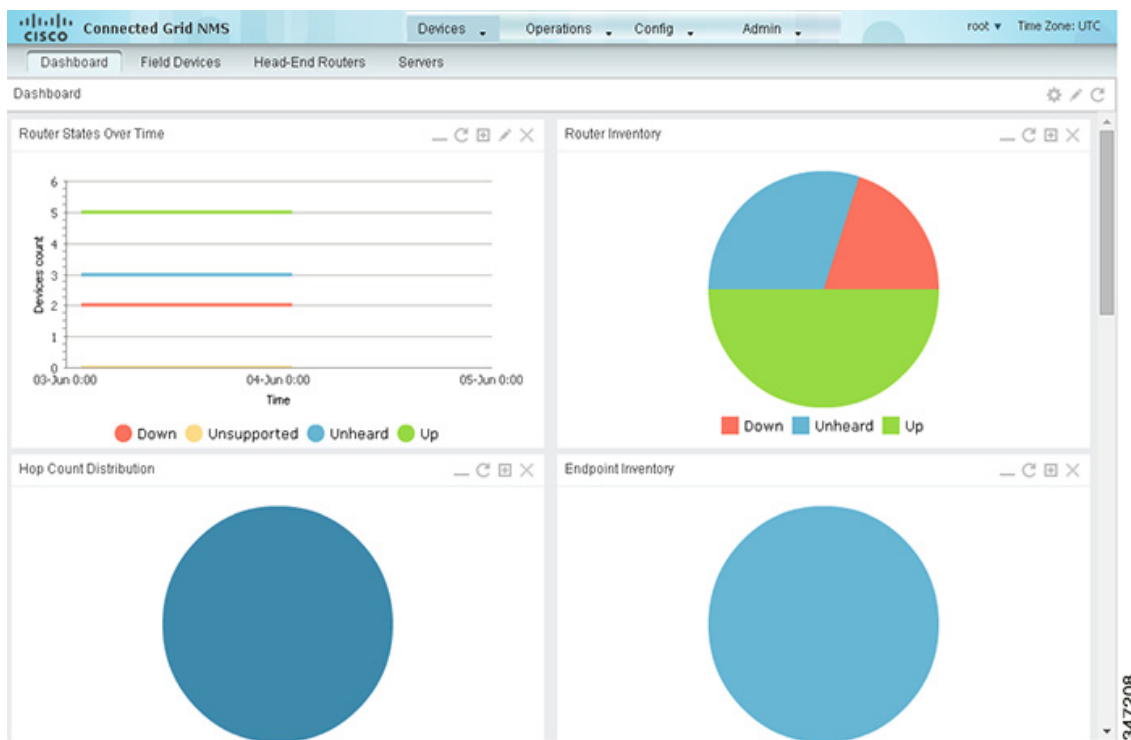
This section describes the following Dashboard features:

- Types of Dashlets

- Repositioning Dashlets

- Setting the Dashlet Refresh Interval

- Adding Dashlets

- Removing Dashlets

- Exporting Dashlet Data

263

Types of Dashlets

The Dashboard displays two types of dashlets:

- Pie-chart dashlets display a ratio of device properties as a pie chart.
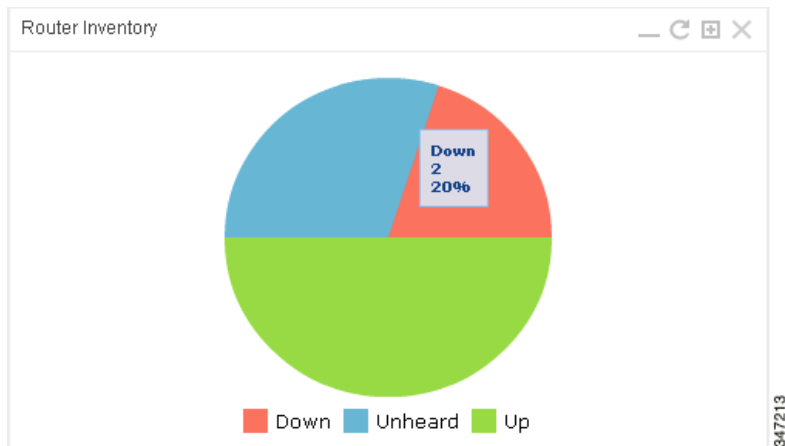
- Line-graph dashlets display graphs that show device counts over time.
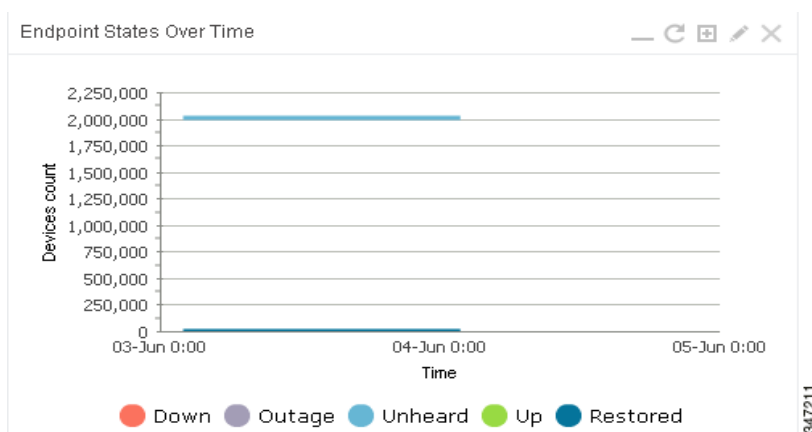
Tip: Graphs set to intervals longer than one day may not display the data at the last datapoint exactly as shown in the matching field on the Device Info page. This is because data aggregation is occurring less frequently than polling to update the fields on the Device Info page. Set these graphs to the 6h or 1d intervals to update the data more frequently. Use intervals longer than one day to view data trends.

Dashboard Dashlets

The CG-NMS Dashboard dashlets are described below.

Dashlet	Description
Router Inventory	This FAR status counts pie chart displays the status distribution and absolute count of FARs.
Router States Over Time	This line graph shows a count of the FARs and their states for the configured time interval.

Dashlet	Description
Mesh Endpoint Inventory	This ME status counts pie chart displays the proportion (and count) of MEs. For example, the count of devices with an Unheard status relative to the other states: Up, Down, and Outage.
Mesh Endpoint States Over Time	This line graph shows a count of MEs and their states for the configured time interval.
Mesh Endpoint Config Group Template Mismatch Over Time	This line graph shows the number of MEs across all configuration groups and particular configuration groups that are out of sync for the configured time interval.
Mesh Endpoint Firmware Group Membership Mismatch Over Time	This line graph shows the number of MEs across all firmware groups and particular firmware groups that are out of sync for the configured time interval.
Config Group Template Mismatch	This pie chart shows the number of devices with matched and mismatched configuration group templates (applicable only to ME configuration groups).
Firmware Group Membership Mismatch	This pie chart shows the number of devices with mismatched firmware groups (applicable only to ME firmware groups).
Hop Count Distribution	This pie chart shows the hop count distribution for mesh devices.
Service Providers Data	This dashlet shows the service provider names, their associated cell IDs (if available), their associated total router count, and the count of down routers. This dashlet also displays the bandwidth usage and a sparkline showing the down routers over time. **Tip:** Click the triangle in any column heading, select Columns in the context menu, and check the Down Routers Over Time check box to hide this column.
Routers With Top Cellular Bandwidth Usage	This bandwidth chart displays the top *n* routers using the maximum cellular bandwidth, where *n* is the number of top routers to display. Click the Filter button and select the number of routers to display from the **Show** drop-down list.

Dashlet	Description

- Click the **Last Billing Period** button to display the bandwidth usage information for the top *n* routers that used the maximum bandwidth during last billing period.

- Click the **Current Billing Period** button to display the bandwidth usage information for the current billing period.

  The start days are defined on the Billing Period Settings tab (**Admin > System Management > Server Settings**).

| Routers With Top Ethernet Bandwidth Usage | This dashlet is similar to the Routers With Top Cellular Bandwidth Usage dashlet, except that it displays the top *n* routers with the maximum Ethernet bandwidth usage. |
| Routers With Least Cellular RSSI | This dashlet displays a chart of routers with the lowest RSSI values at the last poll, which indicates the quality of the signal strength. Use this chart to gauge the cellular channel conditions for FARs. |

Repositioning Dashlets

The Dashboard is configurable to display charts in your preferred arrangement. To configure the Dashboard:

- Click and drag the title bar of a chart to the desired position.

- Click the close box to remove the chart from the page.

- Click the interval button to do the following:

  - Define an interval for line-graph chart displays.

  - Define a custom interval for line-graph chart displays.

  - Select the number of devices to chart for line-graph chart displays.

  - Select a series to refine data in line-graph chart displays.

  - Filter line-graph chart displays by group.

- Click the Settings button in the title bar to set the refresh interval for all charts and add dashlets back to the Dashboard.

To better view dashlets in the bottom of the Dashboard, collapse a dashlet to just its title bar by clicking the dashlet show/hide button (▲). In Figure 2 the Config Group Template Mismatch dashlet is expanded in the Dashboard with several other dashlets collapsed above it. To refresh the Dashboard, click the **Refresh** button (⚙). To refresh a dashlet, click its **Refresh** button.

Figure 2   Dashboard with Collapsed Dashlets
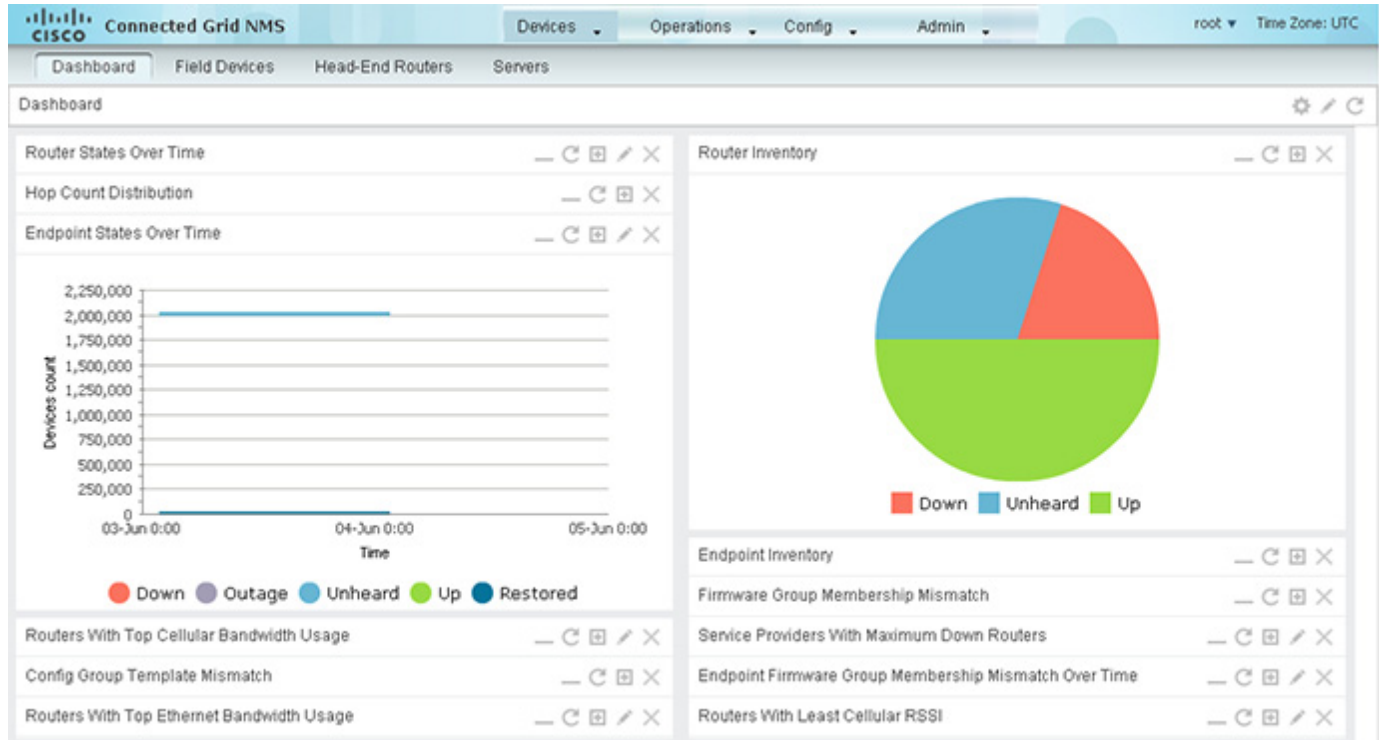
Setting the Dashlet Refresh Interval

To set the refresh interval for dashlets:

1. Choose **Devices > Dashboard**.

2. Click the **Settings** button (⚙).

3. Click **Set Refresh Interval**.
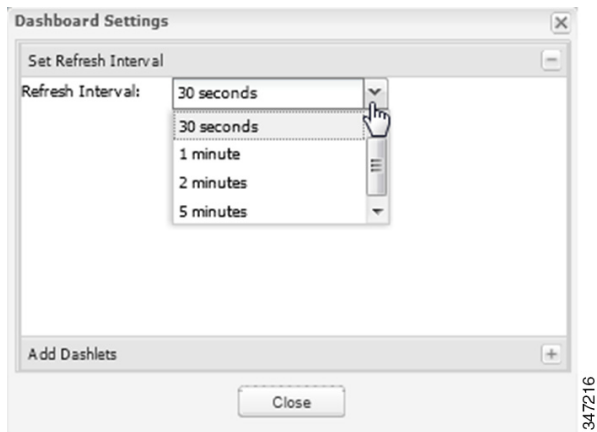
Note: On line-graph dashlets, open the filter bar and click an interval button to display metrics for that time period.

