CHAPTER 18

Settings View

This section covers the basic principles for using the Settings view. Topics in this section include:

Defining Settings

The Settings interface includes the following tabs:

- Users—Enables you to add new Network Manager users, as well as modify and remove existing users.
- Alert Recipients—Enables you to add new alert recipients, as well as modify and remove existing alert recipients.
- Traps—Enables you to automatically update the elements to either enable or disable sending traps.
- Alarms—Enables you view and sort alarms generated by network elements. Allows you to customize alarm severity levels displayed per user profile, enable and disable alarms and create events for alarms to display in the Events table.
- Network Subsets—Enables you to define subsets of the network according to zones and element types used to outline Local user profile network access capabilities.
- Logs—Enables you to define the Network Manager log files and view the logs directory.

- Element Logs—Enables you to define the element log files.
- Element Access—Enables you to define the default access information for each element type.
- Endpoint Management—Enables you to configure the default communication port and access settings for common endpoint types recognized by the Network Manager.
- Auto-detect —Enables you to define when auto-detect should be performed to search the network for elements and add them to the Network Manager database.
- Cisco IOS H.323 Gatekeeper—Enables you to configure the Network Manager to open a communication port with the Cisco IOS H.323 Gatekeeper using the GKTMP TCP-based management protocol.

Defining Users

The Users tab enables you to create, modify or remove Network Manager user profiles, as well as define the access level for Network Manager user.

Topics in this section include:

About User Access

The Network Manager supports three types of network users:

- Administrator—Full read/write access to all managed elements and zones on the network.
- Read only—Read Only access to all elements and zones on the network.
- Local user—Restricted access to managed elements and zones on the network. This user profile is defined with specific read/write and read only access according to zones, elements and criteria for network subsets configured on the Network Subsets tab.

Adding Users

Click **New** to display the Add User window, which enables you to add new users and define user access rights. Add a new Network Manager user by typing a user name and password in the relevant fields and select the appropriate user access level.

Local users can also be configured with read/write access and read only access permissions according to zones and criteria for network subsets defined on the Network Subsets tab. You can also indicate whether a local user may freely add new elements to the Network Manager database throughout all network zones and subsets.

Modifying Users

Select a user from the displayed list and click **Edit** to display the Edit User window. Modify the fields, as required. For more information, see the "Adding Users" section on page 18-2.

Note To remove a user from the database, select the user from the list and then click **Delete**.

Defining Alert Recipients

The Alert Recipients tab enables you to create, modify or remove alert recipients. This includes defining the name and e-mail address of the recipient, the severity level of the alerts to be sent to alert recipients and the user access profile of the recipients.

You should note the following:

- Local users only receive notifications about the alerts on the network subsets for which the local user has been defined as a recipient.
- The alarm level for which you configure an alert recipient to receive notifications is based on the alarm level definitions defined by that user.

Note The Restriction column indicates the user profile of the alert recipient according to user access profile settings configured on the Users tab.

Topics in this section include:

Modifying Mail Server Settings

The mail server through which alert messages are sent by e-mail can be modified using the Resource Manager Configuration Tool.

Note To send email alerts outside of your mail domain to an external address, your mail server should be configured to allow mail relay. An alternative method is to forward the email from a local address to the desired external address.

Adding Alert Recipients

To add alert recipients, use the following procedure:

Procedure

Step 1 Click **Add.**

The Add Alert Recipient window appears, which enables you to add new alert recipients.

Step 2 Enter the name and e-mail of the alert recipient.

Step 3 Select a user profile (Administrator, Read only, Local user).

Step 4 Select the minimum severity level of the alerts to be sent (Warning, Minor, Major, Critical).

Step 5 To enable you to receive an error report via the e-mail, when the alarms have been cleared, click **Notify on alarms clearing**.

Step 6 Select whether to include a custom subject line in the e-mail and enter a string for the custom subject line.

You may also indicate whether to include in the custom subject line details of the elements reported in the alerts.

Step 7 Select **Enable alert** to activate the recipient.

