CHAPTER 7

Managing User Security: Roles and Scopes

These topics describe how Prime Network 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 Prime Network platform, including defining users and passwords.

Overview of User Authentication and Authorization

Note User authentication by Prime Network is disabled if Prime Network is installed with Cisco Prime Central.

Prime Network uses a combination of methods to manage user authentication and authorization:

- *User authentication* can be managed locally by Prime Network or externally by an LDAP application. Either method can be used to validate user accounts and passwords, thus controlling who can log in to Prime Network. If you use Prime Network, user information and passwords are stored in the Prime Network database. If you use an external LDAP application, passwords are stored on the external LDAP server. See External Authentication, page 7-2.
- *User authorization* is managed through a combination of *user access roles* and *scopes*:
  - User access roles control the actions a user can perform in the Prime Network GUI clients. When a user's account is created, the user is assigned an access role that determines the user's *default permissions*. For more information, see Prime Network User Roles, page 7-2.
  - Scopes are groups of network elements that are created by administrators. Once a scope is created, you can assign it to users. A user's default permissions determine the actions the user can perform on the network elements in the scope. These actions are referred to as the user's *security level* on that scope. If desired, you can assign the user a more strict user access role for a scope. For more information, see Device Scopes, page 7-3.

Prime Network determines whether a user is authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect devices), authorization is based on the default permission that is assigned to the user's account.
- For device-based tasks (tasks that do affect devices), authorization is based on the device scope assigned to the user's account—that is, whether the device is in the user's assigned scopes and whether the user meets the minimum security level for that scope.

User authorization information (roles and scopes) is always stored in the Prime Network database. The external LDAP server, if used, only stores passwords.

External Authentication

External authentication means that user authentication and passwords are validated by an external application, rather than by Prime Network. When Prime Network performs the authentication, Prime Network validates users by checking information that is saved in the Prime Network database. If you use an LDAP application, the information is validated by the external LDAP server.

If Prime Network is using external authentication and cannot communicate with the LDAP server, the only user permitted to log back into Prime Network is root. This is because root is also an *emergency user*, and is validated only by Prime Network. The root user can then log into Prime Network, change the authentication method to local, and edit user accounts so that those users can subsequently log in. Prime Network uses LDAP version 3.

Note User authentication by Prime Network is disabled if Prime Network is installed with Cisco Prime Central. However, the emergency user will still be allowed to log into Prime Network.

If you want to use external authentication, you must do the following:

- Perform the necessary installation prerequisites. See the *Cisco Prime Network 3.8 Installation Guide*.
- Configure Prime Network so that it can communicate with the LDAP server. See Configuring Prime Network to Communicate with the External LDAP Server, page 7-10.

If you are switching from external authentication to Prime Network authentication, you can import the user information from the LDAP server into Prime Network. That procedure is described in the Importing Users from the LDAP Server to Prime Network, page 7-13.

Prime Network User Roles

Note User authentication by Prime Network is disabled if Prime Network is installed with Cisco Prime Central.

User roles control the actions a user is authorized to perform in Prime Network. Prime Network provides five predefined security access roles that you can grant to users to enable system functions (see Table 7-1).

Note Users with higher user roles can perform all the actions for which lower roles are authorized. For example, the Configurator is authorized to perform all the actions that the Viewer, Operator and OperatorPlus can perform.

Table 7-1 User Access Roles

Role	Description
Viewer	Views the network, links, events, and inventory. Has read-only access to the network and to nonprivileged system functions.
Operator	Performs most day-to-day business operations such as managing alarms, working with existing maps, viewing network-related information, and managing business attachments.
OperatorPlus	Manages tickets and the alarm lifecycle.
Configurator	Performs tasks and tests related to configuration and activation of services, through Command Builder, Configuration Archive, NEIM, and activation commands.
Administrator	Manages the Prime Network system and its security using the Prime Network Administration GUI.

User access roles are used in two ways: for *default permissions* and for device scope *security levels*.

When you create a user account, you assign one user access role to the account. This role determines the user's default permissions, which in turn determine the GUI-based functions the user can perform (those that do not affect devices). The device-based operations (that do affect devices) the user can perform are controlled by the user's assigned device scopes.

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 Prime Network Administration. These activities are performed with the highest privileges. Prime Network Administration supports multiple administrators.

Once a user account is created, you can assign a device scope to the account. The device scope controls which devices a user can access, and the actions they can perform on those devices. For more information, see Device Scopes, page 7-3.

Device Scopes

Note Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

Device scopes are groups of managed NEs. Users can only access devices when a device scope has been assigned to their account. In this way, you can control the devices a user can access. Furthermore, you can designate a *security level* (user access role) within each scope that controls the actions users can perform on those NEs. (The GUI-based operations (that do not affect devices) are controlled by the user's default permissions.)