4. From the drop-down menu, choose a refresh interval.

5. Close the Dashboard Settings dialog box when finished.

Adding Dashlets

To add dashlets to the Dashboard:

1. Choose **Devices > Dashboard**.

2. Click the **Settings** button (⚙).
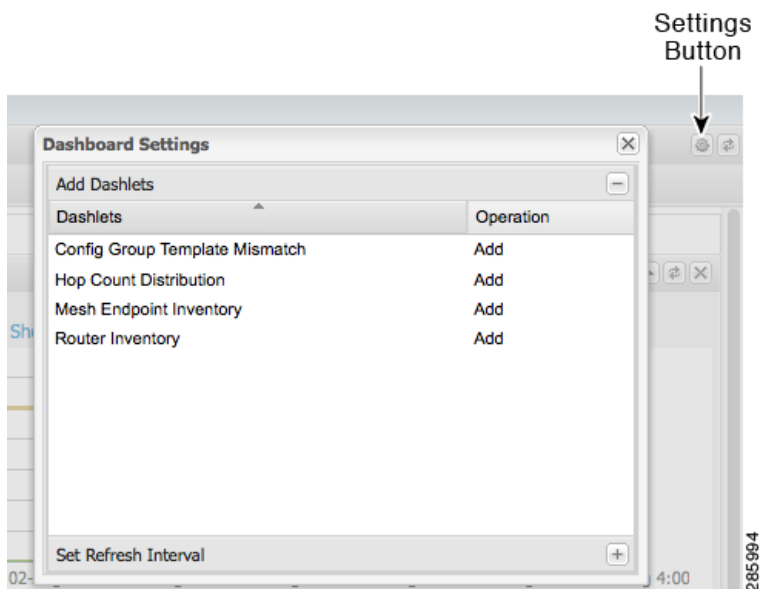
3. Click **Add Dashlets**.

   Note: No dashlets display in this dialog box if all are displaying on the Dashboard.

4. Click the dashlet to add to the Dashboard.

5. Close the Dashboard Settings dialog box when finished.

Removing Dashlets

To delete dashlets from the Dashboard:

1. Choose **Devices > Dashboard**.

2. Click the dashlet **Close** button.

Using Pie Charts to Get More Information

Mouse over any segment of a pie chart to display a callout with information on that segment. Click any segment in the Router Inventory and Mesh Endpoint Inventory pie charts to display the devices in List View.

Setting Dashlet Time Properties

To specify the time interval for data collection for line-graph dashlets, click the interval icon (✐) in the title bar to display the **6h**, **1d**, **1w**, **4w**, or **Custom** buttons. The **6h** button sets the data-collection time interval to the last six hours. The **1d** button sets the time interval to the last 24 hours.

To specify a custom time interval for a line-graph dashlet:

1. Click **Custom**.
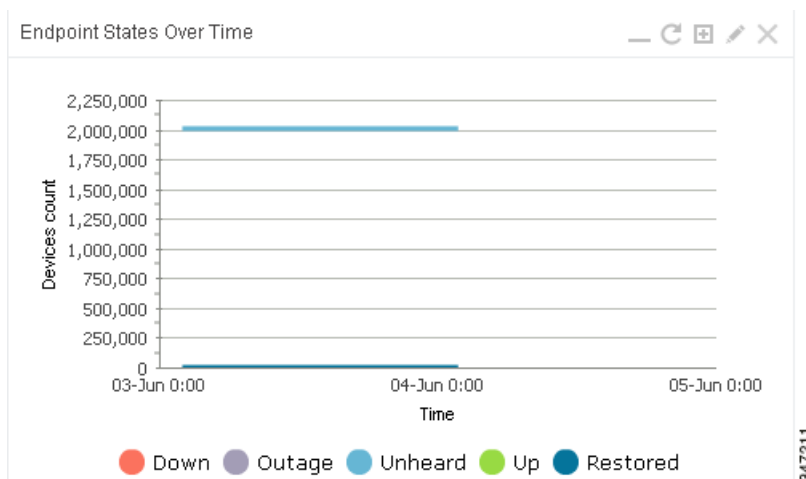
2. In the **From** fields, specify the beginning date and time.
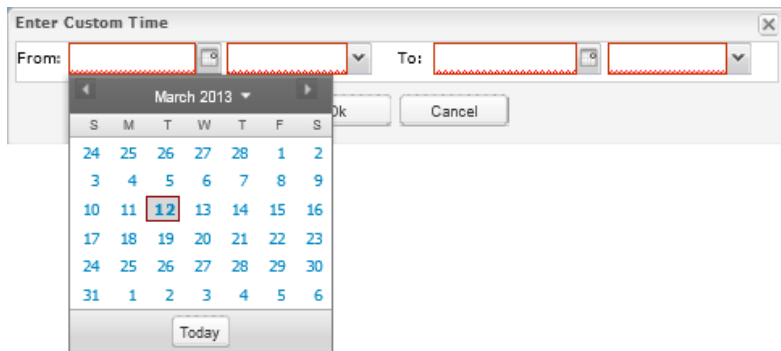
3. In the **To** fields, specify the end date and time.

4. Click **OK**.

Collapsing Dashlets

Click the show/hide icon (⏶) at the top-right of the dashlet to collapse it to its title bar.

Using the Series Selector

You use the Series Selector to refine line-graphs to display by device status. The device options are:

- Routers: Down, Outage, Unsupported, Unheard, and Up

- Mesh Endpoint Config Group: Config Out of Sync and Config In Sync

- Mesh Endpoint Firmware Group: Membership Out of Sync and Membership In Sync

- Mesh Endpoint States: Down, Outage, Unheard, and Up

To use the Series Selector:

1. Click **Series Selector**.
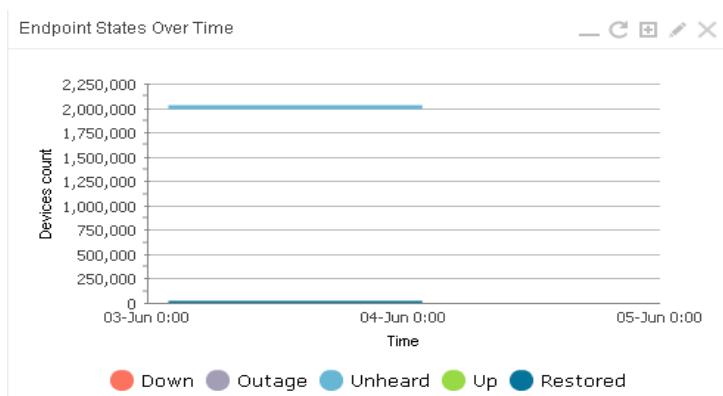
2. In the **Series Selector** dialog box, check the check boxes for the data series to show in the graph.
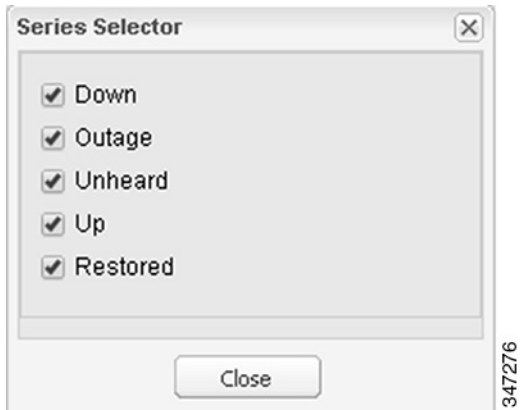
3. Click **Close**.

Using Filters

You use filters to refine the displayed line-graph data by groups. Applied filters display after the dashlet title.

To use the filters:

1. Click **Add Filter** in the line-graph dashlet pane.
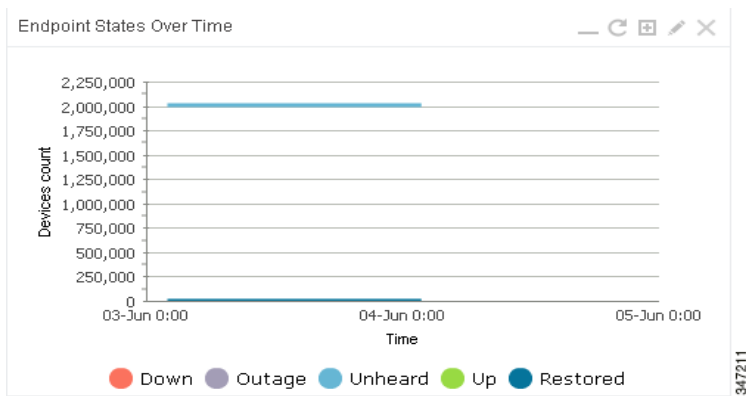
2. From the first drop-down menu, choose a group type.
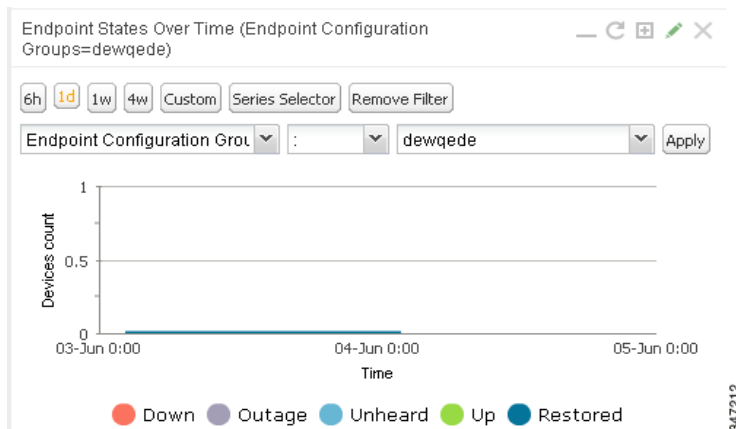
3. From the third drop-down menu, choose a group.

4. Click **Apply**.

The pencil icon is green and the filter displays next to the dashlet name to indicate that a filter is applied.

Note: Click the **Remove Filter** button to remove the filter and close the filter options.

Exporting Dashlet Data

You can export dashlet data to a CSV file.

To export dashlet data:

1. On the desired dashlet, click the export button (![export icon]).

A browser download session begins.

2. Navigate to your default download directory to view the export file.

The filename begins with the word "export-" and includes the dashlet name (for example, export-Node_State_Over_Time_chart-1392746225010.csv).

Monitoring Events

This section provides an overview of events and how to search and sort events, including the following topics:

- Viewing Events

- Filtering by Severity Level

- Advanced Event Search

- Sorting Events

- Searching By Event Name

Viewing Events

As shown in Figure 3, the Events page (**Operations > Events**) lists all events for those devices that CG-NMS tracks. All events are stored in the CG-NMS database server.