Note In the Edit Alert Recipients window, when you configure the Minimum Severity tab to Critical (for example), you receive an e-mail notification for alarms that were configured only as critical by the user, that is selected in the User Profile field.
When you select a Local User (controls only the subset of the network) in the User Profile field, this alert recipient (i.e. the defined e-mail address) receives notifications only for alarms that belong to elements that are part of this network subset. If you select an Administrator or Read only user, then you receive notification on all the alarms.

Modifying Alert Recipients

Select an alert recipient from the displayed list and click **Edit** to display the Edit Alert Recipient window. Modify the fields, as required. For more information, see the "Adding Alert Recipients" section on page 18-3.

Note To remove an alert recipient from the database, select the recipient and then click **Delete**.

Defining Traps

The Traps tab enables you to define whether or not the Network Manager server receives SNMP traps such as alarms and events and allows you forward the traps to addresses specified in the trap forwarding rules. Check **Receive traps from elements** to configure the managed elements to send SNMP traps to the Network Manager.

The Traps tab displays the following information:

- Description
- IP Address
- Port
- Status

Adding a Trap Forwarding Rule

To add a trap forwarding rule, use the following procedure:

Procedure

Step 1 Click **Add.**

The Add Forwarding Recipient window appears, which enables you to define forwarding rules in which you specify an IP address and port number to which traps received from elements are forwarded.

Step 2 Click **OK** to add the new rule to the Network Manager database.

Note To modify and delete existing trap forwarding rules, use the Edit and Delete buttons.

Defining Alarms

The Alarms tab enables you view and sort alarms generated by the elements in the network according to alarm status, alarm message, date and time or element. The displayed severity level can be changed for each alarm according to the level defined by the current user, enable and disable alarms and create events for alarms to display on the Events tab.

The Alarms tab displays the following information:

- Alarm
- Severity
- Status
- Create Event

Modifying an Alarm

Select an alarm and click **Edit** to display the Edit Alarm Properties window which allows you to modify the alarm severity level assignment for each alarm, enable or disable the alarm and create an event which appears on the Events tab.

Defining Network Subsets

The Network Subsets tab enables you to define subsets of the network according to zones and element types using include and exclude criteria for use with Local user access level profiles.

Adding a Network Subset

To add a network subset, use the following procedure:

Procedure

Step 1 Click **Add**.

The Add Network Subset window appears for creating network subsets which are used to define areas of the network based on existing network zones and element types for use in Local user profiles.

The Add Network Subset window contains lists of include and exclude criteria for the network subset which contain details about the zone, child zone and element types specified in the criteria configuration.

For more information about specifying criteria, see the "Adding a Criteria" section on page 18-6.

Note A subset contains all elements which match at least one *Include* criterion but do not match any *Exclude* criterion.

For more information about user profiles, see the "About User Access" section on page 18-2.

Step 2 Click **OK** to add the new network subset.

Note To modify and delete existing network subsets, use the Edit and Delete buttons.

Adding a Criteria

To add a criteria, use the following procedure:

Procedure

Step 1 Click **Add** in the Include criteria or Exclude criteria areas of the Add Network Subset window.

The Add Criterion window appears for creating include or exclude criteria for network management access using the current network subset.

The Add Criterion window contains lists for selecting a network zone and element type and a check box to indicate whether child zones of the specified zone are contained in the criterion.

Step 2 To add the criterion to the relevant list in the Add Network Subset window, click **OK**.

Note To modify and delete existing criteria, use the Edit and Delete buttons.

Defining Logs

The Logs tab enables you to keep a log of operations performed in the Network Manager. The log file name, the maximum file size, the number of backup files to maintain and the level of detail can be defined to be included. In addition, to view the log directory, click the link.

Defining Element Logs

The Element Logs tab enables the Network Manager to locally save log files for those elements, such as MCU elements and gateways, that do not maintain a log of their own. The maximum size of each log file can be defined, as well as the number of backup files to maintain.

Defining Element Access

The Element Access tab enables you to define the default access definitions for each element type in the network. Default element access definitions are used by Network Manager to access elements which use standard settings in order to perform element monitoring and configuration.

