CHAPTER 10

Managing Cisco ANA Security

About this chapter:

This chapter describes how Cisco ANA implements a two-dimensional security engine combining a role-based security mechanism with scopes (groups of Network Elements) that are granted to users. In addition, it describes managing users in the Cisco ANA platform, including, defining users and passwords.

Security Overview, describes the security related concepts and terms used in the Cisco ANA Manage application and throughout this guide.

Customizing Security Flow, describes the steps required to customize security.

Creating Scopes, describes how to group a collection of managed Network Elements together in Cisco ANA Manage. In addition, it describes how to edit the Network Elements included in a scope, view the scope's properties and how to delete a scope.

Creating New Cisco ANA User Accounts, describes how to create permitted users for the current client station.

Granting or Editing a User's Rights, describes how to manage general user account information and the list of scopes assigned to the user as well as the security access roles per scope and assign maps to a user.

Deleting a Cisco ANA User Account, describes how to delete a Cisco ANA user account from the list of users.

Changing a User's Password, describes how the administrator can redefine the user's password. In addition, it describes how the current user can change the user password.

Security Overview

This section describes the security related concepts and terms used in the Cisco ANA Manage application and throughout this guide.

Scopes

Cisco ANA Manage enables the administrator to group a collection of managed Network Elements together in order to enable the user to view and/or manage the NEs based on the user's role or permission.

After the user is allocated a scope (list of Network Elements) and a role, the user can then perform various activities on the Network Elements included in the scope, as follows:

- Activate services.
- Manage alarms in Cisco NetworkVision.
- Manipulate graphical Network Elements in the map.
- View Network Element, inventory, and link properties.
- Add Network Elements to the map view.
- Manipulate business tags per Network Element.
- Manage advanced options, for example, show counters, show utilization, and refresh.

By default Cisco ANA includes a pre-configured scope for the administrator's convenience, which cannot be edited or deleted, namely, **All Managed Elements**. This default scope includes all of the managed Network Elements. A user granted the All Managed Elements scope can view and manage all the Network Elements all the time according to the user's role assigned to the scope.

Default Permissions

The Role or default permission only applies to the activities that are related to GUI functionality, not the activities related to Network Elements, including:

- Application login.
- Manage alarms in Cisco NetworkVision.
- Manage maps—Creating, deleting, and opening.
- Map manipulation—Arrange map, including, aggregations, adding NEs, NEs placement in map, map background and so on.
- Business tag management.

Security Access Roles

Cisco ANA provides five pre-defined security access roles that can be granted to a user in order to enable system functions:

- **Administrator—**Manage the system configuration, and security. Cisco ANA Manage supports multiple administrators.
- **Configurator—**Activate services, and configure the network.
- **Operator Plus—**Manage the alarm life cycle.
- **Operator—**Configure business tags and manage most day-to-day operations.
- **Viewer—**View only access to the network and to non-privileged system functions.

Note Roles can be granted per scope or at an application level (namely, all the activities that are related to GUI functionality, not the activities related to devices). Users can have different roles for different scopes. Role functionality is incremental.

The table below illustrates the functionality per role according to the default permission and Scope based functionality:

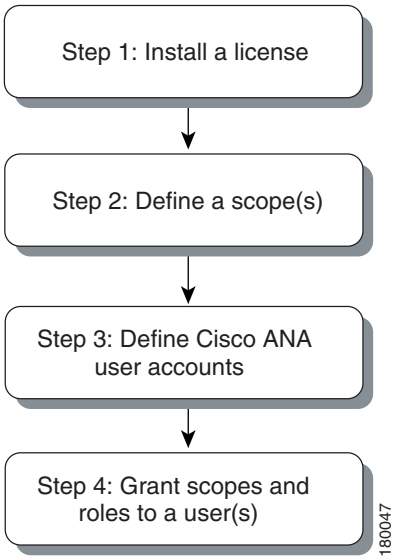
Role	Default Permission Based Functionality	Scope Based Functionality
 Administrator	Platform management: • Manage Cisco ANA Servers, AVMs, transport and VNEs • Global setting—Managing polling groups, protection groups, client licenses and service disclaimers • View DB segments • Create/delete scopes • Manage user accounts • Manage static topology links • Manage VNEs from Cisco ANA Manage or Cisco NetworkVision Map management: • Open, edit, delete all user maps	
 Configurator	Map management: • Create maps Advanced tools: • Ping and Telnet a NE directly from the client • Enable/disable port alarms • Cisco ANA Command Builder	Activation services: • Allow activation commands per managed NE
 OperatorPlus	Map management: • Create new maps and add NEs • Edit/delete/rename maps • Save maps Map manipulation: • Create/break aggregations • Change map layout • Set background image • Create business links	Alarm management: • Acknowledge, remove, and clear alarms that belong to the NEs within a user's scope that have the OperatorPlus role Map manipulation: • Create business tags for NEs Display network information: • Display path tool traffic, rates, drops or any dynamic data

Role	Default Permission Based Functionality	Scope Based Functionality
Operator	Map manipulation: • Create/delete business tags Application: • Open EventVision	Display network information: • Refresh port information from NE
Viewer	Application: • Login to NetworkVision, EventVision • Change user password • View the Device List • View map • View link properties • Use table filter • Export from any table	Display network and business tag information: • View alarm list, alarm properties, and find alarms • Find and view attachments • View NE properties and inventory • Calculate and view affected parties • Open port utilization graph

Customizing Security Flow

The flow below describes the steps required to customize security using Cisco ANA Manage and the order in which they must be performed.

Figure 10-1 Customizing Security Flow



Step 1—Install a license—Enables the administrator to control and monitor the number of Cisco ANA Client and BQL connections over a limited or unlimited period of time based on the client licenses installed. For more information, see the Managing Client Licenses section.

Step 2—Define a scope—Enables the administrator to group a collection of managed Network Elements together in order to enable the user to view and/or manage the Network Elements based on the user's role. For more information, see the Creating Scopes section.

Step 3—Define Cisco ANA user accounts—Enables the administrator to define and manage user accounts. For more information, see the Creating New Cisco ANA User Accounts section.

Step 4—Grant scopes and roles to a user—Enables the administrator to manage general user account information and the list of scopes assigned to the user as well as the security access roles per scope. For more information, see the Granting or Editing a User's Rights section.

Creating Scopes

Cisco ANA Manage enables the administrator to group a collection of managed Network Elements together in order to enable the user to view and/or manage the Network Elements based on the user's role or permission.

Once a scope is created it can be assigned to a user. Multiple scopes can be assigned to a single user and a single scope can be assigned to multiple users. When the scope is assigned to a user, the administrator is required to provide the user with security access roles as well, namely, to define the user's role within the assigned scope. For more information, see the Granting or Editing a User's Rights section.

To create a scope:

Step 1 Select the *Scopes* branch in the Cisco ANA Manage window. The *Scopes* branch is displayed.

Step 2 Right-click to display the menu and select **New Scope** or from *File* menu select **New Scope** or in the toolbar click **New Scope**. The New Scope dialog box is displayed.

- The following fields are displayed in the New Scope dialog box:
- **Scope—**The name of the scope (unique).
- **Available Devices—**A list of all of the available devices.
- **Active Devices—**A list of all of the active devices defined for the scope.

The following buttons are displayed in the New Scope dialog box:

	Add All—Adds all available devices to the **Active Devices** list.
	Add Selected—Adds the active device to the **Active Devices** list.
	Remove Selected—Removes an active device from the scope.
	Remove All—Removes all active devices from the scope.

Step 3 Enter a name for the scope in the **Scope** field.

Step 4 Select a device/s from the list of **Available Devices** and click **Add Selected** to add the device/s to the list of **Active Devices** in the scope.

