CHAPTER 13

Administrative Tasks

This section provides information about various administrative information and tasks.

About Web Security

Cisco netManager is installed with the files needed to immediately begin connecting to the SSL web server using 128 bit encryption.

The files included with the install (root.pem and server.pem) are installed with every copy of Cisco netManager, therefore, your encrypted session may not be as secure as it could be.

These certificate files are installed for demonstration purposes only, and should be replaced with certificates that you generate and sign.

Furthermore, a sample certificate is issued with Cisco as the Common Name. This will always give a Domain Name Mismatch Security Error on every fresh browser session in your environment.

These sample files reside in the Cisco netManager `Install Directory>\data\SSL` directory and should be updated with your own files.

Configuring IP Security

To allow or deny access to Cisco netManager based on IP addresses:

Step 1 Select **GO > Configure > IP Security**.

Step 2 Complete the following:

Allow Hosts—IP addresses and ranges listed in Allow Hosts are granted access to Cisco netManager.

- To add a new IP address or range of IP addresses to this list, click **New**.
- To change an existing entry, click **Edit**.
- To remove an entry, select the entry, then click **Delete**.

Deny Hosts—IP addresses and ranges listed in Deny Hosts are denied access to Cisco netManager.

- To add a new IP address or range of IP addresses to this list, click **New**.
- To edit an existing entry, click its hyperlink in the IP Address column.
- To remove an entry, select it, then click **Delete**.

Step 3 Click **OK**.

Note Addresses which are neither on the allow nor the deny list are allowed. Addresses which are on both lists are allowed.

Stopping and Starting the Web Server

For troubleshooting purposes, the first thing you may want to try is to restart the web server. This stops and restarts all Cisco netManager processes. To stop and restart the web server:

Step 1 Select **Start > Programs > Cisco netManager 1.0 > Daemons > Stop**. This stops the web server.

Step 2 Select **Start > Programs > Cisco netManager 1.0 > Daemons > Start**. This restarts the web server.

Configuring the Web Server

You can edit the SSL and web server ports, session timeout (amount of time after which a session ends for an inactive user).

Note If you are using IIS as your Web server, the Up Web Server options are disabled.

Step 1 Select **GO > Configure > Manage Web Server**.

Step 2 Edit the web server information.

Configuring the Web Interface to use IIS

Follow these steps to run the Cisco netManager web interface through an Internet Information Services (IIS) web server.

Step 1 Stop the following services and applications:

- Cisco netManager Engine service
- Cisco netManager Web service
- Task Tray application

Step 2 Allow MSDE to use SQL Server Authentication. Use Regedit.exe to set:

```
HKEY LOCAL MACHINE\Software\Microsoft\Microsoft SQL
Server\WHATSUP\MSSQLServer\LoginMode=0
```

Step 3 Restart the MSSQL$WHATSUP service.

Step 4 Specify a username and password for Cisco netManager to use when connecting to MSDE:

- **a.** Go to **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.
- **b.** Select the Cisco netManager DSN and click **Configure**. The Configuration wizard appears.
- **c.** Verify that the fields in the first dialog are correct and click **Next**.
- **d.** In the second dialog, verify that the With SQL Server authentication using login ID and password entered by the user option is selected. In this same dialog specify user=`sa` and password=`wug_sa` and click **Next**.
- **e.** In the third dialog, ensure that the first option is selected and Cisco netManager appears in the drop-down menu, and then click **Next**.
- **f.** Continue to click **Next** until you come to the final dialog, and then click **Finish**.

Step 5 Stop IIS.

Step 6 Create a virtual directory in IIS named NmConsole which points to <Cisco netManager install path>\HTML\NmConsole\. Go to Windows **Control Panel** > **Administrative Tools** > **Internet Information Services**. Right-click **Default Web Site** and choose **New > Virtual Directory**. We strongly recommend that you name this new directory NmConsole.

Step 7 Enable parent paths for the default web site (to support use of the relative paths used to navigate in the Cisco netManager web interface).

- **a.** Go to **Control Panel > Administrative Tools > Internet Information Services**.
- **b.** In the IIS Manager, expand Web sites, then right-click the newly created NmConsole virtual directory and choose **Properties**.
- **c.** On the Virtual Directory tab, click **Configuration**.
- **d.** On the Options tab, select **Enable parent paths**. Click **OK**.

Step 8 Set authentication for the virtual directory you set up in Step 6. To do this:

- **a.** In IIS Manager, right-click the virtual directory and select **Properties**, then select the **Directory Security** tab.
- **b.** In **Anonymous access and authentication control**, click **Edit**. Enable anonymous access and set the username and password to a local administrator. Click **OK**.

Step 9 For IIS version 6:

In IIS Manager, select Web Service Extensions and allow Active Server Pages.

Step 10 Restart IIS.