Note The default element access settings on the Access tab for each element, can be overridden. For more information, see the "Configuring SNMP Access" section on page 14-8.

To define access rights, select the element type from the Element type list, and then define access information, including read and write communities, user name and the password (Telnet user name, password and password enable for Cisco IOS H.323 Gatekeeper), HTTP communication port and Telnet password. Click **Upload** to save the information to the Network Manager database.

Certain elements using parameters other than the default settings for the element type may be edited by selecting the element in the Network Tree view and modifying the element Access tab accordingly. For more information, see Chapter 14, "Network Tree View".

Note To view SNMP Community names, select **View SNMP Community names** in the View menu, when the option is already enabled using the Configuration Utility.

Managing an Element

This section includes information about managing an element.

Upgrading an Element

You can upgrade a network element such as an MCU or gateway that is displayed in the Network Tree view or Network Table view. To upgrade an element, use the following procedure:

Procedure

Step 1 Choose an MCU, EMP or Gateway element and then right-click on the element.

Step 2 Choose **Update > Upgrade Software**.

Step 3 Select a software version with which to upgrade the element.

About the Element Management Tab

On the Element Management tab you can define default access definitions for each element type in the network. The default access definitions are used by the Network Manager to access those elements that use standard settings, in order to perform element monitoring and configuration.

Note You can override the default access settings on the Access tab for each element.

The **Element Management** tab includes the following tabs:

- Access
- Software Upgrade Files
- Upload Log

Note To display the type of element to which you want to apply software upgrade files, configuration files or log files, choose an element type from the Show list. If the Access tab is selected, the Show list is disabled.

Using the Access Tab

On the Access tab, you define access rights for an element type.

Defining Access Rights

To define access rights for an element type, use the following procedure:

Procedure

Step 1 Choose an element type from the Element Type list.

Step 2 Define the access information for that element type, including SNMP read and write communities, user name, password, HTTP communication port, and Telnet password.

Step 3 For elements that use parameters other than the default element settings, you can edit these settings by selecting the element in the Network Tree view and then modifying the element on the Access tab. For more information, see Chapter 14, “Network Tree View”.

Step 4 Click **Upload** to save the information in the Network Manager database.

Note You can choose **View > View SNMP Community Names** to view SNMP Community names when the option is enabled using the Administrator Server Configuration.

Using the Software Upgrade Files Tab

On the Software Upgrade Files tab you can manage software upgrade files you receive from a third-party distributor. You can filter the contents of the Software Upgrade Files tab to display only suitable element types by selecting the element type from the Show list.

Adding a Software Upgrade File

To add a software upgrade file from a third-party distributor to the Network Manager database, use the following procedure:

Procedure

Step 1 Click **Add** to open the Add Software Upgrade File window.

Step 2 In the Software Upgrade File field, enter the full path of the software upgrade file you want to add to the Network Manager database, or click **Browse** and then select the file.

Step 3 In the Save As field, enter the name of the file to be saved in the Network Manager database.

Step 4 In the Description field, enter a description of the file.

Step 5 Click **Cancel** if you want to cancel the operation.

Step 6 Click **OK** to save the file in the Network Manager database. The file name appears on the Software Upgrade Files tab.

Editing a Software Upgrade File

Use the following procedure to edit the name and description of a software upgrade file:

Procedure

Step 1 Click **Edit**.

In the Edit Software Upgrade File Details window, the device type is displayed in the Unit Type field.

Step 2 In the File name field, enter the file name.

Step 3 In the Description field, enter a description of the file.

In the Uploaded By field, the user name of the user who added the file to the Network Manager database is displayed.

In the Uploaded On field, the time and date that the file was added to the Network Manager database is displayed.

Step 4 If you want to cancel the operation, click **Cancel**.

Step 5 Click **OK** to save the changes in the Network Manager database.

Deleting a Software Upgrade File

To delete a file from the Network Manager database, click **Delete**.

