Introduction

This chapter provides an overview of the Cisco Connected Grid Device Manager (Device Manager) and includes the following sections:

Overview

This section includes the following topics:

- Application
- Tasks
- Certificates
- Role-based Access Control
- Work Authorization

Application

Cisco Connected Grid Device Manager (Device Manager) is a Windows-based application that field technicians can use to manage the Cisco 1000 Series Connected Grid Routers (CGR 1000) over WiFi or Ethernet.

Cisco Connected Grid Network Management System (Cisco CG-NMS) manages multiple CGR 1000 routers, whereas the Device Manager connects and manages a single CGR 1000 at a time.

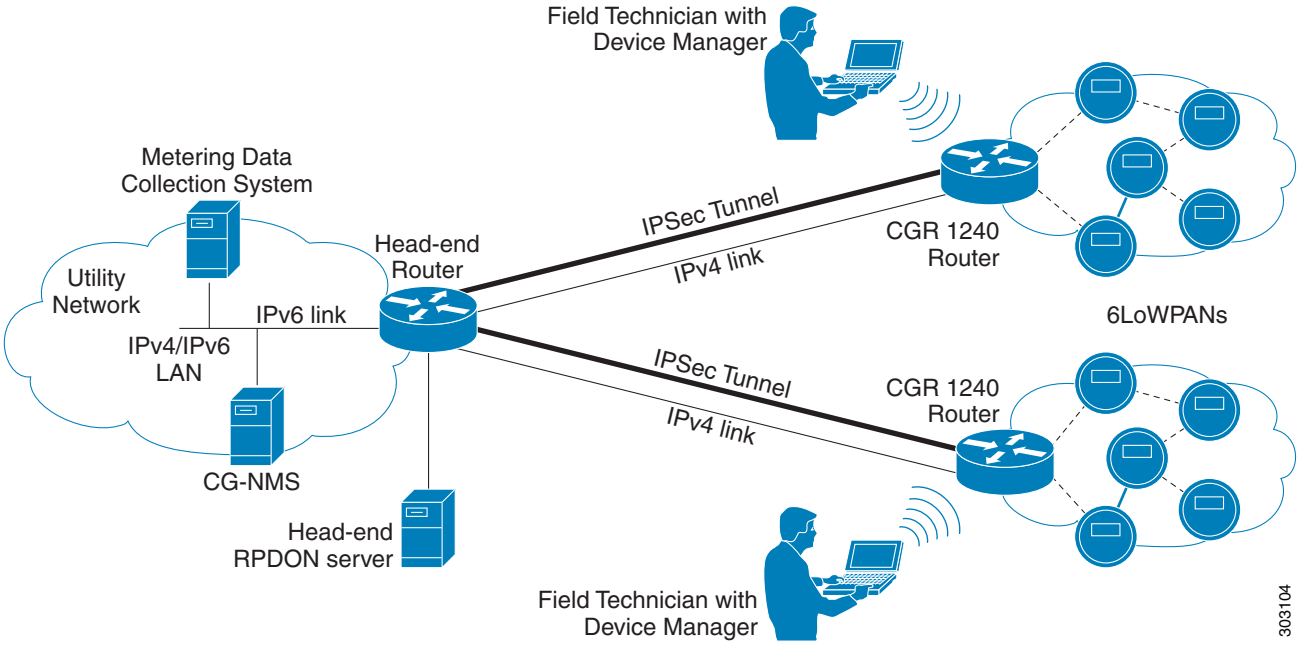
The Device Manager can operate in Connected Grid field deployments operating with or without CG-NMS.

- When operating with CG-NMS (NMS mode), a Device Manager user can retrieve Work Authorizations from the system as well as perform all supported tasks on the At a Glance page (see Figure 1-2) except as limited by the users assigned roles. (See Role-based Access Control.)
- When operating without CG-NMS (non-NMS mode), the Device Manager user does not have access to Work Authorizations; however, the user can perform all supported tasks on the At a Glance page except as limited by the user's assigned roles.

CGR 1000 routers are multi-service communications platforms designed for use in field area networks. The portfolio consists of two models–CGR 1240 and CGR 1120–both ruggedized to varying degrees for outdoor and indoor deployments. Both models are modular and support a wide-range of communications interfaces such as 2G/3G, Ethernet, and WiFi.

The Device Manager connects to the CGR 1000 by using a secure Ethernet or WiFi link. (See Figure 1-1.)

Figure 1-1 Device Manager Application Within a Connected Grid Network



Tasks

The Device Manager enables you to:

- Troubleshoot connectivity between a CGR 1000 and the devices connected to the router. (See Test Connectivity, page 3-12.)
- Bring up or shut down an CGR 1000 interface.

  (See Manage Interfaces, page 3-17.)
- Check and update the current CGR 1000 configuration.