Prime Network provides a predefined scope called All Managed Elements, which cannot be edited. It has these characteristics:

- The scope includes all network elements (as the name implies).
- This scope is automatically assigned to user accounts with Administrator privileges when the accounts are newly created. This is done by default. If necessary, you can edit the scope to have less privileges, or even delete it completely, which would give the Administrator full access to all GUI functions that do not affect devices.
- The scope can be assigned to non-Administrator user accounts, but with lower privileges. For example, for an account with OperatorPlus privileges, you could assign the All Managed Devices scope to the account, but the highest available security level would be Configurator.

Whenever the All Managed Elements scope is assigned to an Administrator—either when the Administrator account is created or after increasing a user's privileges to Administrator role—the scope has a unique (and recognizable) security level called Special. The Special security level is equivalent to the Administrator security level and grants the Administrator user complete access to the network devices.

Note that a device scope can override a GUI user access role. Here is an example:

1. John has the Operator user access role (his default permission) for GUI operations.
2. John has the Configurator role for the device scope CE-SJ.

John can perform Configurator operations on any devices in the device scope CE-SJ, even though his default permission is the Operator user access role.

Table 7-2 describes the actions a user can perform in the GUI clients or in a scope, based on each user access role.

Note Users with higher user roles can perform all the actions for which lower roles are authorized. For example, the Configurator is authorized to perform all the actions that the Viewer, Operator, and OperatorPlus can perform.

Table 7-2 Scope and GUI Functions Permitted According to User Access Roles

User Access Role	GUI-Based Actions Permitted to Users with This Role	Device Based (Scope) Actions Permitted to Users with This Role
Administrator	Administrators are the *only* users that can perform actions in Prime Network Administration, which means managing: • Gateways, units, AVMs, VNEs. • Event notifications • Global settings: Database segments, event management settings, polling groups, protection groups, service disclaimers, report settings, and security settings (including user authentication method and password rules). • Device scopes. • User accounts. • Static topology links. • Workflow templates and workflows. Perform *all* event management actions in Prime Network Events. Perform all monitoring tasks in Prime Network Vision. • Launch PathTracer.	All
Configurator	Advanced tools: • Ping and Telnet an NE directly from the client. • Prime Network Command Builder.	Advanced tools: • Enable and disable port alarms. • Deploy workflows (that have BQL tasks). Activation services: • Add and publish activation commands on managed NE (regardless of whether the NE is inside or outside the Configurator's scope)
OperatorPlus	Maps: • Create new maps and add NEs. • Edit, delete, and rename maps. • Save maps. • Find, select, and filter links.	Display network information: • Include path tool traffic, rates, drops, or any dynamic data.
Operator	• Maps: Group and ungroup aggregations • Create and delete business tags.	Display network information: • Refresh port information from NE.

Table 7-2 Scope and GUI Functions Permitted According to User Access Roles (continued)

User Access Role	GUI-Based Actions Permitted to Users with This Role	Device Based (Scope) Actions Permitted to Users with This Role
Viewer	Application: • Log into Prime Network Vision. • Change user password (if using local authentication). • View the device list, maps, and link properties. • Connect to Workflow Editor and retrieve workflows (but not deploy them). • Use table filter. • Export from any table. Maps: • View and print maps. • Change a map layout. • Resize map elements.	Display network and business tag information: • View alarm list and alarm properties, and find alarms. • Find and view attachments. • View NE properties and inventory. • Calculate and view affected parties. • Open port utilization graph.

These guides provide detailed lists about the roles that are required to use these Prime Network functions:

- *Cisco Prime Network 3.8 User Guide* for Vision, Events, PathTracer
- *Cisco Prime Network 3.8 Customization User Guide* for Command Builder, Workflow Editor, Soft Properties, VNE Customization Builder
- *Cisco Prime Network 3.8 Activation User Guide* for Prime Network Activation scripts
- *Cisco Prime Network 3.8 Change and Configuration Management User Guide* for Prime Network Change and Configuration Management

Steps for Setting Up Users and Scopes

Note These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network.

Follow these steps to set up user accounts and device scopes.