Using the Upload Log Tab

The Upload Log tab displays a history of all endpoint update attempts (software or configuration) and shows all scheduled uploads. The following fields appear on the tab:

- Upload Type—Displays the type of file: configuration or software upgrade.
- File—Displays the name of the configuration or software upgrade file.
- Target IP—Displays the target endpoint IP address.
- Time Submitted—Displays the time and date that the initial upload attempt began.
- Status—Displays one of the following statuses for the upload operation:
  - Pending—Before the first attempt.
  - In progress
  - Success
  - Fail
  - Next Retry—The time of the next attempt is displayed if the previous attempts failed.
  - Retries—x/y where x is the number of failed update/upgrade attempts that were previously performed and y is the total number of attempts that will be performed in the event of failure.

Click **Delete** to delete one or more selected log records.

Click **Delete All** to delete all the log records.

Click **Retry** to attempt to run an update.

Managing an Endpoint

The following section provides information about managing an endpoint.

Upgrading an Endpoint

You can upgrade an endpoint displayed in the Network Tree view or Network Table view. To upgrade an endpoint, use the following procedure:

Procedure

Step 1 Choose an endpoint and then right-click on the endpoint.

Step 2 Choose **Select Update > Upgrade Software**.

Step 3 Select an upgrade for the software version of the selected element.

Configuring an Endpoint

To configure an endpoint, use the following procedure:

Procedure

Step 1 Choose an endpoint and then right-click on the endpoint.

Step 2 Choose **Update > Retrieve Configuration file** or **Update Configuration** to open a window in which you can download a configuration file from an endpoint or upload a stored configuration file to the selected endpoint.

When you choose an endpoint from the Endpoint Type list that supports a software upgrade or an update configuration, the following sub-tabs are available:

- Access
- Software Upgrade Files
- Configuration Files
- Upload Log

Using the Access Tab

On the **Access** tab of the **Endpoint Management** tab, you can configure the default communication port and access settings for common endpoint types that are recognized by the Network Manager.

Note The default values configured on the Access tab might be overridden when configuring a single endpoint using the Endpoints tab in the Network Tree view. For more information, see the "Configuring an Endpoint" section on page 18-11.

Using the Software Upgrade Files Tab

The Software Upgrade Files tab enables management of software upgrade files received from a third-party distributor.

Adding a Software Upgrade File

To add a software upgrade file received from a third-party distributor to the Network Manager database, use the following procedure:

Procedure

Step 1 Click **Add** to add the software upgrade file that you received from a third-party distributor to the Network Manager database.

Step 2 In the Add Software Upgrade File window, enter the full path of the software upgrade file you want to add to the Network Manager database, or click **Browse** and then select the file.

Step 3 In the Save As field, enter the name of the file to be saved in the Network Manager database.

Step 4 In the Description field, enter a description of the file.

Step 5 Click **Cancel** if you want to cancel the operation.

Step 6 Click **OK** to save the file in the Network Manager database. The file name appears on the Software Upgrade Files tab.

Editing a Software Upgrade File

To edit the name and description of a software upgrade file, use the following procedure:

Procedure

Step 1 Choose the software upgrade files you require on the Software Upgrade Files tab and then click **Edit**.

In the Edit Software Upgrade File Details window, the name of the endpoint type is displayed in the Unit Type field.

Step 2 In the File name field, enter the file name.

Step 3 In the Description field, enter a description of the file.

In the Uploaded By field, the user name of the user who added the file to the Network Manager database is displayed.

In the Uploaded On field, the time and date that the file was added to the Network Manager database is displayed.

Step 4 Click **Cancel** if you want to cancel the operation.

Step 5 Click **OK** to save the file in the Network Manager database.

Deleting a Software Upgrade File

Choose a software upgrade file on the Software Upgrade Files tab, and then click **Delete** to remove the selected file from the Network Manager database.

Using the Configuration Files Tab

The Configuration Files tab displays configuration files previously retrieved from endpoints and saved in the Network Manager database. For more information on retrieving configuration information, see the "Retrieving Configuration Parameters" section on page 14-16.