272

Figure 3   Events Page
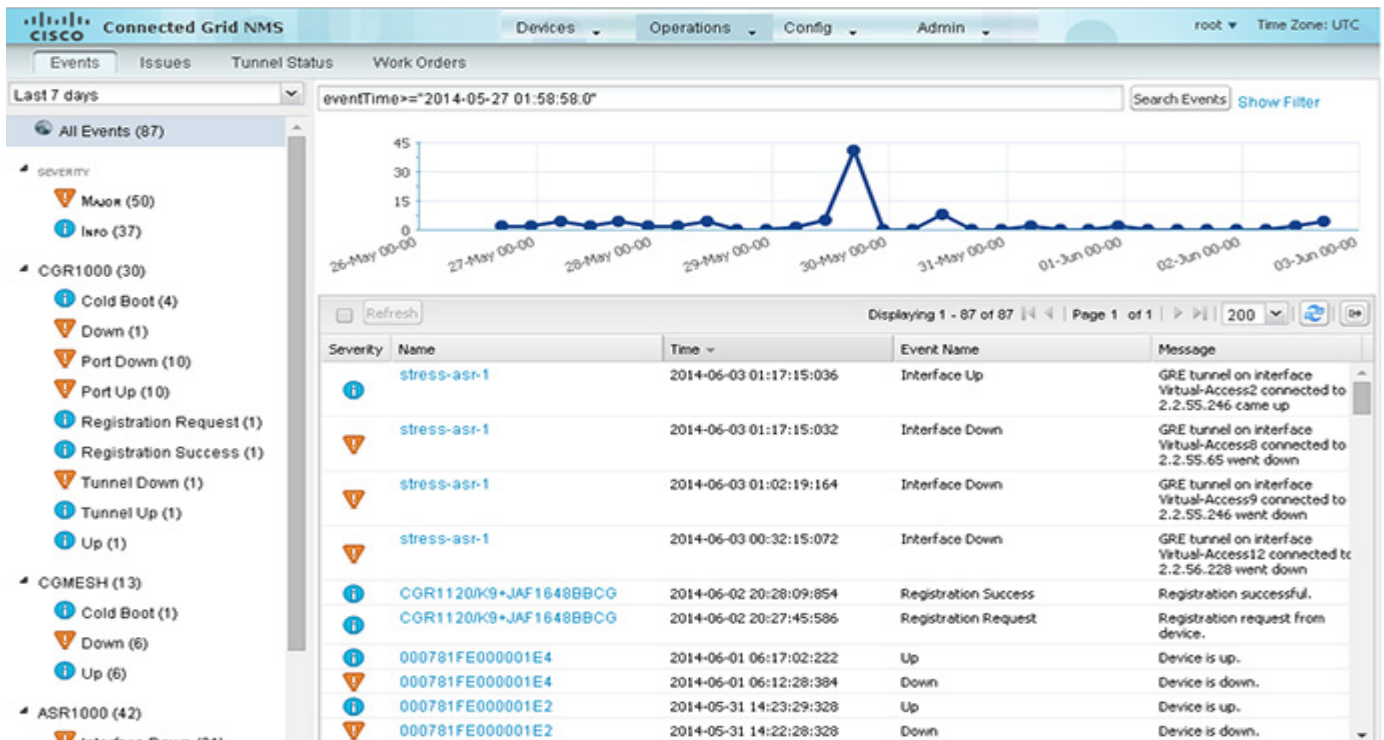
By default, the Events page displays the Events chart, which is a visual view of events in a time line. However, depending on the number of devices the CG-NMS server manages, this page can sometimes time out, especially when the system is fully loaded. In that case, open the Preferences window by choosing *username* > **Preferences** (top right), clearing the check boxes for showing chart and summary counts on the Events page, and clicking Apply.
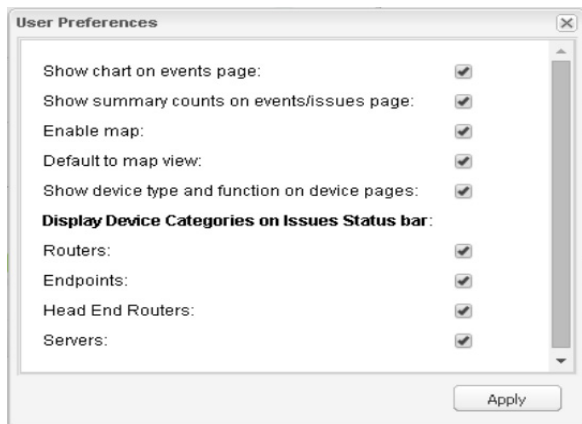
To limit the amount of event data displayed on this page, use the Filter drop-down menu (at the top of the left pane). For example, you can show the events for the last 24 hours relative to the last 30 days, or events for a specific day within the last seven days.

To enable automatic refresh of event data to refresh every 14 seconds, check the check box next to the **Refresh** button. To immediately refresh event data click the **Refresh** button or the refresh icon.

Note: The amount of event data displayed on the Events page is limited by the data retention setting for events (**Admin > System Management > Data Retention**).

All Events Pane Filters

Use the preset filters in the All Events pane to only view those event types.

Device Events

In the left pane, CG-NMS tracks events for the following devices:

- Routers

- Endpoints

- Head-end Devices

- CG Mesh Devices

- NMS Servers

- Database Servers

Event Severity Level

In the left pane, select an event severity level to filter the list view to devices with that severity level:

- Critical

- Major

- Minor

- Info

Each event type has a preset severity level. For example, a Router Down event is a Major severity level event.

Preset Events By Device

CG-NMS has a preset list of events it reports for each device it tracks. A list of those events is summarized under each device in the left pane on the Events page. For example, in the left pane click the show/hide icon (▶) next to Routers to expand the list of all events for routers.

Filtering by Severity Level

To filter by severity level:

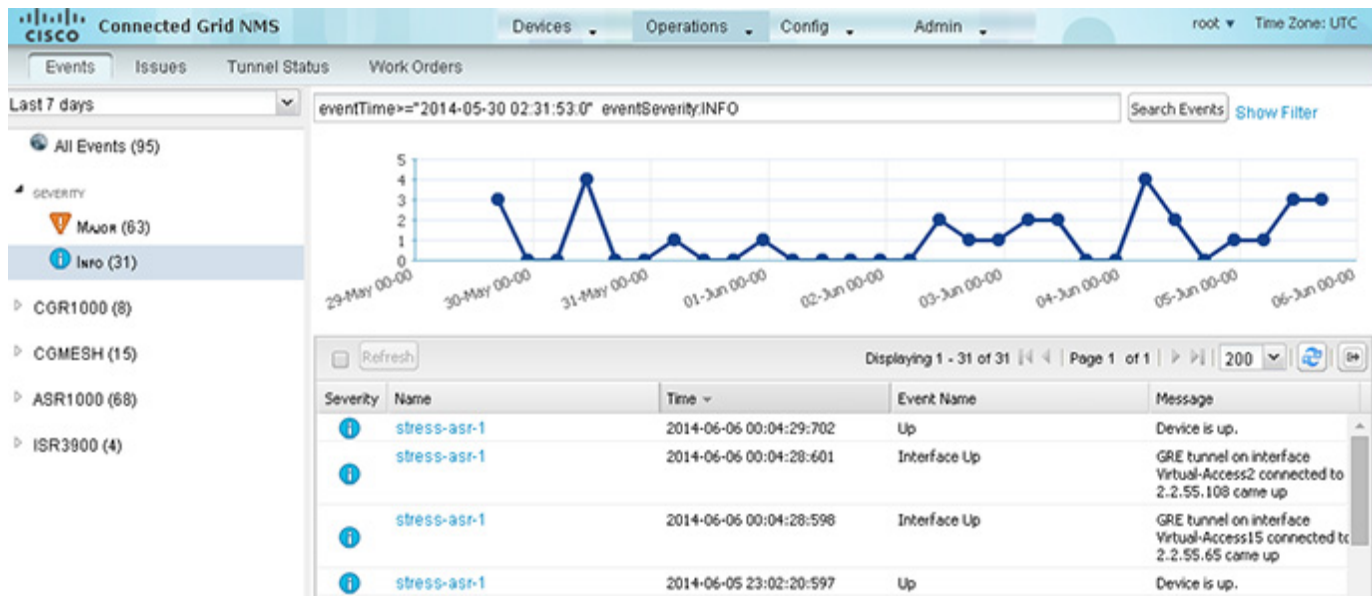1. Choose **Operations > Events**.

2. Click the **SEVERITY** show/hide arrow.

   Note: Only severity levels that have occurred display.

3. Click a severity level (**CRITICAL**, **MAJOR**, **MINOR**, OR **INFO**).

All events of that severity level display in the Events pane.

Advanced Event Search

To use the filter to search for events:

1. Choose **Operations > Events**.

2. Under All Events (left pane), select an event category to narrow down your search.

3. Click the **Show Filter** link at the top of the main pane.

4. Use the filter drop-down menus and fields to specify your search criteria.

5. Click the plus button (+) to add the search strings to the Search field.

Repeat the process of adding search strings to the Search field as needed.

6. Click **Search Events** or press Enter.

The search results display in the Events pane.

You can also add search strings manually, as shown in the following examples:

■ To filter events by Name (EID), enter the following string in the Search Events field, as shown in Figure 3:
name: *router eid string*.
Search Events by Name Filter

Note: Note the use of the asterisk (*) wild card with this filter.

■ To filter by event time period, enter the following string in the Search Events field, as shown in Figure 4:
eventTime*operator*"*YYYY–MM–DD HH:MM:SS:SSS*"

Supported operators are: <, >, >=, <=, :

Note: Do not enter a space between **eventTime** and the operator.

Figure 4   Search Events by Time Filter Example

Sorting Events

To sort events in ascending or descending order, mouse over any column and select the appropriate option from the heading drop-down menu.

Searching By Event Name

To search by event name (for example, Battery Low):

1. Choose **Operations > Events**.

2. Click the device type to search for in the left pane.

3. Click the **Show Filter** link at the top of the right pane.

The filter fields display under the Search Events field.

4. Choose **Event Name** from the left drop-down menu.

5. Choose the event name from the options in the right drop-down menu.

6. Click the plus button (+) at the right to add the filter to the Search Events field.

   The filter syntax appears in the Search Events field.

7. Click the **Search Events** button.

   The search results display in the Events pane.

Exporting Events

You can export events to a CSV file to examine as a log of event severity, time, name and event description by device.

To export events:

1. Choose **Operations > Events**.

2. Click the desired severity level or device type in the left pane.

3. Click the **Export** button (⇥).

   A browser download session begins.

4. Navigate to your default download directory to access the CSV file.

Monitoring Issues

This section provides an overview of issues and how to search for and close issues in CG-NMS, including the following topics:

- Viewing Issues

- Viewing Device Severity Status on the Issues Status Bar

- Adding Notes to Issues

- Searching Issues Using Predefined Filters

- Search Issues Using Custom Filters

- Closing an Issue

Viewing Issues

CG-NMS offers different ways to monitor issues:

- The **Operations > Issues** page (Figure 5) provides a snapshot of the health of the network by highlighting only major and critical events that are active within the network.

- The Issues Status bar (Figure 6) displays in the footer of the browser window and shows a count of all issues by severity for selected devices.

Figure 5   Issues Page

The Issues page provides an abbreviated subset of unresolved network events for quick review and resolution by the administrator. Issues remain open until either the associated event is resolved (and CG-NMS generates a resolution event) or the administrator manually closes the event.

Only one issue is recorded when multiple entries for the same event are reported. Each issue has a counter associated with it. As an associated event is closed, the counter decrements by one. Every open or closed issue has an associated event.

Note: The amount of closed issues data that displays on the Issues page is limited by the **Keep Closed Issues for** data retention setting (**Admin > System Management > Data Retention**), which is based on the time the issue was closed. When the issue was closed displays as the Last Update Time for the issue.

Viewing Device Severity Status on the Issues Status Bar

A tally of issues listed by severity for the selected devices displays in the Issues status bar in the bottom-right of the browser window frame (Figure 6). You can set the device types for issues that display in the Issues status bar in User Preferences (see Setting User Preferences).

Figure 6   Issues Status Bar

Click the Issues status bar to view the Issues Summary pane (Figure 7), which displays issues listed by the selected device category. Click count links in the Issues Summary pane to view complete issue criteria filtered by severity on the **Operations > Issues** page.

Figure 7   Issues Summary Pane

Adding Notes to Issues

On the **Operations > Issues** page, you can maintain notes on issues for the device. Click the Notes link inline with the issue to access any notes entered in the issue or add a note on the Notes for Issues Name page. You can and edit and delete notes from issues on this page. Issues can have multiple notes. The Notes for Issues Name page displays the time the note was created, the name of the user who wrote the note, and the text of the note. You can also add a note when closing a issue. Notes are purged from the database with the issue.

To add a note to an issue:

1. Click the **Notes** link inline with the desired issue or check the check box of the device and click **Add Note**.

The Notes for Issues Name pane displays. The issue in the following example has existing notes.

Monitoring Issues

2. Click **Add Note**.

   The Add Note dialog displays.

3. Insert your cursor in the **Note** field and type your note.

4. Click **Add** when finished.

The note text displays on the Notes for Issues Name pane in the Note column.

To add notes to issues with existing notes:

1. Click the **Notes** link inline with the issue or check the check box of the device and click **Add Note**.

   The Notes for Issues Name pane displays.

2. To add a new note to the issue, click **Add Note**.

   The Add Note dialog displays.

3. Insert your cursor in the **Note** field and type your note.

4. Click **Add** when finished.

To edit an existing note in an issue:

1. Click the **Notes** link inline with the issue.

   The Notes for Issues Name pane displays.

2. To edit an existing note, click the pencil icon (/) at the right of the note that you want to edit.

Monitoring Issues

3. Edit the note, and click **Done** when finished.

To delete a note from an issue:

1. Click the **Notes** link inline with the issue.

The Notes for Issues Name pane displays.

2. To delete a note, click the red X icon (✖) at the right of the note.

3. Click **Yes** to confirm the deletion.

To add a note when closing an issue:

1. Check the check box of the issue to close.

2. Click **Close Issue**.

3. In the Confirm dialog box, insert your cursor in the Note field and type the note text.

4. To confirm that you want to close the issue and save the note, click **Yes**.

283

Searching Issues Using Predefined Filters

To search for open issues for a specific system or severity level:

1. Choose **Operations > Issues**.

   To list only open issues, click **All Open Issues** (left pane).

   Note: By default, CG-NMS displays all issues that occurred within the specified data retention period (see Configuring Data Retention). To see Closed Issues associated with an event type or severity level, change **issueStatus:OPEN** to **issueStatus:CLOSED** in the Search Issues field, and then click **Search Issues**. To list all closed issues, in the left pane, click **All Closed Issues**.

2. Click a device category, event type, or severity level to filter the list.

The filter syntax appears in the Search Issues field, and the search results display in the main pane.