Step 11 Set the internal web server to port 8080, or disable it. If you disable the Cisco netManager web interface, ensure that the reports still load correctly.

Step 12 Restart the services and applications you stopped in Step 1.

Step 13 Connect to the web interface by opening a browser and entering the following address in the Address box: http://ip_address/NmConsole/

Note If you receive a scanning-device error, see Resolving IIS Scanning-Device Error, page 13-4.

Resolving IIS Scanning-Device Error

There is a known issue with IIS when adding a device through IIS. You may receive an "error scanning device" message. There are two methods of resolving this issue:

- The simplest is to set the virtual directory to run under low application protection (http://support.microsoft.com/?id=326086). Use this if Cisco netManager is the only application using IIS.
- If you have other sites/services running in IIS, you'll need to change the account used to launch the Cisco netManager processes. Follow these steps:

Step 1 Open the Component Services control panel (**Start > Run > dcomcnfg.exe**).

Step 2 Navigate to the COM+ Applications folder (**Component Services > Computers > My Computer**).

Step 3 Right-click **IIS Out-Of-Process Pooled Applications** and choose **Properties**.

Step 4 Select the **Identity** tab and change the user in the This user section to an account with administrator access.

Step 5 Restart IIS (be sure to restart the entire IIS suite, not just the web services).

Step 6 For IIS 6 you will also need to change the account used for the Application Pool that Cisco netManager is using in IIS.

Step 7 Open the IIS manager (**Start > Run > inetmgr**).

Step 8 Browse to Application Pools, then right click **DefaultAppPool** and select properties.

Step 9 Select the **Identity** tab, set the Application Pool Identity to Configurable, then enter an account with administrator access and click **OK**.

Step 10 Restart IIS (be sure to restart the entire IIS suite, not just the web services).

Configuring LDAP

Step 1 Select **GO > Configure > LDAP Credentials...**.

Step 2 Enter the following:

- **LDAP Server**—Enter the hostname or IP address of your LDAP server. If you are authenticating to an Active Directory domain, the LDAP server for your domain is a domain controller (DC).
- **LDAP Port**—Enter the number of the port your LDAP server monitors for queries. For most LDAP configurations, the default value of 389 will work.
- **Authorize DN**—Enter the path to the container which holds the users you want to use as Cisco netManager users. See Authorize DN examples, page 13-5.
- **Secure**—Select if you want LDAP queries to be encrypted using SSL. Your LDAP server must be configured to accept SSL connections for this option to work.
- **Test**—Select to bring up the Test dialog box. The Test dialog box allows you to verify that your LDAP credentials are se tup correctly.

Note To enable LDAP credentials to work, you must configure users for those users that you would like to grant access to. These users must match the LDAP credentials you have configured.

Authorize DN examples

- Active Directory
  - If you are using Active Directory, you can authenticate any user on the domain (after setting up a Cisco netManager user which matches the Active Directory login name for that Active Directory user) using the following format. As an example, for the domain CISCOMGR, you would use:

    CISCOMGR%s
  - If you're using Active Directory, but only want to allow users from a specific container to log in, use the following format. As an example, if your user, Bandy Wendy, is in the container, \OU=Sites\OU=KUL\OU=Non-Developers, on the bigbluepuddle.org domain, you would use:

    CN=%s,OU=Non- Developers,OU=KUL,OU=Sites,DC=bigbluepuddle,DC=org

    These DN strings use the Active Directory login name as the Cisco netManager username.
- Standard LDAP Server
  - If you're not using Active Directory, you will need to specify the LDAP attribute and path to the container which holds the user objects you want to use. An example could be;

    CN=%s,OU=Users,o=yourdomain.net

    where %s is username/password information entered from their respective fields.

Note If you are unsure which LDAP attribute to use, or which path to specify, contact your LDAP administrator or LDAP vendor.

Managing Users

Administrators have read-write access privileges. They 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 the same privileges as a guest user, except Cisco_User cannot modify the layout of workspace views, and they can view all reports (including system reports). Cisco_User becomes useful if users or administrators have made modifications to their workspace view (for example, accidentally deleting a report) and want to restore default settings. Administrators can view the default settings of Cisco_User and apply them to themselves or to other users.

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.

Changing Admin Preferences (Password Change)

To change your user account preferences:

Step 1 Select **GO > Configure > Preferences**.

Step 2 Enter the following:

General

- **Language**—Select a language for the application.
- **Change your password**—Click this option to change your account password.

Refresh Intervals

- **Workspace report**—Enter a time (in seconds) for how often workspace reports should refresh.
- **Full report**—Enter a time (in seconds) for how often reports should refresh.
- **Devices tab**—Enter a time (in seconds) for how often the Devices tab should refresh.

Web Alarms

- **Enable Web alarms**—Check this box to enable Web alarms.
- **Check every**—If you enable Web alarms, enter a time (in seconds) for how often Cisco netManager should check for Web alarms.
- Click **OK**.