Editing a Configuration File

To edit the name and description of a configuration file, use the following procedure:

Procedure

Step 1 On the Configuration Files tab, choose the required endpoint configuration files.

Step 2 To modify the name and description of the selected files, click **Edit**.

In the Edit Configuration File Details window, the endpoint type is displayed in the Unit Type field.

Step 3 In the File name field, enter the file name.

Step 4 In the Description field, enter a description of the file.

In the Retrieved by field, the name of the user who retrieved the file from the Network Manager database is displayed.

In the Retrieved from field, the IP address of the endpoint from which the configuration parameters were retrieved is displayed.

In the Retrieved on field, the time and date at which the file was retrieved is displayed.

Step 5 Click **Cancel** if you want to cancel the operation.

Step 6 Click OK to save the file in the Network Manager database.

Displaying the Upload Log

The Upload Log tab displays a history of endpoint update attempts that includes the following information:

- Upload Type—The type of upload operation: configuration or software upgrade.
- File—The name of the configuration or software upgrade file.
- Target IP—The target endpoint IP address.
- Time Submitted—The time and date at which the initial upload attempt began.

- Status—Displays one of the following statuses for the upload operation:
  - Pending—Before the first attempt.
  - In progress
  - Completed
  - Failed
  - Next Retry—The time of the next attempt (in case the previous attempt failed).
  - Retries—x/y where x is the number of failed update or upgrade attempts previously performed and y is the total number of attempts to be performed in case of failures.

Click **Delete** to delete the selected log records.

Click **Retry** to attempt to run the update.

Defining Auto-detect

The Auto-detect tab enables you to define policies for running the auto-detect mechanism to discover new elements.

The Auto-detect tab includes a check box that configures auto-detect to run automatically whenever the server is restarted. In addition, to run auto-detect at regular intervals, check **Run autodetect every (hrs)** and then selecting the time interval from the list.

The Auto-detect tab includes a check box to configure whether the Auto-detect routine uses the default element access information defined on the Element Access tab. Additional access settings can be defined for element types with access settings which are different from the default settings. Each of the additional element access settings can be enabled or disabled. This provides additional control for determining on which types of elements the auto-detect routine performs a search.

Caution Elements manually deleted from the Network Manager database are not detected when running subsequent auto-detect routines. Deleted elements must be manually added to the Network Manager database.

Topics in this section include:

- Adding Auto-detect Access Information, page 18-14
- Modifying Auto-detect Access Information, page 18-15

Adding Auto-detect Access Information

To add auto-detect access information, use the following procedure:

Procedure

Step 1 Click **Add**.

Step 2 Select the unit type in the list, enter a description and SNMP read community, SNMP write community, user name and password details.

The SNMP read community is the only mandatory field.

Step 3 To activate the access information setting, select **Enable**.

Caution The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

Note To view SNMP Community names, select **View SNMP Community Names** in the View menu, when the option is already enabled using the Configuration Utility.

Modifying Auto-detect Access Information

Select an auto-detect access information setting from the displayed list and click **Edit** to display the Edit Auto-detect Access Information window. Modify the fields, as required. For more information, see the "Adding Auto-detect Access Information" section on page 18-14.

Note To remove an Auto-detect access information setting from the database, select the access type and then click **Delete**.

Configuring a Cisco IOS H.323 Gatekeeper

The Cisco IOS H.323 Gatekeeper tab enables you to configure the Network Manager to get calls and registration information from the Cisco IOS H.323 Gatekeeper and allows you to modify the communication port number.

Note If the GKTMP port is not opened either by the Network Manager or the Cisco IOS H.323 Gatekeeper, information is updated less frequently.

You configure the Cisco IOS H.323 Gatekeeper by selecting **Automatically open port for Cisco IOS H.323 Gatekeeper GKTMP** to enable communication with the Network Manager via the Cisco IOS H.323 Gatekeeper GKTMP TCP-based management protocol. The default port is *20000* and automatically displays in the GKTMP port box which may also be set with an alternative value according to the settings on your Cisco IOS H.323 Gatekeeper.