Search Issues Using Custom Filters

To search by creating custom filters:

1. Choose **Operations > Issues**.

2. Click **Show Filter**.

3. From the Filter drop-down menus, choose the appropriate options.

   For example, to filter severity levels by EID:

   - In the left pane, select a severity level.
   - From the first Filter drop-down menu, choose **EID**.
   - In the third Filter field, enter the EID of the device to discover issues about.

   You can also enter the search string in the Search Issues field. For example:

   issueSeverity:CRITICAL issueStatus:OPEN eid:CG-NMS-DB+localhost

4. Click **Search Issues**.

   The issues, if any, display in the Search Issues section (right pane).

Monitoring Issues
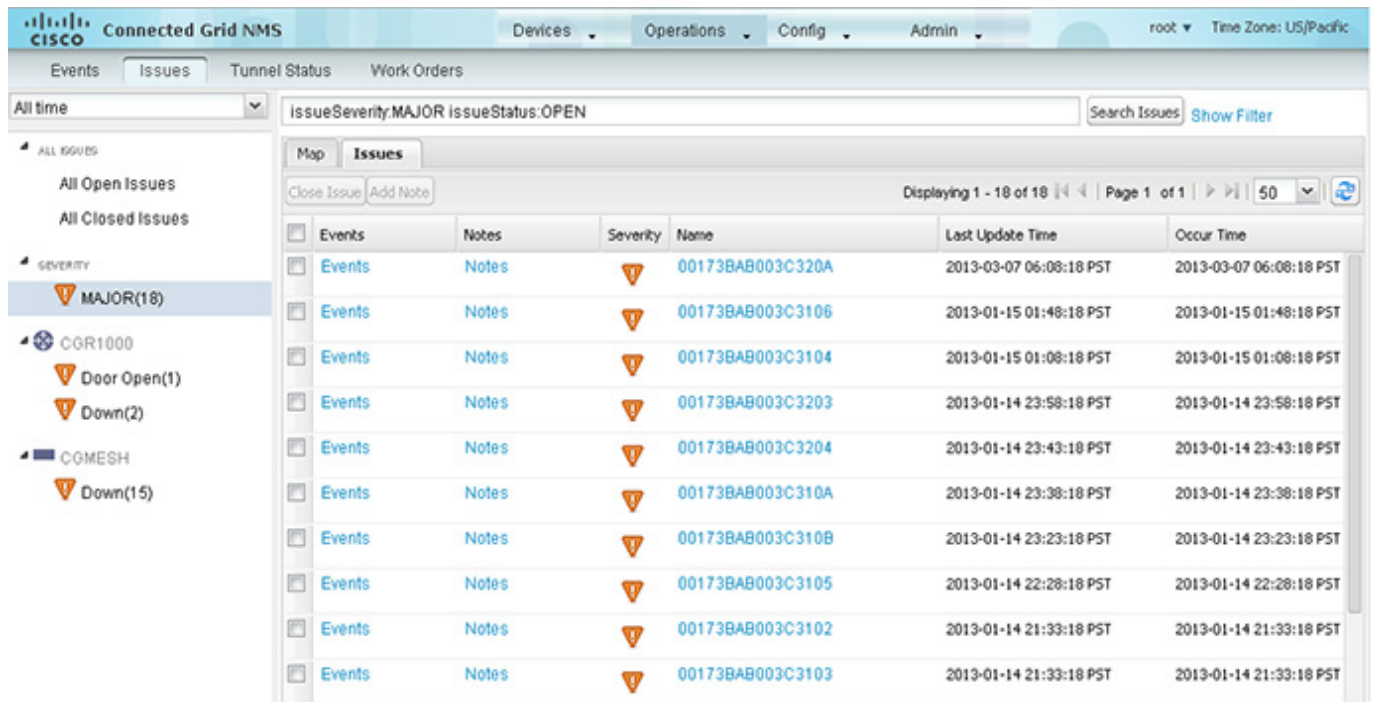
5. Click the **Events** link to display events associated with an issue.

   The Events for Issue Name pane displays all events for that device.
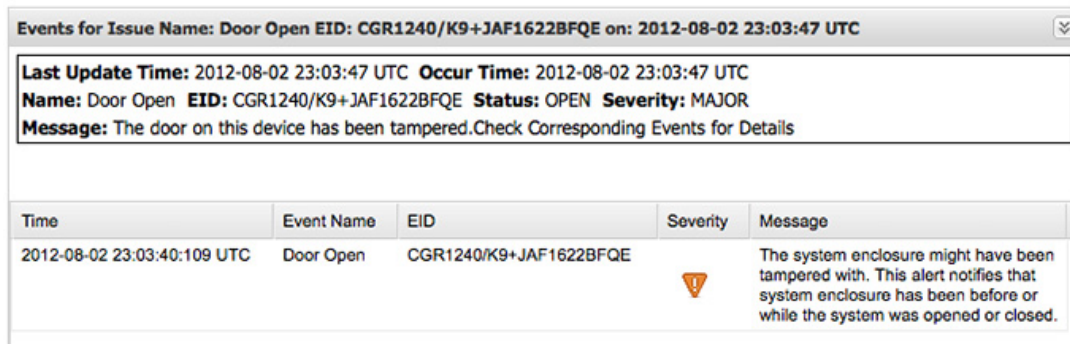
6. Click **Search Issues** or any link in the left pane to return to the Issues pane.

Closing an Issue

In most cases, when an event is resolved, the issue is closed automatically by the software. However, when the administrator has actively worked on resolving the issue, it might make sense to close the issue directly. When the issue is closed, CG-NMS generates an event.

To close a resolved issue:

1. Choose **Operations > Issues**.

2. Locate the issue by following the steps in either the Searching Issues Using Predefined Filters or Search Issues Using Custom Filters section.

3. In the Search Issues section (right pane), check the check boxes of the issues to close.

4. Click **Close Issue**.

   Note: You can also add a note to the issue at this time.

5. Click **Yes**.

Viewing Device Charts

- Router Charts

- Mesh Endpoint Charts

Router Charts

CG-NMS provides these charts in the Device Info pane on the Device Details page for any FAR:

Table 1   Device Detail Charts

Chart	Description
Mesh Link Traffic	Shows the aggregated WPAN rate for a FAR over time.
Mesh Endpoint Count	Shows the number of MEs over time.
Cellular Link Traffic	Shows the aggregated WPAN rate per protocol over time.
Cellular RSSI	Cellular RSSI.
WiMAX Link Traffic	Shows the receiving and sending rates of the WiMAX link traffic for the FAR over time.
WiMAX RSSI	Shows the receiving and sending rates of the WiMAX RSSI traffic for the FAR over time.
WPAN Traffic	(Master only) Shows Dual PHY WPAN traffic trends.
Ethernet Link Traffic	Shows the receiving and sending rates of the Ethernet traffic for the FAR over time.
Cellular Bandwidth Usage Over Time	Shows the bandwidth usage over time for the cellular interface.
Ethernet Bandwidth Usage Over Time	Shows the bandwidth usage over time for the Ethernet interface.

Figure 8 shows the Mesh Link Traffic and Mesh Endpoint Count charts.

Figure 8 **FAR Device Charts**
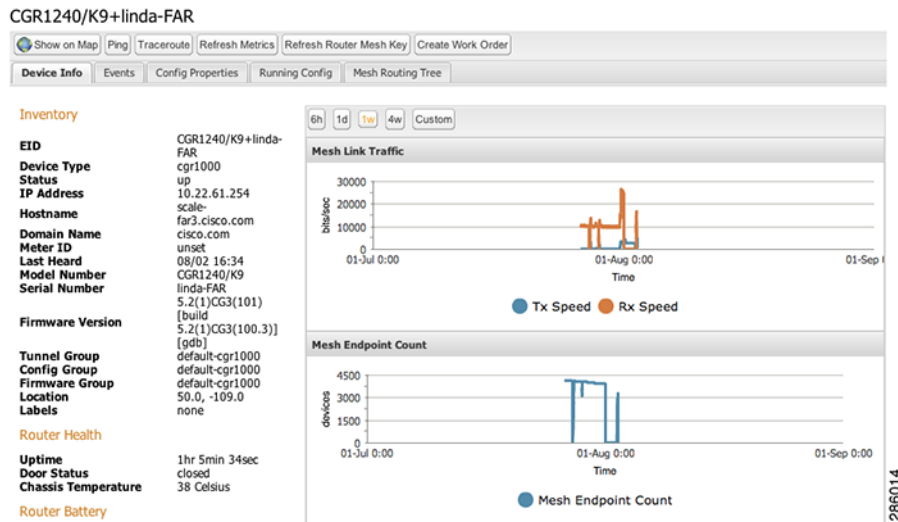
Mesh Endpoint Charts

CG-NMS provides the charts listed in Table 2 in the Device Info pane on the Device Details page (Figure 9) for any ME.

Table 2 **Device Detail Charts**

Chart	Description
Mesh Link Traffic	Shows the aggregated WPAN rate for a FAR over time.
Mesh Path Cost and Hops	Shows the RPL path cost value between the element and the root of the routing tree over time (see Configuring RPL Tree Polling).
Mesh Link Cost	Shows the RPL cost value for the link between the element and its uplink neighbor over time.
Mesh RSSI	Shows the measured RSSI value of the primary mesh RF uplink (dBm) over time.

Viewing Device Charts

Figure 9   Mesh Endpoint Device Charts

<< Back

00173BAB003C3100

| Show on Map | Ping | Traceroute | Sync Config Membership | Sync Firmware Membership | Block Mesh Device |

| **Device Info** | Events | Config Properties | Mesh Routing Tree |

Inventory

EID	00173BAB003C3100
Device Type	cgmesh
Status	up
IP Address	2001:dead:beef:6108:217:3bab:3c:3100
Meter ID	unset
Last Heard	2012-07-24 17:05
Model Number	OWCM/3.1
Serial Number	00173BAB003C3100
Firmware Version	5.0.92
Config Group	default-cgmesh
Firmware Group	default-cgmesh
Location	49.4, -132.9
Labels	none

Mesh Endpoint Health

Uptime	unknown

Mesh Link Settings

SSID	unit
PANID	323
Transmit Power	-34
Security Mode	1

Mesh Link Metrics

Mesh Link Transmit Speed	7.32 bits/sec
Mesh Link Receive Speed	121.63 bits/sec
Mesh Link Transmit Packet Drops	0 drops/sec
Mesh Route RPL Hops	3 hops
Mesh Route RPL Link Cost	1
Mesh Route RPL Path Cost	3
Mesh Route RSSI	-42 dBm
Mesh Route Reverse RSSI	-45 dBm
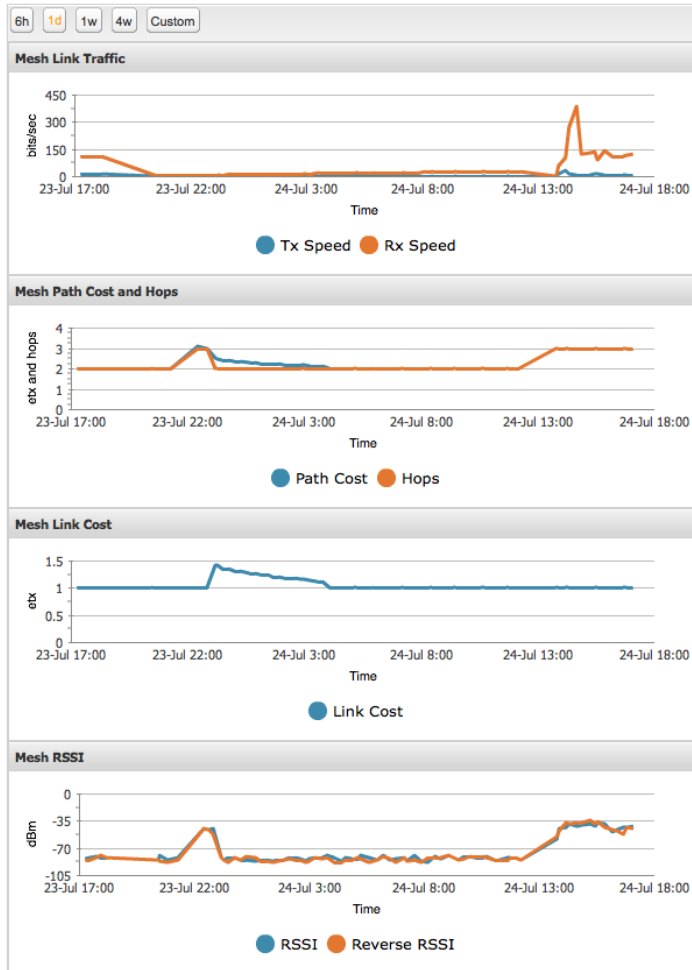
Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bits/sec)	Tx Drops (bits/sec)	Rx Speed (bits/sec)
lo	up	up	0:0:0:0:0:0:0:1/64		0		0
lowpan	up	up	2001:dead:beef:6108:217:3bab:3c:3100/64 fe80:0:0:0:217:3bab:3c:3100/64	00173bab003c3100	6.8		139.55
ppp	up	up	fe80:0:0:0:0:0:0:1/64	00173bab003c3100	13.24		7.43

Network Routes

Destination	Next Hop IP Address	Next Hop Element ID	Interface	Hops	Path Cost	Link Cost	RSSI	Reverse RSSI
default	fe80:0:0:0:217:3bab:3c:3102	00173BAB003C3102	lowpan	3	3	1	-39	-43

Routing Path

Hops	IP Address	Element ID	Status	Last Heard
this element	2001:dead:beef:6108:217:3bab:3c:3100	00173BAB003C3100	up	2012-07-24 17:05
1 hop	2001:dead:beef:6108:217:3bab:3c:3102	00173BAB003C3102	up	2012-07-24 16:44
2 Hops	2001:dead:beef:6108:217:3bab:3c:3208	00173BAB003C3208	up	2012-07-24 16:53

286000

Managing High Availability Installations

This chapter describes how to set up CG-NMS for high availability, and includes the following sections:

- Overview of CG-NMS High Availability

- HA Guidelines and Limitations

- Configuring CG-NMS Installations for HA

Overview of CG-NMS High Availability

This section provides an overview of CG-NMS high availability installations, including the following sections:

- Load Balancer

- Server Heartbeats

- Database High Availability

- Tunnel Redundancy

CG-NMS is a critical application for monitoring and managing a connected grid. CG-NMS High Availability (CG-NMS HA) solutions address the overall availability of CG-NMS during software, network, or hardware failures.