Step	Description	See:
1	Configure external authentication if you want to use an external LDAP server to store passwords and authenticate users.	Using an External LDAP Server for Password Authentication, page 7-7
2	Set up the global password and security rules.	Managing Global Security Settings, page 7-7

Step	Description	See:
3	Define scopes. This enables you to group specific managed network elements so that users can view and manage those network elements based on their individual user role.	Creating and Managing Scopes, page 7-16
4	Define Prime Network user accounts. This enables you to define and manage user accounts, including the maps the user can access.	Managing User Accounts and Controlling User Access, page 7-19

Managing Global Security Settings

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

The global Security Settings control the following:

- Using an External LDAP Server for Password Authentication, page 7-7—This topic explains how external authentication works, prerequisites and how to use the Authentication Method window, how to import a list of users, and how to change from external to local authentication.
- Setting Global Password Rules, page 7-14—The global Password Settings window allows you to specify password strength, the number of allowed password retries, and how often users should change their passwords. These rules are applied to all users.
- Automatically Disabling Accounts for Inactive Users, page 7-15—The User Account settings specifies when user accounts should be disabled due to inactivity.

Using an External LDAP Server for Password Authentication

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

The following topics describe how you can use an external LDAP server to perform user authentication. By default, Prime Network users internal authentication, which means passwords are stored in and verified against the data that is stored in the Prime Network database. If you want to use external authentication, these topics will guide you through the process.

- How Does External Authentication Work?, page 7-8
- Prerequisites for Using LDAP, page 7-9
- Configuring Prime Network to Communicate with the External LDAP Server, page 7-10
- Importing Users from the LDAP Server to Prime Network, page 7-13
- Changing from External to Local Authentication, page 7-14

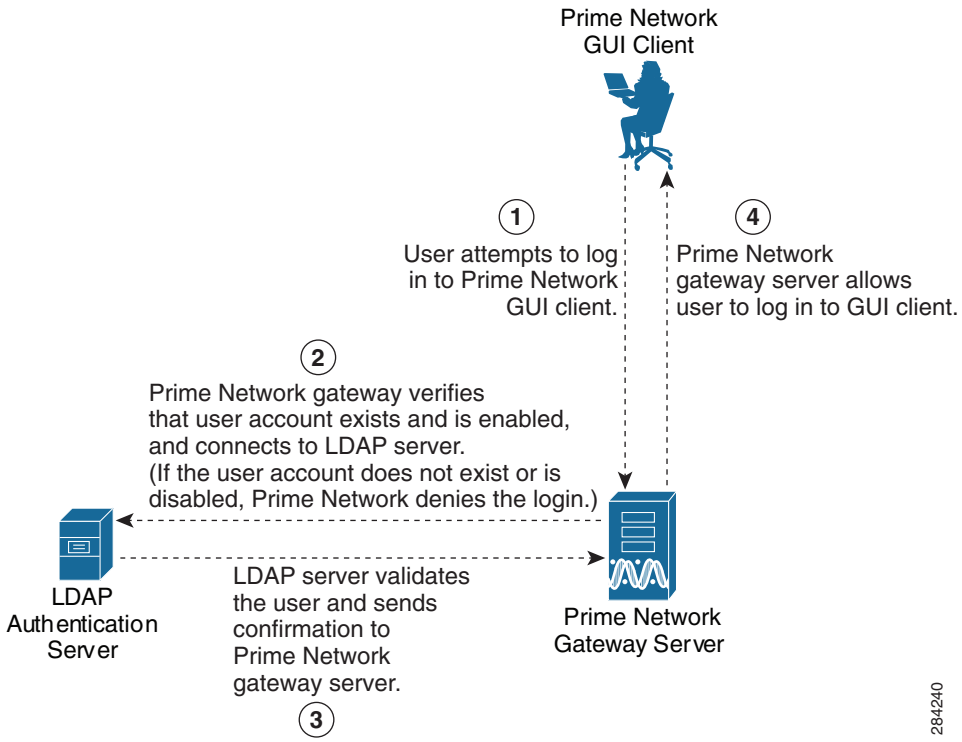
How Does External Authentication Work?

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

User authentication can be managed locally by Prime Network or externally by a Lightweight Directory Access Protocol (LDAP) application. If you use an external authentication, user information is checked against what is stored in the external LDAP server (instead of the Prime Network database). The external authentication server only stores login and password information; information pertaining to user roles and scopes is stored in the Prime Network database.

As illustrated in Figure 7-1, when a user logs in to the GUI client, the gateway server contacts the LDAP server to authenticate the user. If the user is successfully authenticated, the LDAP server sends a confirmation to the gateway server, and the gateway server allows the user to log in to Prime Network. From that point on, the user can perform functions and access network elements as specified by their roles and scopes (see Overview of User Authentication and Authorization, page 7-1).

Figure 7-1 User Authentication Process with External LDAP Server



The root user is the *emergency* user. The LDAP emergency user is validated only by Prime Network. Consequently, if the LDAP server goes down, root can log back into Prime Network.

Note If Prime Network is installed with Cisco Prime Central, the emergency user will still be allowed to log into Prime Network.

