



CHAPTER 1

Cisco netManager Overview

Cisco netManager is a data and IP communications network monitoring solution that provides monitoring of your network devices, services, or applications. You can use Cisco netManager to visualize, monitor, diagnose and report data status of your data and IP communications deployment.

Cisco netManager lets you initiate monitoring of devices in your network, and execute actions based on device state changes, so you can identify network failures before they become catastrophic.



Note

The ability to view and monitor IP communication devices depends upon the type of licensing you have.

The Cisco netManager HomeSpace workspace is the first screen you see after logging in to the web interface. For more information on your home workspace, see [“About Workspaces” section on page 15-1](#).

Device Management and Mapping

After installing Cisco netManager you can [import](#) device credentials using a seed file or [add](#) individual devices manually or as a map. The [device list](#) shows a summary of all monitored devices in your network and also allows you to perform various tasks using the [context menu](#). For more information, see [Chapter 5, “Managing Devices.”](#)

Topology Views

Cisco netManager provides two topological views of your network:

- Service Level View displays a logical topology view of IP communication devices in your network.
- Topology View displays a physical topology view of all the physical connections and devices in your network.

For more information, see [Chapter 17, “Using Topology Views.”](#)

Polling/Listening

Cisco netManager actively polls devices to determine their status. You can use preconfigured monitors, or create your own, to poll services on a device, and to passively listen for messages sent across the network. Monitors can also report on device performance by checking and reporting on device resources, such as disk, CPU, and interfaces. For more information on polling and monitors see the following:

- [Chapter 6, “Polling”](#)
- [Chapter 8, “Using Active Monitors”](#)
- [Chapter 9, “Using Passive Monitors”](#)

Actions

Depending on the responses received from polling, or the types of messages received, Cisco netManager initiates actions to notify you of any change on your network. Actions speed problem resolution through options such as alerting via email or pager, or restarting a service. For more information on actions see [Chapter 7, “Using Actions.”](#)

Reporting and Workspaces

Reports provide current status, performance, and historical data for devices and monitors. Workspaces let you focus on segments of the network and create your own *views* into the report data. They provide crucial network data in one location, which allows for quick and easy access. Cisco netManager offers over 100 instances of workspace content and reports. Each administrative user can have their own workspace with configurable workspace content. For more information on reports and workspaces, see the following:

- [Chapter 14, “Using Full Reports”](#)
- [Chapter 15, “Understanding Workspaces”](#)
- [Chapter 16, “Workspace Content”](#)

Cisco netManager Console and Web Interfaces

Cisco netManager offers two types of interfaces, the Windows console interface and the web interface, which offer largely the same functionality. We recommend that you do the initial set up — discovery and mapping — on the console, then use the web interface for additional setup of monitors and workspaces, users and permissions, and for day-to-day monitoring.

- Windows console interface

The Cisco netManager console is a Windows application, through which you can configure and manage the application and the database that drives it.

- Web interface

The web interface provides access to Cisco netManager functionality, through HTTP or HTTPS, from a web browser.

User Management

Administrators have read-write access privileges. Administrators can manage and configure users, devices, device groups, reports, and notifications. They can also acknowledge and clear events. Guest users, by default, have read-only privileges. These users can verify operational status using topology displays, search for phone and device information, view operational alerts on devices and phones in the network, view all reports (except system reports), and modify workspace views. Administrators can modify a guest user's access privileges.

There is another user profile called Cisco_User that cannot be modified or deleted. Cisco_User has read-only privileges and will always have default settings. Cisco_User has the same privileges as a guest user, with the following exceptions: Cisco_User cannot modify the layout of workspace views and they can view all reports (including system reports). Cisco_User becomes useful if a user or administrator has made modifications to his workspace view (for example, accidentally deleting a report) and wants to restore default settings. The administrator can view the default settings of Cisco_User and apply them to himself or to another user.

**Note**

Administrators can copy Cisco_User profile when creating new users.

The administrator can assign privileges to a user from the Manage Users dialog box.

- Step 1** Select **Go > Configure > Manage Users...**
- Step 2** Click **Add** to create a new user or **Edit** to modify an existing user.
- Step 3** Enter the name of the user in the User Name field.
- Step 4** Select the method of authenticating the user:
 - **Internal.** Use Cisco netManager's internal user database.
 - **LDAP.** Use an external LDAP database.
- Step 5** Enter the user's password (only if Authentication Type is set to Internal).
- Step 6** Enter the user's password again in the Confirm Password field.
- Step 7** From Home Group, select the device group that the user will see when they log into Cisco netManager's web interface. If they have the correct group access rights, they will be able to navigate out of this group.
- Step 8** From Device Group Settings, click Set Device Group Access Rights to make a change to which groups the user has read and write access to.

**Note**

This section is only visible after a user has been created. After initial creation, you are prompted to set device group permissions.

- Step 9** From User Rights, select which options to give the user access to:
 - **Manage Users**—Create and edit users for the web interface. This option also allows users to specify device group and device access rights.
 - **Manage IP Security**—Allows or refuses users access to the web interface to specific IP addresses.
 - **Configure Active Monitors**—Configure active monitors for devices in the database.
 - **Configure Passive Monitors**—Configure passive monitors for devices in the database.
 - **Manage Groups**—Create, edit, or remove device groups, in the groups in which the user has access.

- **Access Group and Device Reports**—View group and device reports for the groups to which the user has access.
 - **Access System Reports**—View system reports.
 - **Configure LDAP Credentials**—Configure LDAP credentials for the web interface.
 - **Configure Credentials**—Configure SNMP and Windows credentials.
 - **Change Your Password**—Change their own password.
 - **Configure Actions**—Create and edit actions in the Action Library.
 - **Manage Devices**—Add new devices and edit existing devices in the groups in which the user has access.
 - **Manage Web Server**—Change the configuration of the web server.
 - **Manage Recurring Actions**—Create, edit, or remove Recurring Actions, in the groups in which the user has access.
 - **Translations**—Translate Cisco netManager dialog boxes.
 - **Configure Workspaces**—Configure workspaces in the web interface.
 - **Configure Action Policies**—Create, edit, or remove Action Policies, in the groups in which the user has access.
 - **Configure Performance Monitors**—Configure performance monitors for devices in the database.
 - **Access Active Discovery Results**—Access active discovery results.
 - **Manage Workspace Views**—Access the Workspace Library and manage workspace views.
-