Note Multiple rows can be selected using the standard Microsoft® Windows selection keys.

Step 5 Click **OK**. The scope is saved and is displayed in the *Workspace*.

Editing a Scope and Viewing a Scope Properties

Cisco ANA Manage enables the administrator to edit the details of a scope and to view the scope's properties.

To edit a scope or view scope properties:

Step 1 Select the *Scopes* branch in the Cisco ANA Manage window's *Tree* pane. The *Scopes* table is displayed in the *Workspace*.

Step 2 Select the scope that you want to edit or view in the *Workspace*.

Step 3 Right-click the required scope to display the shortcut menu, and select **Properties**, or from *File* menu select **Properties** or in the toolbar, click **Properties**. The Properties dialog box is displayed.

For more information about the Properties dialog box, see the Creating Scopes section.

Step 4 Edit and/or view the properties as required.

Step 5 Click **OK**. The Properties dialog box is closed.

Deleting Scopes

A device scope (lists of devices or Network Element groups) can also be deleted.

Note When a scope is deleted, it is deleted from all users who have the assigned scope.

To delete a scope:

Step 1 Select the *Scopes* branch in the Cisco ANA Manage window's *Tree* pane. The *Scopes* table is displayed in the *Workspace*.

Step 2 Select the scope that you want to delete in the *Workspace*.

Note Multiple rows can be selected using the standard Microsoft® Windows selection keys.

Step 3 Right-click the required scope to display the shortcut menu, and select **Delete**. The scope is deleted and is not displayed in the *Workspace*.

Creating New Cisco ANA User Accounts

The *Users* branch enables the administrator to define and manage user accounts. This includes, managing general user information as well as security access rights, and forced login changes, as required. The administrator can also monitor the user's last login time.

Note Creating a new user using the New User dialog box, is only part of the "creating-user" process. Granting user security rights to operate Cisco ANA applications are defined in the User Properties dialog box. For more information, see the Granting or Editing a User's Rights section.

The new user is created with a set of pre-defined system defaults, as follows:

- No scopes are assigned to the user
- The number of connections is unlimited
- The password must be changed every 30 days

Note Cisco NetworkVision has the following pre-configured password defaults—
The maximum length of the user name and full name is 20 characters.
The minimum length of the user password is 8 characters.
The maximum length of the password is 20 characters.
The minimum number of digits that must be included in the user password is 1.
The user name cannot contain any special characters like * # ? and so on.
The password cannot contain the User Name or vice versa.

To define a user account:

Step 1 Select the *Users* branch in the Cisco ANA Manage window. The *Users* branch is displayed.

Step 2 Right-click to display the menu and select **New User** or from *File* menu select **New User** or in the toolbar click **New User**. The New User dialog box is displayed.

Note Clicking **Show Password Rules** displays the current password rules.

The following fields are displayed in the New User dialog box:

- **User Name—**The new user's name used for logging in (mandatory).

  Note The user name is unique and a maximum of 20 characters may be used. Special characters may not be used.

- **Full Name—**The full name of the user (optional).

  Note A maximum of 20 characters may be used, but no special characters may be used.

- **Description—**A free text description of the user (optional).

- **Password—**Enter the new password (mandatory).

Note A minimum of 8 characters must be used, including, at least 1 digit. The maximum length of the user password is 20 characters.

- **Confirm Password—**Enter the new password again to confirm the new password (mandatory).

The **Role** dropdown list enables the administrator to define the security access role (permission) for the new user.

Note The permission only applies to activities or actions that are not related to a NE (Network Element). For more information on the functionality that a user can perform, see the Security Access Roles section.

When a new user is defined as an **Administrator** this user can perform all administrative actions, including opening all maps, working with all scopes and managing the system using Cisco ANA Manage. All of this is performed with the highest privileges. Cisco ANA Manage supports multiple administrators. Access rights do not need to be defined for an administrative user. For more information, see the Security Access Roles section.