Prerequisites for Using LDAP

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

You must meet the following prerequisites before you can configure Prime Network to use LDAP:

- The LDAP server must be reachable from the Prime Network server, including port 389 for nonencrypted communication, 636 for encrypted communication.
- The LDAP server must support LDAPv3 protocol.
- Windows Server 2003 Active Directory must be configured. Configuring a Secure Connection with the Windows Server 2003 Active Directory, page 7-9
- For encrypted communication, a certificate must be installed on the Prime Network server. See Installing the LDAP Certificate on the Prime Network Gateway Server, page 7-10.

Configuring a Secure Connection with the Windows Server 2003 Active Directory

To manage users in the Active Directory from Java, the connection to the server must be secure. Follow these procedures to make the server connection secure.

If you are using Secure Socket Layer (SSL) for encryption between the Prime Network server and the LDAP server, the Windows server must be a domain controller installed with an Enterprise Certificate Authority. To guarantee a secure connection, you must request and install the appropriate certificate.

To obtain the certificate from the LDAP server and place it on the gateway:

Step 1 Use Router Discovery Protocol (RDP) to log into the remote LDAP server.

Step 2 Choose **Start > Programs > Administrative Tools > Domain Controller Security Policy**.

Step 3 In the left pane, choose **Security Settings > Public Key Policies > Automatic Certificate Request Settings**.

Step 4 Right-click the right pane and choose **New > Automatic Certificate Request**.

Step 5 Click **Next**.

Step 6 Choose **Domain Controller** and click **Next**.

Step 7 Click **Finish**.

Step 8 Restart the server.

Step 9 After the server restarts, enter the following command on the command line:

```
# netstat -na
```

The SSL port 636 should be active; for example:

```
TCP    0.0.0.0:636        0.0.0.0:0          LISTENING
```

Installing the LDAP Certificate on the Prime Network Gateway Server

Prime Network requires a certificate to open a context with the LDAP server. To import the certificate into the system .truststore file, complete the following steps:

Step 1 Download the certificate from the relevant LDAP workstation:

a. From the client workstation, go to http://*ldaphost*/certsrv, where *ldaphost* is the fully qualified domain name or IP address of the LDAP server.

b. For blade LDAP, enter the service provider username and password.

c. Click **Download a CA certificate, certificate chain, or CRL**.

d. Choose **Previous cmpdc** in the **CA certificate** option.

e. Click **Download CA certificate**.

f. Save the certnew.cer file on the workstation. You can rename the file as CA.*LDAP-IP-address*.cer.

Step 2 Log into your workstation.

Step 3 Go to ~/Main/resourcebundle/com/sheer and copy the .cer file to that directory.

Step 4 Enter the following command on the command line:

```
# keytool -import -alias LDAPID -file CA.LDAP-IP-address.cer -keystore .truststore
```

Note Use the password in the security.properties file in this directory. Be sure to use a unique ID to set a unique alias.

Step 5 Enter the following command to check your LDAP certificates on the system .truststore file:

```
# keytool -list -keystore .truststore
```

Configuring Prime Network to Communicate with the External LDAP Server

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

Use this procedure to configure the Prime Network gateway server to communicate with the LDAP server, and to test the connection after it is configured. You can configure a primary and secondary LDAP server. This procedure uses LDAP terminology, such as distinguished name (DN), common name (CN), and domain component (DC). An LDAP distinguished name uniquely identifies a user in the LDAP database, similar to a full filename but in reverse order. CNs and DCs are attributes of the domain name.

Before You Begin

Make sure you have performed the required prerequisites that are described in the *Cisco Prime Network 3.8 Installation Guide*:

- The LDAP server is correctly configured.
- You know the port number needed for the SSL or simple encryption protocol. These are normally 636 for SSL and 389 for simple.

- If you select SSL for the Application-LDAP Protocol, the SSL certificate must be installed on the Prime Network gateway.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To configure the Prime Network gateway server to communicate with the LDAP server:

Step 1 Choose **Global Settings > Security > Authentication Method**.

Step 2 Click **LDAP Authentication** to activate the LDAP Settings area.

Step 3 Complete the LDAP settings. The settings include specifying LDAP schema attributes, such as CN (common name) and DC (domain component).

Table 7-3 LDAP Authentication Method Settings

Field	Description
LDAP URL	LDAP server name and port number, in the following format: **ldap://***host.company***.com:***port* where: • *host.company***.com**—Fully qualified domain name or IP address of the LDAP server, followed by the final two fields of the Distinguished Name Suffix (company.com, described below • *port*—Network port of the LDAP server. The LDAP server port number is normally 389 for simple encryption and 636 for SSL encryption. To specify a primary and secondary LDAP server, use the following format: **ldap://***host1.company***.com:***port1* **ldap://***host2.company***.com:***port2* For example: **ldap://ldapsj.acme.com:636 ldap://ldapsfo.acme.com:636**
Distinguished Name Prefix	First part of the LDAP DN, which is used to uniquely identify users. Enter the information exactly as shown: **CN** (The actual format is **CN=***Value*, which specifies the common name for specific users. =*Value* will be automatically populated with Prime Network usernames.)