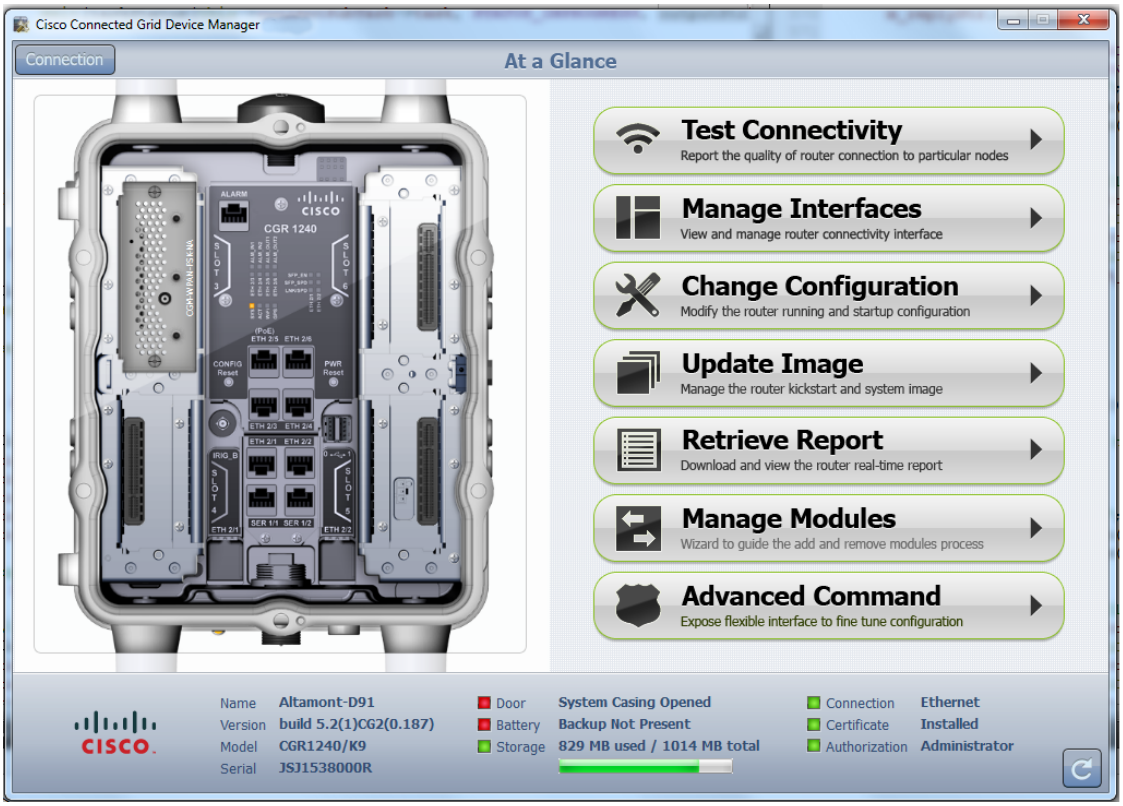
  (See Change Configuration, page 3-22 and Advanced Command, page 3-33.)
- Update the CGR 1000 image on the router.

  (See Update Image, page 3-25.)
- View real-time CGR 1000 configuration log for troubleshooting. (See Retrieve Report, page 3-27.)
- Add and Remove Modules from the CGR 1000 by employing a wizard that guides you through the process. (See Manage Modules, page 3-28.)
- Use advanced commands to troubleshoot the CGR 1000.

(See Advanced Command, page 3-33.)

You initiate all tasks from the At a Glance page. (See Figure 1-2.)

Figure 1-2 At a Glance Page for the CGR 1240



In addition to supported tasks (right side), the At a Glance page provides a view of the CGR 1000 router to which the Device Manager is connected (left side).

At the bottom of the page, you can find the following information:

- Name of the router
- Version of the software
- Model number of the CGR 1000
- Serial number of the CGR 1000
- Door status of the system casing, (Opened or Closed) for the router (CGR 1240 only)
- Battery status, when an optional backup battery is installed (CGR 1240 only)
- Slots within the system and modules installed in those slots (CGR 1120 only)
- Storage status, including amount of storage available
- Connection method of the Device Manager to the CGR 1000 (WiFi or Ethernet)
- Certificate status
- Authorization indicates the user role of the connected user

Tip To refresh the At a Glance page, click the **Refresh** icon (lower right side).

Certificates

You can import certificates through the Device Manager by employing the Setup wizard or by command line. The application launches the Setup wizard when either the user clicks the Setup icon or when the certificate is not detected. (See Import Certificates.)

Role-based Access Control

As a user, you are assigned roles that manage your access to operational and management functions of the Device Manager, which are summarized on the At a Glance page.

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

- When operating in non-NMS mode, the Device Manager supports four roles (admin, tech, viewer, and upload image). The assigned certificate extension Object ID (OID) manages roles and user access. Your administrator defines certificate extension OIDs for Device Manager roles on the Certificate Authority (CA) server.
  - Admin–User can perform all the supported tasks.
  - Technician–User can perform the following tasks: Test connectivity, manage interfaces, update image, retrieve reports, and manage modules.
  - Viewer–User can perform the following tasks: Test connectivity using predefined targets, view status of interfaces, and retrieve reports.
  - Upload Image–User can perform the following task: Upload an image to the CGR 1000.
- When operating in NMS mode, the Device Manager supports three roles (admin, tech, and viewer). The role that the CG-NMS administrator assigns to a Work Authorization manages user access.
  - Admin–User can perform all the supported tasks.
  - Technician–User can perform the following tasks: Test connectivity, manage interfaces, update image, retrieve reports, and manage modules.
  - Viewer–User can perform the following tasks: Test connectivity using predefined targets, view status of interfaces, and retrieve reports.

Note In NMS mode, user roles defined in CG-NMS take precedence over certificate-defined roles. For example, if you run Device Manager in non-NMS mode and then start Device Manager in NMS mode, the roles used in non-NMS mode are removed and the roles defined in CG-NMS take effect.

Work Authorization

The Work Authorization page is the opening page of the Device Manager when configured to operate in NMS mode. On this page, you can view and select work authorizations for CGR 1000 routers and synchronize with the Cisco CG-NMS to download work authorizations. The Device Manager only needs to be connected to CG-NMS to download and update the work authorizations.

At the CG-NMS, an admin assigns a user role for each of these work authorizations. (See Role-based Access Control.)

Tip You must enable Command Authorization on the CGR 1000 to support this functionality on the Device Manager. (See Enabling Feature on Router.)

Additional Information

You can find configuration guides and release notes for Cisco 1000 Series Connected Grid products at:

www.cisco.com/go/cgr1000-docs