The **Force Password Change at Next Login** checkbox is selected by default and forces the user to change the user password at next login.

The following button is displayed in the New User dialog box:

- **Create—**Adds the new user to the list of Cisco ANA Client users and the new user name is displayed in the *Workspace*.

Step 3 Enter a unique **User Name** (mandatory).

Step 4 Enter a **Full Name** and **Description** (optional).

Step 5 Enter a **Password** (mandatory).

Step 6 Enter the password again in the **Confirm Password** field (mandatory).

Step 7 Select a security access role for the new user from the **Role** dropdown list.

Step 8 Click **Create**. The new user name and default security access role are displayed in the *Workspace*.

Granting or Editing a User's Rights

Once the administrator has defined the scopes and the new user accounts, Cisco ANA Manage enables the administrator to manage or edit general user account information and the list of scopes assigned to the user, the security access roles per scope, and assign maps to a user.

Note A user may have different security access roles for different scopes, and maps.

In addition, the administrator can view the properties of a user.

General User's Rights

Cisco ANA Manage enables the administrator to manage or edit general user account information. In addition, the administrator can view the properties of a user.

To grant or edit a user's rights:

Step 1 Select the *Users* branch in the Cisco ANA Manage window's *Tree* pane. The *Cisco ANA Users* table is displayed in the *Workspace*.

Step 2 Right-click the required user to display the shortcut menu.

Step 3 From the shortcut menu, select **Properties**. The Properties dialog box is displayed with the *General* tab selected by default.

The **General** tab contains general user account information and the following fields are displayed:

- **User Name—**The current user's name. The user name cannot be modified.
- **Last Login**—The date and time that the user last logged in.
- **Full Name—**The full user name.
- **Description—**A description of the user.

The following checkboxes are displayed in the **General** tab of the Properties dialog box:

- **Enable Account—**Select this option to enable the user account or uncheck to disable the user account. The user account is automatically locked when the number of logins defined is exceeded (the **Limit Connections to** option is selected). An administrator can manually lock or unlock a user's account at any time. A user whose account is locked cannot login to the system.
- **Limit Connections to—**The number of instances of the Cisco ANA Client applications that the user can access at any one time. For example, if the number of connections is limited to 10, the user can have 5 instances of Cisco ANA Manage and 5 instances of Cisco NetworkVision open at the same time. If the user then tries to open an instance of Cisco EventVision the user will be unable to do so.
- **Force Password Change After—**The number of days after which a user is forced to change their password.
- **Force Password Change at Next Login—**Select this option to force the user to change the user password at next login. The administrator can define this option at any time.

Step 4 Edit the general properties as required.

User's Security Rights

To define a User's default security rights, you use the *Security* tab in the User Properties dialog box.

To edit a user's default security rights:

Step 1 Select the *Users* branch in the Cisco ANA Manage window's *Tree* pane. The *Cisco ANA Users* table is displayed in the *Workspace*.

Step 2 Right-click the required user to display the shortcut menu, and select **Properties**. The User Properties dialog box is displayed.

Step 3 Select the **Security** tab. The **Security** tab is displayed.

The **Security** tab controls the user's capability to view and manage the application, and Network Elements by granting the user scopes and security access roles. By default a new user is assigned a Viewer security access role. The following columns are displayed in the table in the **Security** tab of the Properties dialog box—

- **Scope Name—**The name of the scope.
- **Security Level—**The security access role defined for the scope. For more information about security access roles, see the Security Access Roles section.

The following buttons are displayed in the Properties dialog box when the **Security** tab is selected:

- **Add—**Adds the new scope.
- **Remove—**Deletes the selected scope from the user's active rights.
- **Edit—**Edits the selected permission of the user.

Step 4 Click **Add** to add the scope to the **Active Rights** of the user. The Security Level dialog box is displayed.

The following area is displayed in the Security Level dialog box:

- **Available Scopes—**Lists all of the predefined and unassigned scopes.