Table 7-3 LDAP Authentication Method Settings (continued)

Field	Description
Distinguished Name Suffix	Second part of the LDAP distinguished name, which specifies the location in the directory: **,CN=Users,DC=***LDAP_server*,**DC=***company*,**DC=com** where: • **,CN=Users**—Common name for the type of user; enter **Users**. For example: **,DC=Users** • **,DC=***LDAP_server*—Domain component that specifies the fully qualified domain name or IP address of the Prime Network server. For example: **,DC=ldapsj** • **,DC=***company*—Beginning of the domain name. For example: **,DC=acme** • **,DC=com**—End of the domain name; enter **com**. For example: **,DC=com** The form should: • Begin with a comma. • End without any ending symbols or punctuation. For example: **,CN=Users,DC=ldapsj,DC=cisco,DC=com**
Application-LDAP Protocol	Encryption protocol used for communication between the Prime Network gateway server and the LDAP server. **Note** The encryption protocol used must be configured on both the Prime Network gateway server and the LDAP server. The supported protocols are: • **SIMPLE**—Encrypt using LDAP. Uses port 389 by default. • **SSL**—Encrypt using SSL. Uses port 636 by default. The SSL certificate must be installed on the Prime Network gateway (see the *Cisco Prime Network 3.8 Installation Guide*.

Step 4 Click **Test Connection** to test the connection between the gateway server and the LDAP server.

Step 5 Click **Apply**.

Step 6 Restart the gateway for your changes to take effect. See Starting and Stopping the Gateway and Checking AVM Status, page 2-3.

You can now manage user passwords using the external LDAP server.

Importing Users from the LDAP Server to Prime Network

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

You can perform a bulk import of users from the LDAP Data Interchange Format (LDIF) file. The Prime Network **import_users_from_LDIF_file.pl** command has the following attributes:

- LDIF filename.
- Prime Network role—Administrator, Configurator, Operator, OperatorPlus, and Viewer (the default).
- username—Attribute name as it appears in the LDIF file. The username can appear in the LDIF file as username only, or in the format *username@domain*. In both cases, after the import, the Prime Network user is the name only (without the *@domain* suffix).
- user description—Attribute name as it appears in the LDIF file.
- user full name—Attribute name as it appears in the LDIF file.

The LDIF file has the following constraints:

- For each user, the username attribute is mandatory. The description and full name are optional.
- All other attributes are ignored.
- The LDIF file should reside in the gateway workstation under the ~/Main directory.

For example, for a Windows LDAP server, enter the following command to produce a valid LDIF file:

```
# ldifde -l description,displayName,userPrincipalName -f desired-filename -r
objectClass=user
```

The **import_users_from_LDIF_file.pl** command has the following syntax:

import_users_from_LDIF_file.pl *ldif-filename* [*roleName*] *username-attribute-name user-desc-attribute-name full-name-attribute-name*

Example LDIF File and Import Command

This example uses an LDIF file named users.LDF, with the following contents:

```
dn: CN=xxx,CN=Users,DC=ldapsj,DC=com
changetype: add
displayName: xxx
userPrincipalName: xxx@acme.com

dn: CN=yyyy,CN=Users,DC=ldapsj,DC=com
changetype: add
displayName: yyyy
userPrincipalName: yyy@acme.com

dn: CN=zzz,CN=Users,DC=ldapsj,DC=com
changetype: add
description: description
displayName: zzz
userPrincipalName: zzz@acme.com
```

This corresponding Prime Network command is as follows:

```
# cd $ANAHOME/Main/scripts
# import_users_from_LDIF_file.pl users.LDF userPrincipalName description displayName
```

This example would create three users with a Viewer role.

Note All imported users are created with non-Prime Network authentication permissions (LDAP authentication). If the username already exists in Prime Network, the new user is not created.

Changing from External to Local Authentication

Note The Authentication Method feature is disabled if Prime Network is installed with Cisco Prime Central. However, the emergency user will still be allowed to log into Prime Network.

If Prime Network is using external authentication and cannot communicate with the LDAP server, the only user permitted to log back into Prime Network is root. This is because root is the *emergency user,* and is validated only by Prime Network. The root user can then log into Prime Network, change the authentication method to local, and edit user accounts so that those users can subsequently log in. For information on editing user accounts, see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To change from external to local authentication, follow this procedure:

Step 1 Choose **Global Settings > Security > Authentication Method**.