CG-NMS provides two main levels of HA, as shown in Figure 1:

- CG-NMS Server HA—This is achieved by connecting multiple CG-NMS servers to a Cisco ACE 4710 load balancer. Traffic originating at MEs, FARs, and ASRs goes to the load balancer, which uses a round-robin protocol to distribute the load among the CG-NMS cluster servers.

- CG-NMS Database HA—This is achieved by configuring two CG-NMS Database servers: a primary server and a standby (or secondary) server. When the primary database receives new data it sends a copy to the standby database. A separate system runs the Observer (the Observer can also run on the standby server), which is a program that monitors the CG-NMS Database servers. If the primary database fails, the Observer configures the standby server as the new primary database. CG-NMS Database HA works in single and cluster CG-NMS server deployments.

289

Figure 1   CG-NMS Server and Database HA
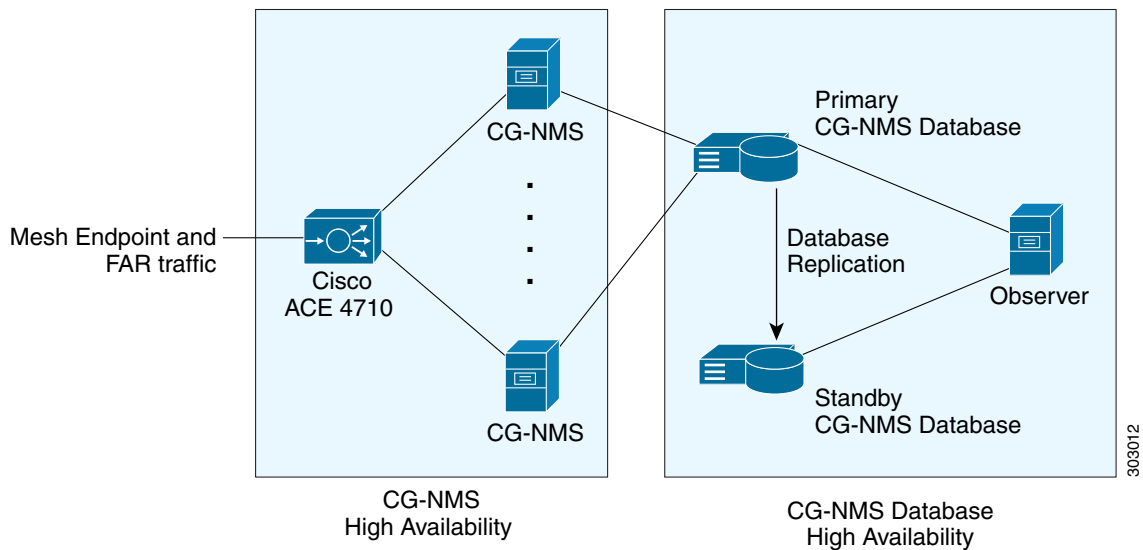
In addition to CG-NMS Server and Database HA, CG-NMS improves reliability by adding tunnel redundancy. This is achieved by defining multiple tunnels between one FAR and multiple ASRs. If one tunnel fails, the FAR routes traffic through another tunnel.

Figure 2   CG-NMS Tunnel Redundancy
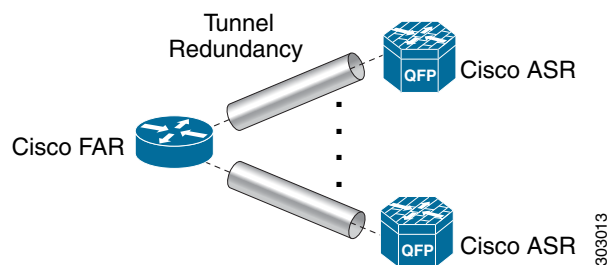
CG-NMS HA addresses these failure scenarios:

Failure Type	Description
CG-NMS server failure	If a server within a CG-NMS server cluster fails, the load balancer routes traffic to the other servers in the cluster.
CG-NMS database failures	If the primary database fails, the associated standby database becomes the primary database. This is transparent to the CG-NMS servers. All CG-NMS servers in the cluster connect to the new primary database.
Tunnel failure	If a tunnel fails, traffic flows through another tunnel.

Load Balancer

The Load Balancer (LB) plays a critical role in CG-NMS HA, as it performs these tasks:

- Load balances traffic destined for CG-NMS.

- Maintains heartbeats with servers in the cluster and detects any failure. If a CG-NMS server fails, the LB directs traffic to other cluster members.

Cisco recommends using the Cisco ACE 4710 (Cisco ACE) as the load balancer in this deployment. See http://www.cisco.com/en/US/partner/products/ps7027/tsd_products_support_series_home.html for information on the Cisco ACE 4710.

Server Heartbeats

The LB maintains heartbeats with each CG-NMS server in the cluster. In the health monitoring mechanism adopted by the CG-NMS solution (there are alternate solutions), the heartbeats are regular GET messages to CG-NMS on port 80. CG-NMS expects an HTTP 200 OK response from an active CG-NMS server.

You can configure these heartbeat parameters on the LB:

- Periodicity of probes—This is the number of seconds between heartbeats. The default value on the Cisco ACE is 15 seconds

- Number of retries—This is the number of times the LB tries to send a heartbeat to a non-responding CG-NMS server before declaring it down. The default number of retries is 3.

- Regular checks after failure detection—The LB checks whether the server is back online at this time interval. The default failure detection check value is 60 seconds.

Database High Availability

CG-NMS Database HA works in CG-NMS single-server and cluster deployments. CG-NMS HA uses Oracle Active Dataguard to deploy Oracle HA. To configure HA for the CG-NMS Database, use the Oracle Recovery Manager (RMAN) and Dataguard Management CLI (DGMGRL).

The CG-NMS Database HA configuration process involves:

- Configuring the primary and secondary databases the same on separate physical servers.

    Note: The secondary database server is also referred to as the standby database.

    Note: There is a possibility of losing some data during a database failover.

- Configuring data replication to be performed over SSL using an Oracle *wallet*. The wallet contains a self-signed certificate to facilitate quick deployment.

    Note: The Oracle wallet bundled with the CG-NMS RPMs uses self-signed certificates. You can configure custom certificates and wallet to facilitate replication.

    Note: There is no performance impact when performing data replication over SSL.

- Using the sys user for replication and *not* cgms_dev.

- Configuring replication as asynchronous to prevent performance bottlenecks.

By default, CG-NMS connects to the database using TCP over port 1522. Replication uses TCPS (TCP over SSL) on port 1622.

The scripts for configuring CG-NMS Database HA are included in the CG-NMS Oracle Database RPM package (cgms-oracle-*version_number*.x86_64.rpm). When you install the CG-NMS Database, the HA scripts are located in $ORACLE_HOME/cgms/scripts/ha.

Tunnel Redundancy

To add another layer of redundancy to your CG-NMS deployment, configure multiple tunnels to connect every FAR in a FAR tunnel provisioning group to multiple ASRs. For example, you could configure CG-NMS to provision two tunnels for every FAR. One tunnel is active over the Cellular interface, while the redundant tunnel is configured to communicate with a second ASR over the WiMAX interfaces.

To configure tunnel redundancy, you need to:

1. Add ASRs to a tunnel provisioning group.

2. Modify the tunnel provisioning templates to include commands to create additional tunnels.

3. Define policies that determine the mapping between interfaces on the FAR and ASR interfaces:

   ■ Configuring Tunnel Provisioning Policies

   ■ Modifying the Tunnel Provisioning Templates for Tunnel Redundancy

HA Guidelines and Limitations

Note the following about CG-NMS HA configurations:

■ CG-NMS HA does not include HA support for other network components like FARs, ASRs, and the load balancer.

■ Zero service downtime is targeted by CG-NMS HA, but it is not guaranteed.

■ All CG-NMS nodes must on the same subnet.

■ All CG-NMS nodes must run on similar hardware.

■ All CG-NMS nodes must run the same software version.

■ Run the CG-NMS setup script (/opt/cgms/bin/setupCgms.sh) on all the nodes.

■ Run the DB migration script (/opt/cgms/bin/db-migrate) on only one node.

■ The /opt/cgms/bin/print_cluster_view.sh script displays information about CG-NMS cluster members.

Configuring CG-NMS Installations for HA

This section describes the various configuration settings for CG-NMS HA installations, including the following sections:

■ Setting Up CG-NMS Database for HA

■ Disabling CG-NMS Database HA

■ Load-Balancing Policies

■ Running LB Configuration Example

■ Configuring Tunnel Provisioning Policies

■ Modifying the Tunnel Provisioning Templates for Tunnel Redundancy

Setting Up CG-NMS Database for HA

To set up the CG-NMS Database HA:

1. Set up the standby database (see Setting Up the Standby Database).

> **Note:** Always configure the standby database first.

- The default SID for the standby server is **cgms_s** and *not* cgms.
- Before setting up the standby server for HA, ensure that the environment variable $ORACLE_SID on the standby server is set to **cgms_s**.
- The port is always 1522.

2. Set up the primary database (see Setting Up the Primary Database).

- The default SID for the primary server is **cgms**.
- Before setting up the primary server for HA, ensure that the environment variable $ORACLE_SID on the primary server is set to **cgms**.

3. Set up CG-NMS for database HA (see Setting Up CG-NMS for Database HA).

4. Set up the database Observer (see Setting Up the Observer).

Setting Up the Standby Database

To set up the standby database server for HA, run the setupStandbyDb.sh script. This script prompts for configuration information needed for the standby database, including the IP address of the primary database.

```
$ ./setupStandbyDb.sh
$ Are you sure you want to setup a standby database ? (y/n)? y

09-20-2012 13:59:18 PDT: INFO: User response: y
09-20-2012 13:59:18 PDT: INFO: CGMS_S database does not exist.
Enter the SYS DBA password. NOTE: This password should be same as the one set on the primary server:
Re-enter password for SYS DBA:
09-20-2012 13:59:58 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-20-2012 14:00:09 PDT: INFO: User entered CG-NMS DB password.
Enter primary database server IP address: 192.168.1.12
09-20-2012 14:00:27 PDT: INFO: Cleaning up instance - cgms_s
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
…
Total System Global Area  329895936 bytes
Fixed Size    2228024 bytes
Variable Size  255852744 bytes
Database Buffers   67108864 bytes
Redo Buffers    4706304 bytes
...
09-20-2012 14:00:29 PDT: INFO: ========== CGMS_S Database Setup Completed Successfully ==========
```

Setting Up the Primary Database

To set up the primary database server for HA, run the setupHaForPrimary.sh script. This script prompts for configuration information needed for the primary database, including the IP address of the standby database.

```
$ ./setupHaForPrimary.sh
[oracle@pdb ha]$ ./setupHaForPrimary.sh
09-20-2012 13:58:39 PDT: INFO: ORACLE_BASE: /home/oracle/app/oracle
09-20-2012 13:58:39 PDT: INFO: ORACLE_HOME: /home/oracle/app/oracle/product/11.2.0/dbhome_1
09-20-2012 13:58:39 PDT: INFO: ORACLE_SID : cgms
09-20-2012 13:58:39 PDT: INFO: Make sure the above environment variables are what you expect

Are you sure you wish to configure high availability for this database server ? (y/n)? y

09-20-2012 13:58:45 PDT: INFO: User response: y
Enter standby database server IP address: 192.168.1.10
09-20-2012 13:58:56 PDT: INFO: Secondary listener reachable. Moving on with configuration
mkdir: cannot create directory `/home/oracle/app/oracle/oradata/cgms': File exists
09-20-2012 13:58:58 PDT: INFO: Reloading the listener to pick the new settings

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 13:58:58


…
DGMGRL> 09-20-2012 14:14:54 PDT: INFO: Please start the 'Observer' on appropriate server for ha
monitoring
Total time taken to perform the operation: 975 seconds
09-20-2012 14:14:54 PDT: INFO: ==========  Completed Successfully ==========
```

Setting Up the Observer

The Observer should run on a separate server, but can be set up on the server hosting the standby database.