The following dropdown list is displayed in the Security Level dialog box:

- **Security Level**—Displays the security access roles for the defined scopes. For more information about security access roles, see the Security Access Roles section.

Step 5 Select a scope from the **Available Scopes** list.

Step 6 Select the required security access role from the **Security Level** dropdown list.

Step 7 Click **OK**. The scope is added to the list of **Active Rights** in the **Security** tab of the User Properties dialog box.

Step 8 Click **Apply/OK**. The Properties dialog box is closed.

Map User Permissions

Cisco ANA Manage enables the administrator to assign a map(s) to the user. When the user logs in to Cisco NetworkVision, the user can only open and manage the map(s) assigned to the user by the administrator.

To assign maps to a user:

Step 1 Select the *Users* branch in the Cisco ANA Manage window's *Tree* pane. The *Cisco ANA Users* table is displayed in the *Workspace*.

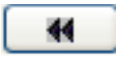
Step 2 Right-click the required user to display the shortcut menu, and select **Properties**. The User Properties dialog box is displayed.

Step 3 Select the **Maps** tab. The **Maps** tab is displayed.

The **Maps** tab is divided into two parts:

- The left hand side displays a list of all of the available maps in the database that have not been assigned to the user.
- The right hand side displays all the maps that have been assigned to the user, and which the user can open and manage in Cisco NetworkVision.

The following buttons are displayed between the available maps and assigned maps lists in the **Map** tab:

	Moves the selected map to the **Assigned Maps** list.
	Move the entire available map list to the **Assigned Maps** list.
	Removes a selected map from the assigned map list to the **Available Map** list.
	Removes the entire assigned map list to the **Available Map** list.

Step 4 Select a map/s from the list of **Available Maps** and click on the required button (as described above) to add the map to the list of **Assigned Maps** to the user.

Note Multiple rows can be selected using the standard Microsoft® Windows selection keys.

Step 5 Select and move maps between the two lists, as required, using the appropriate buttons.

Step 6 Click **OK** to confirm the user's assigned map(s).

Deleting a Cisco ANA User Account

An administrator can also delete a Cisco ANA user account.

To delete a user account:

Step 1 Select the *Users* branch in the Cisco ANA Manage window's *Tree* pane. The *Users* table is displayed in the *Workspace*.

Step 2 Select the user that you want to delete in the *Workspace*.

Note Multiple rows can be selected using the standard Microsoft® Windows selection keys.

Step 3 Right-click the required user to display the shortcut menu and select **Delete**. The selected user is deleted and is not displayed in the *Workspace*.

Changing a User's Password

Cisco ANA Manage enables the administrator to change the user's password at any time. When this happens the user is usually forced to change the password at the next login.

In addition, the current user can also initiate a change of password, where the user will be required to enter the old password in order to validate the new password.

To change a user's password (administrator):

Step 1 Select the *Users* branch in the Cisco ANA Manage window's *Tree* pane. The *Users* table is displayed in the *Workspace*.

Step 2 Select the user in the *Workspace* whose password you want to change.

Step 3 Right-click the required user to display the shortcut menu and select **Change Password**. The Change Password dialog box is displayed.

Note Clicking **Set Password Rules** displays the password rules.

Step 4 Enter the new password in the **Password** and **Confirm Password** fields.

Step 5 Click **OK**. A confirmation message is displayed.

Step 6 Click **OK**. The Change Password dialog box is closed.

Cisco ANA Manage enables the current user to also initiate a change of password.

To change the current user's password:

Step 1 From the *Tools* menu select **Change User Password**. The Change User Password dialog box is displayed.

Note Clicking **Set Password Rules** displays the password rules.

Step 2 Enter the old password in the **Old Password** field.

Step 3 Enter the new password in the **New Password** and **Confirm Password** fields.

Step 4 Click **OK**. A confirmation message is displayed.

Step 5 Click **OK**. The Change User Password dialog box is closed.