Step 2 Click Prime Network **Authentication** to activate local authentication.

Step 3 Click **Apply**.

Step 4 Restart the gateway for your changes to take effect. See Starting and Stopping the Gateway and Checking AVM Status, page 2-3.

Step 5 Reconfigure user accounts accordingly (see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22).

Setting Global Password Rules

Note The Password Settings feature is disabled if Prime Network is installed with Cisco Prime Central.

You can set password rules that will apply to all new user accounts and to existing accounts when users change their passwords. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To set up or change global password rules:

Step 1 Choose **Global Settings > Security Settings > Password Settings**. The Title and Message fields appear in the content area.

Step 2 Configure the general settings in the General area:

- Password Validity Period—Number of days after which users must change their password.
- Number of Attempts Before Lockout—Choose a value from 3 to 7, or Unlimited. If a user is locked out, they cannot log back in until an administrator reenables their account (see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22).

Step 3 Check the check boxes for the password strength settings you want to apply to all users by default:

- Number of previous passwords that cannot be repeated (1 to 15)
- Number of character types required in password (0 or 3)
- Whether repeated characters can be used consecutively
- Whether usernames can appear in passwords
- Words that cannot appear in any passwords (comma-separated list)

Step 4 Click **Apply** to immediately apply your settings.

After you click **Apply**, the password settings are applied to all new user accounts. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

For information about the main menu that is displayed in the Prime Network window, see Password Settings Window, page 1-26.

Automatically Disabling Accounts for Inactive Users

Note The User Account Settings feature is disabled if Prime Network is installed with Cisco Prime Central.

You can configure Prime Network to disable a user account when a user has not logged in for a specified period of days. By default, this period is 30 days.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To change this setting:

Step 1 Choose **Global Settings > Security Settings > User Account Settings**.

Step 2 Enter the number of days after which the accounts will be disabled.

Step 3 Click **Apply** to immediately apply your settings.

After you click **Apply**, the password settings are applied to all new user accounts. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

You can reenable a user account as described in Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

For information about the main menu that is displayed in the Prime Network window, see User Account Settings Window, page 1-27.

Creating and Managing Scopes

Note Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

Prime Network Administration enables you to group specific managed network elements so that users can view and manage those network elements based on their user role or permission.

After 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, you must provide the user with security access roles that define the user's role within the assigned scope. See Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

These topics explain how to manage scopes:

- Creating Device Scopes in Prime Network, page 7-16
- Viewing and Editing Existing Device Scopes, page 7-18
- Deleting a Device Scope from Prime Network, page 7-18

Creating Device Scopes in Prime Network

Note Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

A scope is a group of devices. Users cannot perform any devices until you create a scope and apply it to their user account.

Note By default, users can only view links if both endpoints are in this scope. If you want to change this setting so that only one link endpoint is required, see Viewing Links in Device Scopes, page 7-17.

To create a scope:

Step 1 Right-click **Scopes** and choose **New Scope** to open the New Scope dialog box.

Step 2 In the Scope field, enter a name for the scope.

Step 3 Add devices to the scope by selecting them from the Available Devices list and moving them to the Selected Devices list.

Note You can select multiple devices by using the Ctrl key.

Step 4 Click **OK**. The scope is saved and is displayed in the content area.

Step 5 If you want a user to be allowed

Note that the scope does not have a default security level. When you add the scope to a user's account, you specify their security role on the scope at that time. This allows you to provide different security levels for different users.

Viewing Links in Device Scopes

By default, a user can view a link in Prime Network Vision only if *both* link endpoints are in the user's device scope. If you want to make links viewable if only *one* endpoint is in a user's scope, you must edit the registry as follows. Changes are applied to all device scopes in the system.

Step 1 Log into the gateway as *network-user* (where *network-user* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of *network-user* is **network38**), and change to the *NETWORKHOME*/Main directory:

```
# cd $ANAHOME/Main
```

Step 2 To check the current setting, run the following command (which is one line):

```
# ./runRegTool.sh -gs 127.0.0.1 get 0.0.0.0
"site/mmvm/services/securitymanager/linkoid-by-any-side"
```

A return of false means it is set to the default; that is, both links must be in a user's scope to be viewable.