Note: The password required for running Observer is the same as the SYS DBA password. See Creating the CG-NMS Oracle Database

To set up the Observer:

1. On a separate server, run the observer script.

```
$ ./manageObserver.sh start cgms_s password
$ DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
...
Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Observer started
```

2. Run the getHaStatus.sh script to verify that the database is set up for HA.

```
$ ./getHaStatus.sh
...
Configuration - cgms_dgconfig

  Protection Mode: MaxPerformance
  Databases:
    cgms   - Primary database
    cgms_s - (*) Physical standby database

Fast-Start Failover: ENABLED

Configuration Status:
SUCCESS

DGMGRL>
Database - cgms
```

294

```
   Role:          PRIMARY
   Intended State:  TRANSPORT-ON
   Instance(s):
     cgms

Database Status:
SUCCESS

DGMGRL>
Database - cgms_s

   Role:          PHYSICAL STANDBY
   Intended State:  APPLY-ON
   Transport Lag:   0 seconds
   Apply Lag:       0 seconds
   Real Time Query: OFF
   Instance(s):
     cgms_s

Database Status:
SUCCESS
```

Setting Up CG-NMS for Database HA

To set up CG-NMS for database HA:

1. Stop CG-NMS.

2. Run the setupCgms.sh script.

   The script prompts you to change the database settings. Enter **y**. Then, the script prompts you to enter the primary database server information (IP address, port, and database SID). After that, the script prompts you to add another database server. Enter **y**. Then, the script prompts you to enter the standby database server information (IP address, port, and database SID), as follows:

   Note: CG-NMS always uses port 1522 to communicate with the database. Port 1622 is only used by the database for replication.

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [128.107.154.246]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

295

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait
...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait
...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n

09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n

09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

Disabling CG-NMS Database HA

To disable CG-NMS Database HA:

1. On the server running the Observer program, stop the Observer:

```
$ ./manageObserver.sh stop cgms_s password
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
$ Observer stopped
```

2. On the standby CG-NMS Database server, delete the standby database:

```
$ ./deleteStandbyDb.sh

Are you sure you want to delete the standby database ? All replicated data will be lost (y/n)? y

09-20-2012 14:27:02 PDT: INFO: User response: y
09-20-2012 14:27:02 PDT: INFO: Cleaning up instance - cgms_s
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.
```

```
Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
DGMGRL> DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Disabled.
DGMGRL> 09-20-2012 14:27:06 PDT: INFO: Removing dataguard configuration
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Removed configuration
DGMGRL> 09-20-2012 14:27:07 PDT: INFO: Stopping the database

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:27:07 2012

Copyright (c) 1982, 2011, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> ORA-01109: database not open


Database dismounted.
ORACLE instance shut down.
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:27:19

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm)(PORT=1522))(CONNECT_DATA=(SERVER=DEDIC
ATED)(SERVICE_NAME=cgms_s)))
The command completed successfully
Cleaning up instance - cgms_s
09-20-2012 14:27:29 PDT: INFO: ==========  Completed Successfully ==========
```

3. On the primary CG-NMS Database server, delete the HA configuration:

```
$ ./deletePrimaryDbHa.sh
Are you sure you want to delete the high availability configuration ? All replicated data will be
lost (y/n)? y

09-20-2012 14:25:25 PDT: INFO: User response: y
09-20-2012 14:25:25 PDT: INFO: Removing secondary configuration from primary

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:25:25 2012

Copyright (c) 1982, 2011, Oracle.  All rights reserved.
```

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
System altered.
...
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
09-20-2012 14:25:28 PDT: INFO: Removing data guard config files
09-20-2012 14:25:28 PDT: INFO: Removing standby redo logs
09-20-2012 14:25:29 PDT: INFO: Creating listener file
09-20-2012 14:25:29 PDT: INFO: Listener successfully configured.
09-20-2012 14:25:29 PDT: INFO: Recreating tnsnames ora file
09-20-2012 14:25:29 PDT: INFO: reloading the listener

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:29

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
The command completed successfully

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:30

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Starting /home/oracle/app/oracle/product/11.2.0/dbhome_1/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 11.2.0.3.0 - Production
System parameter file is /home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Log messages written to
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
STATUS of the LISTENER
------------------------
Alias                     cgmstns
Version                   TNSLSNR for Linux: Version 11.2.0.3.0 - Production
Start Date                20-SEP-2012 14:25:30
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
/home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Listener Log File
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))
Services Summary...
Service "cgms" has 1 instance(s).
  Instance "cgms", status UNKNOWN, has 1 handler(s) for this service...
The command completed successfully
09-20-2012 14:25:30 PDT: INFO: ==========  Completed Successfully ==========
```

Load-Balancing Policies

The following table describes the load-balancing policy for each type of traffic the LB supports:

Traffic	Load Balancing Policy
HTTPS traffic to and from browsers and CG-NMS API clients (IPv4; ports 80 and 443)	The LB uses Layer 7 load balancing for all traffic from Web browsers and CG-NMS API clients. The LB uses stickiness for general HTTPS traffic.
For FAR IPv4 traffic going to ports 9121 and 9120: ■ Tunnel Provisioning on port 9120 over HTTPS ■ Regular registration and periodic on 9121 over HTTPS	The LB uses Layer 3 load balancing for all FAR traffic. This is the traffic from the FAR to CG-NMS.

For IPv6 CSMP traffic to and from mesh endpoints (MEs):
■ UDP traffic over port 61624
   – Registration
   – Periodic transmission of metrics
   – Firmware push
   – Configuration push
■ UDP traffic over port 61625
For outage notifications sent by MEs.
	The LB uses Layer 3 load balancing for all ME traffic to port 61624, and outage messages to port 61625.

Running LB Configuration Example

The following is an example of the running configuration of a properly configured CG-NMS LB:

```
# show running-config
Generating configuration....

ssh maxsessions 10

boot system image:c4710ace-t1k9-mz.A5_1_1.bin

hostname cgnmslb2
interface gigabitEthernet 1/1
  switchport access vlan 10
  no shutdown
interface gigabitEthernet 1/2
  description server-side
  switchport access vlan 11
  no shutdown
interface gigabitEthernet 1/3
  description client-side
  switchport access vlan 8
  no shutdown
interface gigabitEthernet 1/4
  switchport access vlan 55
  no shutdown
```

299

```
access-list ALL line 8 extended permit ip any any
access-list everyone line 8 extended permit ip any any
access-list everyone line 16 extended permit icmp any any
access-list ipv6_acl line 8 extended permit ip anyv6 anyv6
access-list ipv6_acl2 line 8 extended permit icmpv6 anyv6 anyv6



ip domain-lookup
ip domain-name cisco.com
ip name-server 171.68.226.120
ip name-server 171.70.168.183

probe http probe_cgnms-http
  port 80
  interval 15
  passdetect interval 60
  expect status 200 200
  open 1

rserver host 12-12-1-31
  ip address 12.12.1.31
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 12-12-1-32
  ip address 12.12.1.32
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-202
  description realserver 2002:cafe:server::202
  ip address 2002::202
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-211
  ip address 2002:cafe:server::211
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice

serverfarm host cgnms_2
  description cgnms-serverfarm
  probe probe_cgnms-http
  rserver 2002-cafe-server-202 61624
    conn-limit max 4000000 min 4000000
    inservice
  rserver 2002-cafe-server-211 61624
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host cgnms_2_ipv4
  probe probe_cgnms-http
  rserver 12-12-1-31
    conn-limit max 4000000 min 4000000
    inservice
  rserver 12-12-1-32
    conn-limit max 4000000 min 4000000
    inservice

sticky ip-netmask 255.255.255.255 address source CGNMS_SRC_STICKY
  serverfarm cgnms_2_ipv4


class-map type management match-any remote_access
```

```
    2 match protocol xml-https any
    3 match protocol icmp any
    4 match protocol telnet any
    5 match protocol ssh any
    6 match protocol http any
    7 match protocol https any
    8 match protocol snmp any
class-map type management match-all ssh_allow_access
    2 match protocol ssh any
class-map match-any virtual-server-cgnms
    2 match virtual-address 2002:server:cafe::210 udp eq 61624
class-map match-any vs_cgnms_ipv4
    3 match virtual-address 12.12.1.101 tcp eq https
    4 match virtual-address 12.12.1.101 tcp eq 9120
    5 match virtual-address 12.12.1.101 tcp eq 9121
    6 match virtual-address 12.12.1.101 tcp eq 8443
    7 match virtual-address 12.12.1.101 tcp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match virtual_cgnms_l7
  class class-default
    serverfarm cgnms_2
policy-map type loadbalance first-match vs_cgnms_l7_v4
  class class-default
    sticky-serverfarm CGNMS_SRC_STICKY

policy-map multi-match cgnms_policy_ipv6
  class virtual-server-cgnms
    loadbalance vip inservice
    loadbalance policy virtual_cgnms_l7
    loadbalance vip icmp-reply active
policy-map multi-match int1000
  class vs_cgnms_ipv4
    loadbalance vip inservice
    loadbalance policy vs_cgnms_l7_v4
    loadbalance vip icmp-reply active

interface vlan 8
  bridge-group 1
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
interface vlan 10
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  service-policy input int1000
  no shutdown
interface vlan 11
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
interface vlan 55
  bridge-group 1
  access-group input everyone
  access-group input ipv6_acl
  service-policy input cgnms_policy_ipv6
  no shutdown
```

```
interface bvi 1
  ipv6 enable
  ip address 2002:server:cafe::206/64
  no shutdown
interface bvi 2
  ip address 12.12.1.100 255.255.255.0
  no shutdown

domain cisco.com

ip route 2011::/16 2002:server:cafe::101
ip route 2001:server:cafe::/64 2002:cafe::101
ip route 11.1.0.0 255.255.0.0 12.12.1.33
ip route 15.1.0.0 255.255.0.0 12.12.1.33
ip route 13.211.0.0 255.255.0.0 12.12.1.33

context VC_Setup1
  allocate-interface vlan 40
  allocate-interface vlan 50
  allocate-interface vlan 1000

username admin password 5 $1$CB34uAB9$BW8a3ijjxvBGttuGtTcST/  role Admin domain
default-domain
username www password 5 $1$q/YDKDp4$9PkZl1SBMQW7yZ7E.sOZA/  role Admin domain de
fault-domain

ssh key rsa 1024 force
```

Configuring Tunnel Provisioning Policies

Use tunnel policies to configure multiple tunnels for a FAR. Each tunnel is associated with an interface on a FAR and an HER. If a tunnel provisioning group has one or more HERs, CG-NMS displays a policy in the Tunnel Provisioning Policies tab (**Config > Tunnel Provisioning**). Use this policy to configure FAR-to-HER interface mapping.

To map FAR-to-HER interfaces in CG-NMS:

1. Choose **Config > Tunnel Provisioning**.

2. In the TUNNEL GROUPS pane, select a group to configure with tunnel redundancy.

3. Create a CSV or XML file that lists the HERs to add to the group in the format *EID, device type*, as follows:

```
eid,deviceType
asr-0, asr1000
asr-1, asr1000
asr-2, asr1000
```

4. Click **Assign Devices to Group** to import the file and add HERs to the group.
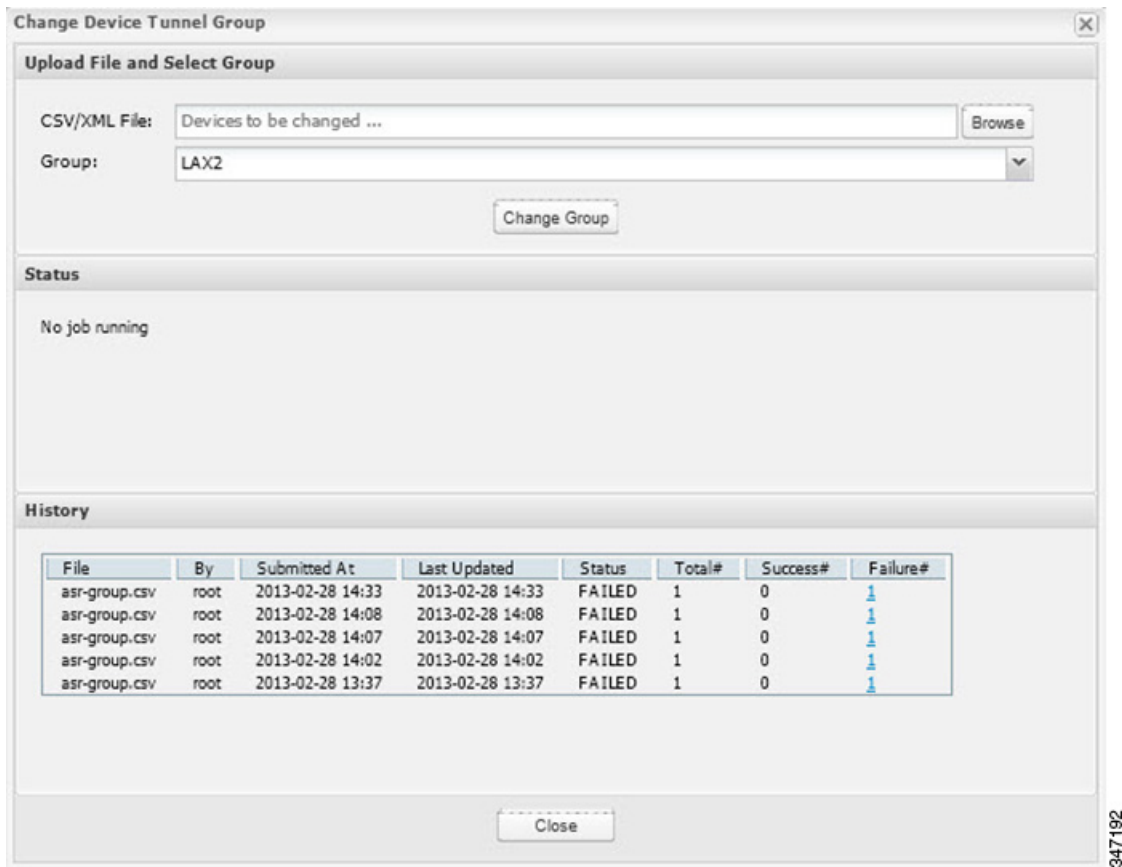
Note: An HER can a member of multiple tunnel provisioning groups.

5. With the tunnel provisioning group selected, click the **Policies** tab.
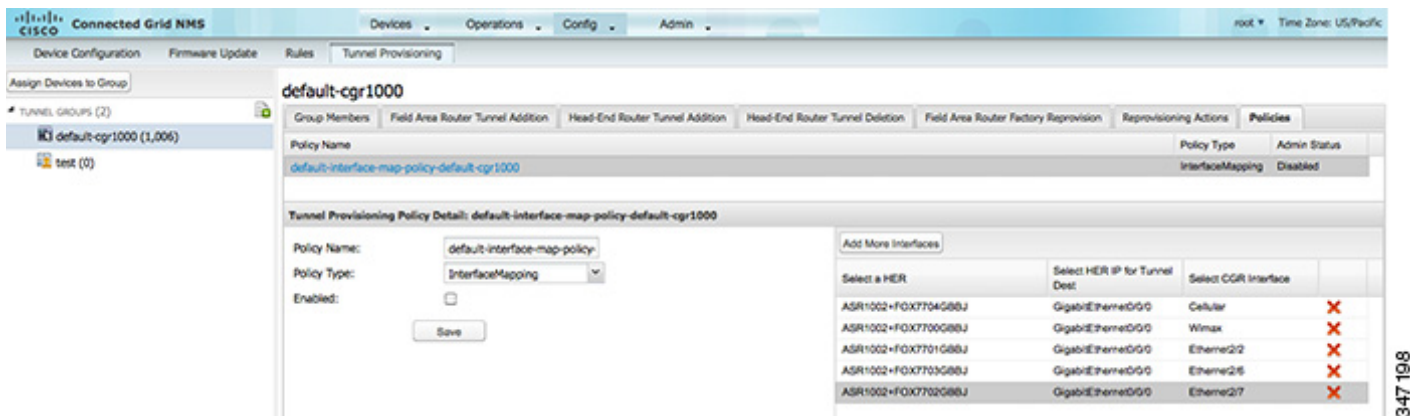
By default, CG-NMS displays the InterfaceMapping policy.

Note: InterfaceMapping is the only policy type currently supported in CG-NMS.

CG-NMS displays one interface mapping entry for every HER in the group. You can add or remove interface mapping entries as needed.

6. In the Policy Name field, enter the name of the policy.

7. To add an interface-mapping entry to the policy, click **Add More Interfaces**.

To delete an entry, click **Delete** (✖) for that entry.

8. To configure an interface-mapping entry, click the Policy Name link, and complete the following as necessary:

   a. To select a different HER, click the currently selected HER and choose a different one from the **Select a HER** drop-down menu.

   b. To select the HER IP for the tunnel destination on the HER, click the selected interface and choose a different one from the **Select HER IP** drop-down menu.

   c. To select the FAR interface that maps to the selected HER interface, choose an interface from the **Select CGR Interface** drop-down menu.

   d. Click **Update**.

9. To enable the policy, check the **Enabled** check box.

10. Click **Save**.

Modifying the Tunnel Provisioning Templates for Tunnel Redundancy

After defining the tunnel provisioning policy for a tunnel provisioning group, modify the Field Area Router Tunnel Addition and the Head-End Router Tunnel Addition templates to include commands to establish the multiple tunnels defined in the policy.

Field Area Router Tunnel Addition Template Example

In this example, bold text indicates the changes made to the default Field Area Router Tunnel Addition template to create multiple tunnels:

```
<#--
  Configure a Loopback0 interface for the FAR. This is done first as features
  look for this interface and use it as a source.

  This is independent of policies
-->
interface Loopback0
  <#--
    Now obtain an IPv4 address that can be used to for this FAR's Loopback
```

```
     interface. The template API provides methods for requesting a lease from
     a DHCP server. The IPv4 address method requires a DHCP client ID and a link
     address to send in the DHCP request. The 3rd parameter is optional and
     defaults to "CG-NMS". This value is sent in the DHCP user class option.
     The API also provides the method "dhcpClientId". This method takes a DHCPv6
     Identity association identifier (IAID) and a DHCP Unique  IDentifier (DUID)
     and generates a DHCPv4 client identifier as specified in RFC 4361. This
     provides some consistency in how network elements are identified by the
     DHCP server.
  -->
  ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32
  <#--
    Now obtain an IPv6 address that can be used to for this FAR's loopback
    interface. The method is similar to the one used for IPv4, except clients
    in DHCPv6 are directly identified by their DUID and IAID. IAIDs used for
    IPv4 are separate from IAIDs used for IPv6, so we can use zero for both
    requests.
  -->
  ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128
exit

<#-- Make certain the required features are enabled on the FAR. -->
feature crypto ike
feature ospf
feature ospfv3
feature tunnel
<#-- Features ike and tunnel must be enabled before ipsec. -->
feature crypto ipsec virtual-tunnel

<#--
  Toggle on/off the c1222r feature to be certain it uses the Loopback0
  interface as its source IP.
-->
no feature c1222r
feature c1222r

<#-- Configure Open Shortest Path First routing processes for IPv4 and IPv6. -->
router ospf 1
exit
router ospfv3 2
exit

<#--
  Now that OSPF has been configured complete the configuration of Loopback0.
-->
interface Loopback0
  ip router ospf 1 area ${far.ospfArea1!"1"}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
exit

<#-- Configure Internet Key Exchange for use by the IPsec tunnel(s). -->
crypto ike domain ipsec
  identity hostname
  policy 1
    <#-- Use RSA signatures for the authentication method. -->
    authentication rsa-sig
    <#-- Use the 1536-bit modular exponential group. -->
    group 5
  exit
exit
crypto ipsec transform-set IPSecTransformSet esp-aes 128 esp-sha1-hmac
crypto ipsec profile IPSecProfile
  set transform-set IPSecTransformSet
```

```
        exit

    <#--
      Define template variables to keep track of the next available IAID (IPv4)
      and the next available tunnel interface number. We used zero when leasing
      addresses for Loopback0, so start the IAID at one.
    -->
    <#assign iaId = 1>
    <#assign interfaceNumber = 0>

    <#--
      The same logic is needed for each of the IPsec tunnels, so a macro is used
      to avoid duplicating configuration. The first parameter is the prefix to
      use when looking for the WAN interface on the FAR to use for the source of
      the tunnel. The second parameter is the OSPF cost to assign to the tunnel.
    -->
    <#macro configureTunnel interfaceNamePrefix destinationInterface her tunnelIndex ospfCost>
      <#--
        If an interface exists on the FAR whose name starts with the given prefix
        and an IPv4 address as been assigned to that interface then the IPsec
        tunnel can be configured, otherwise no tunnel will be configured. The
        template API interfaces method will return all interfaces whose name
        starts with the given prefix.
      -->
      <#assign wanInterface = far.interfaces(interfaceNamePrefix)>
      <#-- Check if an interface was found and it has an IPv4 address. -->
      <#if (wanInterface[0].v4.addresses[0].address)??>
        <#--
          Determine the HER destination address to use when configuring the tunnel.
          If the optional property "ipsecTunnelDestAddr1" has been set on this FAR
          then use the value of that property. Otherwise look for that same property
          on the HER. If the property is not set on the FAR or the HER, then fallback
          to using an address on the HER GigabitEthernet0/0/0 interface.
        -->
        <#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

        <#if !(destinationAddress??)>
          ${provisioningFailed("Unable to determine the destination address for IPsec tunnels")}
        </#if>
        interface Tunnel${interfaceNumber}
          <#assign interfaceNumber = interfaceNumber + 1>
          description IPsec tunnel to ${her.eid}
          <#--
            For a tunnel interface two addresses in their own tiny subnet are
            needed. The template API provides an ipv4Subnet method for leasing an
            IPv4 from a DHCP server. The parameters match those of ipv4Address,
            with a fourth optional parameter that can be used to specify the
            prefix length of the subnet to request. If not specified the prefix
            length requested will default to 31, which provides the two addresses
            needed for a point to point link.

            NOTE: If the DHCP server being used does not support leasing an IPv4
            subnet, then this call will have to be changed to use the ipv4Address
            method and the DHCP server will have to be configured to respond
            appropriately to the request made here and the second request that
            will have to be made when configuring the HER side of the tunnel.
            That may require configuring the DHCP server with reserved addresses
            for the client identifiers used in the calls.
          -->
          <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
          <#assign iaId = iaId + 1>
          <#-- Use the second address in the subnet for this side of the tunnel. -->
          ip address ${lease.secondAddress}/${lease.prefixLength}
          ip ospf cost ${ospfCost}
          ip ospf mtu-ignore
```

```
        ip router ospf 1 area ${far.ospfArea1!"1"}
        tunnel destination ${destinationAddress}
        tunnel mode ipsec ipv4
        tunnel protection ipsec profile IPSecProfile
        tunnel source ${wanInterface[0].name}
        no shutdown
    exit
  </#if>
</#macro>


<#--
  Since we are doing policies for each tunnel here, the list of policies passed to this template can be
  iterated over to get the tunnel configuration viz interface mapping

  tunnelObject.ipSecTunnelDestInterface is the "interface on CGR"
  tunnelObject.ipSecTunnelSrcInterface is the "interface on HER"
  tunnelObject.her is the HER of interest
 -->

<#list far.tunnels("ipSec") as tunnelObject>
    <@configureTunnel tunnelObject.ipSecTunnelDestInterface tunnelObject.ipSecTunnelSrcInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>  <----- Loop through policies (aka Tunnels)
</#list>

<#--
  Make certain provisioning fails if we were unable to configure any IPsec
  tunnels. For example this could happen if the interface properties are
  set incorrectly.
-->
<#if iaId = 1>
  ${provisioningFailed("Did not find any WAN interfaces to use as the source for IPsec tunnels")}
</#if>

<#--
  Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
  center.
-->
<#macro configureGreTunnel destinationInterface her tunnelIndex>

<#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

<#if !(destinationAddress??)>
    ${provisioningFailed("Unable to determine the destination address for GRE tunnels")}
</#if>

interface Tunnel${interfaceNumber}
  <#assign interfaceNumber = interfaceNumber + 1>
  description GRE IPv6 tunnel to ${her.eid}
  <#--
    The ipv6Subnet method is similar to the ipv4Subnet method except instead
    of obtaining an IPv4 subnet it uses DHCPv6 prefix delegation to obtain an
    IPv6 prefix. The prefix length will default to 127, providing the two
    addresses needed for the point to point link. For the IAID, zero was used
    when requesting an IPv6 address for loopback0, so use one in this request.
  -->
  <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
  ipv6 address ${lease.secondAddress}/${lease.prefixLength}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
  ospfv3 mtu-ignore
  tunnel destination ${destinationAddress}
  tunnel mode gre ip
  tunnel source Loopback0
  no shutdown
```

```
    exit

</#macro>

<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
    <@configureGreTunnel greTunnelObj.greDestInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```