Using the Cisco netManager Console

There are a few tasks that cannot be performed via the Cisco netManager web interface. For these tasks, you must use the console. The console is available from the server where Cisco netManager is installed (**Start > All Programs > Cisco netManager 1.1 > Cisco netManager 1.1 Discovery**).

Changing the Date and Time Format

To change the date and time format:

Step 1 From the Cisco netManager console, select **Configure > Program Options**.

Step 2 Select the **Regional** section.

For each of the three date formats, select the one that best suits your needs.

Step 3 Click **OK**.

These formats can be seen in use on several of the reports available on the Reports view.

Changing How Long Report Data Is Stored

Ping Active Monitor data is stored in the Cisco netManager database to populate the Performance reports available in the application.

Step 1 From the Cisco netManager console, select **Configure > Program Options**.

Step 2 In Program Options, select **Report Data**.

On the Report Data section, you can change the settings for raw data, hourly data, and daily data.

Step 3 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Changing the Device State Colors or Icons

To change the device state colors or icons:

Step 1 From the Cisco netManager console, select **Configure > Program Options**.

Step 2 In Program Options, select **Device States**.

To change an existing icon or state, select the entry from the list and click **Edit**.

Step 3 Adjust the shape and color of the icon using the settings in the Device State Editor.

Step 4 Click **OK** to save changes.

If the default settings do not fit your needs, click **Add** to create a new device state, using the internal state and state time that you need.

Changing Clock or Regional Preferences

To use a 24-hour clock instead of the default 12-hour clock:

Step 1 From the Cisco netManager console, select **Configure > Program Options**.

Step 2 Select the **Regional** section.

Step 3 Select the **Use 24 hour clock** option.

Step 4 Click **OK**.

Managing Notifications

Notification configuration options are available through the system registry. The registry location where these options can be set is at

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco netManager\1.1

Notifications run as a separate service, CiscoNotificationService.exe, and it relies on NmService.exe to sense the events that happen on the system.

Configuring SMTP Load

The notification engine uses a thread pool to send out e-mail notifications. The number of threads that talk to the e-mail servers at the same time is controlled so that the servers do not overload. You can increase the number of threads to increase the throughput of e-mails sent or you can decrease the number of threads to reduce the load at the e-mail server.

Step 1 From the server where Cisco netManager is installed, select **Start > Run**.

Step 2 Enter **regedit**. The Registry Editor window appears.

Step 3 Navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco netManager\1.1 folder.

Double-click **notification_max_threads** to modify the number of threads.This key must be of type REG_DWORD and must have a minimum of 1 and a maximum of 500. The default value is 32.

Note The maximum number of threads is created only if there is a need; for example, if a flurry of events occurs in the system and causes many e-mails to be sent. But if the number of concurrent operations is higher than the number that your e-mail server can support, the SMTP server could drop connections, causing you to lose e-mail. (Failed e-mail send operations are retried a maximum of three times. All errors and e-mails sent are logged.)

Performance and E-Mail Details

The default e-mail configuration supports 75 e-mails per second to be sent in situations of extreme activity. This figure can be affected by the actual SMTP server used, SMTP server responsiveness, and conditions on the network. If your server can take a greater load, the figures can be improved by increasing the number of concurrent threads that are active in the thread pool, as described in Configuring SMTP Load, page 13-9.

Note

- Some antivirus products automatically scan outgoing e-mail, which can affect performance. See the appropriate antivirus product documentation to disable this option.
- It is good practice to create e-mail aliases rather than configuring several e-mail addresses. This allows for better mail delivery performance and also makes it easier to create several notification rules that use the same e-mail addresses.
- If multiple SMTP servers are configured as part of multiple rules, the concurrency figures will likely be lower than what is supported.

Configuring Socket Timeouts

The default socket timeouts for connection, read, and write can be controlled using registry keys created in the same location. The timeouts are not kept too high by default to avoid issues due to erroneous configurations. However, timeouts can be increased to deal with a slow network. They keys that control the timeouts are the following:

- connection timeout—notification_socket_connect_timeout (default 30)
- read timeout—notification_socket_read_timeout (default 10)
- write timeout—notification_socket_write_timeout (default 5)

Note All keys must be of type REG_DWORD and have a maximum of 50 and a minimum of 1.

Notification Logging

The default log files are created in the <cnm install folder>\logs. E-mail notification logs contain records of all e-mails sent and errors encountered when sending e-mail. The default filename is NotificationEmailApp.log.

Events that need to be sent out along with changes in the system configuration (rules devices groups) are processed by the Notification engine. A record of this activity can be found in CiscoNotificationFrameWorkApp.log.

Note If the default log levels are changed in the log configuration for these files, the messages will cease to appear.