Head-End Router Tunnel Addition Template

In this example, bold text indicates the changes made to the default Head-End Router Tunnel Addition template to create multiple tunnels:

```
<#--
  Define template variables to keep track of the IAID (IPv4) that was used by
  the FAR template when configuring the other end of the tunnel. This template
  must use the same IAID in order to locate the same subnet that was leased by
  the FAR template so both endpoints are in the matching subnet.
-->
<#assign iaId = 1>

<#--
  The same logic is needed for each of the IPsec tunnels, so a macro is used.
-->
<#macro configureTunnel ipSecTunnelSrcInterface ipSecTunnelDestInterface her tunnelIndex ospfCost>
  <#--
    Only configure the HER tunnel end point if the FAR tunnel end point was
    configured. This must match the corresponding logic in the FAR tunnel
    template. The tunnel will not have been configured if the WAN interface
    does not exist on the FAR or does not have an address assigned to it.
  -->
  <#assign wanInterface = far.interfaces(ipSecTunnelDestInterface)>
  <#if (wanInterface[0].v4.addresses[0].address)??>
    <#-- Obtain the full interface name based on the prefix. -->
    <#assign interfaceName = wanInterface[0].name>
    <#--
      Locate a tunnel interface on the HER that is not in use. The template
      API provides an unusedInterfaceNumber method for this purpose. All of
      the parameters are optional. The first parameter is a name prefix
      identifying the type of interfaces, it defaults to "tunnel". The second
      parameter is a lower bound on the range the unused interface number must
      be in, it defaults to zero. The third parameter is the upper bound on
      the range, it defaults to max integer (signed). The method remembers
      the unused interface numbers it has returned while the template is
      being processed and excludes previously returned numbers. If no unused
      interface number meets the constraints an exception will be thrown.
    -->
    interface Tunnel${her.unusedInterfaceNumber()}
      description IPsec tunnel to ${far.eid}
      <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
      <#assign iaId = iaId + 1>
      ip address ${lease.firstAddress} ${lease.subnetMask}
      ip ospf cost ${ospfCost}
      ip ospf mtu-ignore
      tunnel destination ${wanInterface[0].v4.addresses[0].address}
      tunnel mode ipsec ipv4
      tunnel protection ipsec profile IPSecProfile
      tunnel source ${ipSecTunnelSrcInterface}
      no shutdown
    exit
    router ospf 1
      network ${lease.prefix} ${lease.wildcardMask} area ${far.ospfArea1!"1"}
```

```
      exit
   </#if>
</#macro>


<#list far.tunnels("ipSec") as tunnelObject>
        <@configureTunnel tunnelObject.ipSecTunnelSrcInterface tunnelObject.ipSecTunnelDestInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>
</#list>


<#--
   Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
   center.
-->
<#macro configureGreTunnel greSrcInterface her tunnelIndex>
interface Tunnel${her.unusedInterfaceNumber()}
   description GRE IPv6 tunnel to ${far.eid}
   <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
   ipv6 address ${lease.firstAddress}/${lease.prefixLength}
   ipv6 enable
   ipv6 ospf 2 area ${far.ospfV3Area1!"0"}
   ipv6 ospf mtu-ignore
   tunnel destination ${far.interfaces("Loopback0")[0].v4.addresses[0].address}
   tunnel mode gre ip
   tunnel source ${greSrcInterface}
exit
</#macro>


<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
        <@configureGreTunnel greTunnelObj.greSrcInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```

Configuring CG-NMS Installations for HA

Troubleshooting CG-NMS

This chapter describes how to troubleshoot common CG-NMS issues.

- Tunnel Provisioning DHCP Configuration Issues

- Mesh Endpoint Registration Issues

- Recovering an Expired Database Password

- Unlocking the CG-NMS Database Password

- CG-NMS Service Will Not Start

- Exception in the server.log File on the CG-NMS Server

- Resetting the root Password

- Second CG-NMS Server Not Forming a Cluster

- CG-NMS Service Restarts Automatically

- FAR Management Issues

- Mesh Endpoint Management Issues

Note: Always reference the release notes for your CG-NMS version.

Tunnel Provisioning DHCP Configuration Issues

If there is a problem allocating an address, CG-NMS logs a Tunnel Provisioning Failure event. The log entry includes details of the error.

To monitor the address allocation process:

- Check the CG-NMS server.log file to determine if CG-NMS is sending a DHCP request during tunnel provisioning.

- Check your DHCP server log file to determine if the DHCP request from CG-NMS reached the DHCP server.

If requests are not reaching the server:

- Ensure that the DHCP server address is correct on the **Provisioning Settings** page in CG-NMS (**Admin > System Management > Provisioning Settings**).

- Check for network problems between CG-NMS and the DHCP server.

If the DHCP server is receiving the request but not responding:

- View the DHCP server log file, and ensure that the DHCP server is configured to support requests from the link address included in the DHCP requests. The link address is defined in the tunnel provisioning template.

- Ensure that the DHCP server has not exhausted its address pool.

If the DHCP server is responding, but CG-NMS is not processing the response:

- Ensure that the lease time is infinite. Otherwise, CG-NMS will not process the response.

- View the DHCP server logs and CG-NMS server logs for other errors.

Mesh Endpoint Registration Issues

To determine why MEs register with CG-NMS, CG-NMS collects the registration reason code from the MEs and logs events and the code with other relevant information as printed key value pairs to help diagnose registration issues.

Here is an example of a logged event:

```
?Event logged: Event(id=0, eventTime=1335304407477, eventSeverity=0, eventSource=cgmesh,
eventMessage=Mesh node registered due to cold  boot: [lastReg: 0, lastRegReason: 1],
NetElement.id=10043, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null
```

Table 1 lists reason codes for ME registration and corresponding event:

Table 1   Mesh Endpoint Registration Reason Codes

Registration Reason Code	Code	Event Type Name	Severity	Message	Description
REASON_UNKNOWN	0	unknownRegReason	INFO	Mesh node registered for unknown reason.	
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	The message includes the new IP address of the ME.
REASON_ADMIN	2	manualReRegistration	INFO	Mesh node registered due to manual registration.	The endpoint received an NMSRedirectRequest without a URL field.
REASON_IP_CHANGE	3	rejoinedWithNewIP	INFO	Mesh node registered with new IP address.	The message includes the new IP address of the ME.
REASON_NMS_CHANGE	4	nmsAddrChange	INFO	Mesh node registered due to NMS address change.	The CG-NMS IP address changed OUTSIDE of an NMSRedirect (a new DHCPv6 option value was received).
REASON_NMS_REDIRECT	5	manualNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	Endpoint received an NMSRedirect request.
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	Endpoint received an error from CG-NMS.

In addition to generating events when MEs register with CG-NMS, CG-NMS also generates events after receiving a WPAN change TLV `WPANStatus`.

```
Event logged: Event(id=0, eventTime=1335304407974, eventSeverity=0, eventSource=cgmesh,
eventMessage=WPAN change due to migration to better PAN: [lastChanged: 0, astChangedReason: 4],
NetElement.id=10044, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

Table 2 lists reasons for ME WPAN changes and the corresponding event

Table 2   Reasons for Mesh Endpoint WPAN Changes

Registration Reason Code	Code	Event Name	Severity Type	Description
IEEE154_PAN_LEAVE_UNKNOWN	-1	unknownWPANChange	MAJOR	WPAN change for unknown reason.
IEEE154_PAN_LEAVE_INIT	0	meshInit	N/A	No event is generated for this code.
IEEE154_PAN_LEAVE_SYNC_TIMEOUT	1	meshConnectivityLost	MAJOR	WPAN change due to mesh connectivity loss.
IEEE154_PAN_LEAVE_GTK_TIMEOUT	2	meshLinkKeyTimeout	MAJOR	WPAN change due to mesh link key timeout.
IEEE154_PAN_LEAVE_NO_DEF_ROUTE	3	defaultRouteLost	MAJOR	WPAN change for no default route.
IEEE154_PAN_LEAVE_OPTIMIZE	4	migratedToBetterPAN	MAJOR	WPAN change due to migration to better PAN.

For these events, the message includes the time elapsed since the ME left the network to when it rejoined. CG-NMS displays the amount of time the ME was offline since the event was logged (for example, 4 hours 23 minutes ago).

Recovering an Expired Database Password

To recover from an expired password, run these commands:

```
su - oracle

sqlplus sys/cgmsDbaAccount@cgms as sysdba
  alter user cgms_dev identified by test;
  alter user cgms_dev identified by password;
  exit;
```

Unlocking the CG-NMS Database Password

If you enter an incorrect CG-NMS Database password multiple times, Oracle locks your user account. Unlock your password using the Oracle software, as shown in this example:

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
  alter user cgms_dev account unlock;
  exit;
```

CG-NMS Service Will Not Start

If the CG-NMS service does not start:

1. Validate connectivity to the database:

    a. Log in as root on the CG-NMS server.

    b. Enter the following at the command prompt:

    ```
    service cgms status
    ```

    c. Verify the database server IP address and that CG-NMS can connect to the database.

      ■ If the IP address is incorrect or if CG-NMS cannot access the database, run **setupCgms.sh** and enter the correct values.

    d. Run the **service cgms status** command and verify connectivity.

    e. Start CG-NMS.

2. Verify that the JRE version installed on the server is correct (see System Requirements).

3. Verify that database migration was performed successfully.

Exception in the server.log File on the CG-NMS Server

If the there is an exception in the server.log file indicating that CG-NMS could not open the cgms_keystore file, then the cgms_keystore password stored in the cgms.properties file on the CG-NMS server is incorrect.

The password for the cgms_keystore file is encrypted and stored in the /opt/cgms/server/cgms/conf/cgms.properties file.

To encrypt or decrypt the password, use the /opt/cgms/bin/**encryption_util.sh** script.

Verify or update the password in the cgms.properties file, and if an update is required, restart CG-NMS after modifying the password.

Resetting the root Password

If you forget the password of the CG-NMS root user account, reset the password by running the /opt/cgms/bin/**password_admin.sh** script.

Second CG-NMS Server Not Forming a Cluster

Typically, discovery of nodes in a CG-NMS cluster is automatic. As long as the CG-NMS servers are on the same subnet, they form a cluster.

If you install a CG-NMS server and it does not join the cluster:

1. Verify that your servers are on the same subnet, can ping each other, and share the same cluster name.

2. Check the status of all members by running the /opt/cgms/bin/print_cluster_view.sh script.

3. Modify the cluster name, as follows:

    a. Change the value of the HA_PARTITION_NAME parameter on all CG-NMS cluster nodes, and then restart them.

    b. Change the value of the UDP_MULTICAST_ADDR parameter (unique multicast address) to match on all nodes in the cluster.

    c. Change the value of the CLUSTER_BIND_ADDR parameter to the interface to which you want the NMS to bind.

4. Verify that all the cluster nodes are configured to use NTP (see Configuring NTP Service).

5. Check the /etc/hosts file and verify that the IP address is correctly mapped to the hostname of the local server.

CG-NMS Service Restarts Automatically

When the CG-NMS services are started, the watchdog script is invoked. The watchdog script checks the health of the CG-NMS services. If the watchdog script detects an anomaly, it logs the conditions in the /opt/cgms/server/cgms/log/cgms_watchdog.log file

The watchdog script tries three times to determine if the anomaly condition improved. If not, it restarts the CG-NMS services automatically, unless the database has become unreachable. If the database is not reachable, the watchdog stops the CG-NMS services. Check the log files, including server.log, to determine what is causing the restarts.

Manually disable the watchdog process by running the /opt/cgms/bin/deinstall_cgms_watchdog.sh script on the CG-NMS server as root.

FAR Management Issues

This section presents common issues with FAR management and possible resolutions.

Certificate Exception

If this exception appears in the server.log file stored on the CG-NMS server when a FAR attempts to register with CG-NMS, the cgms_keystore file does not contain the CA server certificates or the CA certificates that were imported into the cgms_keystore file are incorrect:

```
SSLException: Received fatal alert: unknown_ca
```

For information about how to import certificates into the cgms_keystore file, see Generating and Installing Certificates.

FAR Keeps Reloading and Does Not Switch to the Up State

When a FAR is continuously reloading every time it contacts CG-NMS, it could be because the configuration pushed to the FAR by CG-NMS is not being applied successfully.

Check the server.log file on the CG-NMS server for clues on the cause of the configuration push failure. Sometimes, typos in the in the Field Area Router Tunnel Addition template cause this failure (CG-NMS does not provide template validation).

Note: When a FAR registers with CG-NMS, CG-NMS queries the FAR with show commands. CG-NMS then configures the FAR based on the configuration commands in the Field Area Router Tunnel Addition template.

Other reasons for continuous reloads may be:

■ A bad WAN link that drops packets and does not allow the registration to complete.

■ Firewall issues. Ensure that the firewall allows traffic in both directions and that traffic to and from the correct ports is allowed to pass.

Incorrect FAR State in CG-NMS

In CG-NMS, a FAR might appear in a Down state even though you can ping and trace the route to it without a problem.

CG-NMS manages the FAR via the CGDM service running on the FAR. So even though the FAR is pingable and reachable, it is important to verify that the jetty server and call home features are enabled on the FAR:

```
'show run callhome' should have 'enable' in the config and 'sh jvm status'
```

Mesh Endpoint Management Issues

This section presents common issues with ME management and possible resolutions.

Mesh Endpoints Not Registering with CG-NMS

Verify that the MEs have joined the FAR and are pingable from CG-NMS over IPv6. If they are pingable, verify the following:

- The clock is in sync.

- The DHCP server used by the MEs is programmed with the correct CG-NMS IP address.

- The MEs are running an image compatible with the current version of CG-NMS.

- If HSM is used, HSM must be online and responding correctly.

Licensing Issues

This section presents common issues with license management and possible resolutions.

Device Import Failure

The importing of devices into CG-NMS is dependent on the number of allotted CG-NMS server licenses.

Verify that your CG-NMS server has the adequate license count available for the number and type of devices being imported into the CG-NMS database.

Only unique device EIDs are allowed in CG-NMS. Check that no one else imported this device EID in to CG-NMS or is currently trying to import the same device EID. Verify that no other user is simultaneously importing the same device into CG-NMS.

License File Upload Failure

An expired license file will cause an error. Check the license file validity and expiration date.