Step 3 To change the setting so that only one link endpoint is required, run the following command (which is one line):

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/mmvm/services/securitymanager/linkoid-by-any-side" true
```

Step 4 When the gateway server returns a success message, restart it.

Viewing and Editing Existing Device Scopes

Note Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

To view the properties of an existing scope, simply right-click the scope and select **Properties**.

When editing a scope, keep the following mind:

- You can add or delete devices from an existing scope. The changes will be applied to all user accounts that have access to that scope.
- You cannot change the name of an existing scope.
- You can change the security level on a device scope, but not from the Scopes window. You must edit the user account in the Users window. See Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

To edit a scope by adding or deleting devices:

Step 1 Select **Scopes** to populate the list of existing scopes.

Step 2 Right-click a scope and choose **Properties**.

Step 3 Modify the scope device list by selecting them from the Available Devices list and moving them to the Selected Devices list.

Note You can select multiple devices by using the Ctrl key.

Step 4 Click **OK**. The scope is updated and is displayed in the content area.

Deleting a Device Scope from Prime Network

Note Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

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

To delete a scope:

Step 1 Select **Scopes** in the navigation pane.

Step 2 Right-click the scope you want to remove, then choose **Delete**.

Note You can select multiple scopes by using the Ctrl key.

The scope is deleted and is removed from the content area.

Managing User Accounts and Controlling User Access

Note These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network. If you migrate from standalone to working with Cisco Prime Central, you must create the Cisco Prime Central users using the Cisco Prime Portal portal, even if the users already existed in standalone mode. (Cisco Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Cisco Prime Central user.)

The Users windows enable you to define and manage user accounts. This includes managing general user information as well as security access rights and forced login changes, as required. You can also monitor a user's last login time. See the following topics for more information:

- Creating a New User Account and Viewing User Properties, page 7-19
- Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22
- Controlling User Access to Maps (Maps Tab), page 7-23

Creating a New User Account and Viewing User Properties

Note These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network. If you migrate from standalone to working with Cisco Prime Central, you must create the Cisco Prime Central users using the Cisco Prime Portal portal, even if the users already existed in standalone mode. (Cisco Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Cisco Prime Central user.)

The following procedure describes how to define a user account. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Step 1 Right-click **Users** and choose **New User** to open the New User dialog box.

To view an existing user's account, right-click a user account and choose **Properties**.

Step 2 Enter the general information about the user in the General Settings area. For existing users, click the General tab to display this information.

Field	Description
User Name	Enter the new user's name to be used for logging in.
Full Name	(Optional) Enter the full name of the user.
Description	(Optional) Enter a free text description of the user.

Field	Description
External user only	If checked, Prime Network will only let the user log in if the user's password can be validated by an external LDAP server. The password fields are disabled. (If external authentication is being used, the box is checked by default. See Using an External LDAP Server for Password Authentication, page 7-7.) Click **Test Connection** to confirm the connection between the gateway and the LDAP server.
Password	Enter the new Prime Network password, which is then stored in the Prime Network database. Passwords must adhere to the global password rules set by the administrator (see Setting Global Password Rules, page 7-14). This field is disabled if you are using LDAP (external user) for authentication.
Confirm password	Reenter the new Prime Network password.

Step 3 Click **Next** and configure the GUI client and device authorization settings for the user. For existing users, click the Authorization tab to display these settings.

Field	Description
User Role	Select the role that will control the actions the user can perform in the Prime Network, such as which functions they can use in the GUI clients. Click **Read More** for a description of the roles; you can also get more information from Prime Network User Roles, page 7-2. For information on the special All Managed Elements scope, see Device Scopes, page 7-3.
Device Security	Select scopes and apply the security levels to them that will control the actions the user can perform on devices. You can apply different security levels for different scopes. If you do not apply a security level to a scope, it defaults to the Viewer level. **Note** Users will not see any devices in the GUI client unless a device scope is assigned to their account. Use the following buttons to manage scopes. Note that the edit and remove buttons only affect the scopes assigned to this user. • **Add**—Add a scope to this user account from the list of available scopes. • **Edit**—Edit the security level for a scope *assigned to this user.* (This edit function only changes the user's scope security level; it does not change the scope device list. That must be done from the Scopes drawer. • **Remove**—Deletes a scope *from this user's account*. • **New Scope**—Creates a new scope and adds it to the list of available scopes *for all users*. See Creating Device Scopes in Prime Network, page 7-16. Changes that you apply to a scope will be applied to all users that have access to that scope.

Step 4 Click **Next** and enter the account settings for the user. For existing users, click the Account tab to display these settings. (If you are creating a new account, you can also click **Finish** to accept the default account settings. The default settings are provided in the following.)

Field	Description	Default
Enable Account	Enables and disabled the user account. You can manually lock or unlock a user's account at any time. A user whose account is locked cannot log into the system until you reenable their account. The user account is automatically locked if: • The number of logins defined is exceeded (see the Limit Connections field in the following). • The user account is not active for a certain number of days, as configured in the Global Settings branch (see Automatically Disabling Accounts for Inactive Users, page 7-15); by default, this period is 30 days.	Enabled.
Force Password Change at Next Login	Check this check box to force the user to change their user password when they next log in. This field is disabled if the gateway server is using external LDAP authentication.	Enabled.
Limit Connections:	The maximum number of Prime Network client sessions that the user can be running at any one time. This includes all client types including BQL sessions and workflow invocations. Leaving this field blank means the user can have *unlimited* connections. **Note** The workflow mechanism requires 3 connections. If you set this value to lower than 3, users will not be able to access the workflow mechanism.	10 connections
Force Password Change After ___ Days	Forces the user to change their password after a specific number of days. Uncheck this check box to allow the user to retain their current password indefinitely. This field is disabled if the gateway server is using external LDAP authentication.	Controlled by Global Settings; see Setting Global Password Rules, page 7-14.

Step 5 Click **Finish**. and Prime Network creates the account. After the confirmation message is displayed, click **Close** to close the dialog box. The new account is displayed in the Users table.

Viewing, Changing, and Disabling User Accounts and Device Scope Access

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

Administrators can view, edit, or disable an individual user's account settings.

To change global settings such as password rules and inactivity periods, see Managing Global Security Settings, page 7-7. The global settings control settings for all users.

Step 1 Select **Users** to populate the list of existing user accounts.

Step 2 Right-click a user account and choose **Properties** to open the user properties dialog box.

Step 3 Edit the following fields, as required (not all fields are editable).

Field	Description
General Tab	
Full Name	(Optional) Full name of the user.
Description	(Optional) Free text description of the user.
Authorization Tab	
User Role	The role that will control the actions the user can perform in the Prime Network, such as which functions they can use in the GUI clients. For information on how to make changes, see Creating a New User Account and Viewing User Properties, page 7-19.
Device Security	Scopes and apply the security levels to them that will control the actions the user can perform on devices. For information on how to make changes, see Creating a New User Account and Viewing User Properties, page 7-19.
Account Tab	
Enable Account	Enables and disabled the user account.
Force Password Change at Next Login	Force the user to change their user password when they next log in. This field is disabled if the gateway server is using external LDAP authentication.
Limit Connections:	The maximum number of Prime Network client sessions that the user can be running at any one time. This includes all client types.
Force Password Change After ___ Days	Forces the user to change their password after a specific number of days. Uncheck this check box to allow the user to retain their current password indefinitely. This field is disabled if the gateway server is using external LDAP authentication.

Step 4 Click **Apply** to apply your changes, and click **OK** to close the Properties dialog box

Controlling User Access to Maps (Maps Tab)

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

You can use the Maps tab to control user access to existing maps.

Note This feature is disabled by default.

When logging into Prime Network Vision, new users do not have permission to view any existing maps; they can only access maps they create going forward. However, administrators can assign existing maps to new users by enabling this feature and manually assigning the maps.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To enable this feature:

Step 1 Log into the gateway as *network-user* (where *network-user* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of *network-user* is **network38**), and change to the *NETWORKHOME*/Main directory:

```
# cd $ANAHOME/Main
```

Step 2 Run the following command (which is one line):

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/mmvm/services/securitymanager/map-security-enabled" true
```

Step 3 When the gateway server returns a success message, restart the gateway.

To assign maps to a user (after enabling the feature):

Step 1 Select **Users** in the Prime Network window.

Step 2 Right-click the required user, then choose **Properties**. The User Properties dialog box is displayed.

Step 3 Click the **Maps** tab. The Maps tab is divided into two parts:

- The left side displays a list of all available maps in the database that have not been assigned to the user.
- The right side displays all maps that have been assigned to the user and that the user can open and manage in Prime Network Vision.

Step 4 Choose a map from the list of Available Maps, then click the required button to add the map to the list of Assigned Maps to the user.

Note You can select multiple rows by using the Ctrl key.

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

Step 6 Click **OK** to confirm the user's assigned maps.

Deleting a Prime Network User Account

Note This feature is disabled if Prime Network is installed with Cisco Prime Central.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

If you want to disable a user account but not delete it, see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

To delete a user account:

Step 1 Select **Users** in the navigation pane.

Step 2 Right-click the account you want to remove, then choose **Delete**.

The account is deleted and is removed from the content area.

Changing a User's Prime Network Password

Note This feature is disabled if Prime Network is installed with Cisco Prime Central.

You can use Prime Network Administration to change a user's Prime Network password at any time. Passwords must adhere to the global password rules set by the administrator (see Setting Global Password Rules, page 7-14).

The following procedures apply only if you are using Prime Network to validate users. If you are using an external LDAP application to manage passwords, you must change the passwords in the LDAP server.

There are different procedures for administrators and for users, as described in the following. The root user password can also be changed using these procedures.

Note If you have lost the root password, you can create a new one using the procedure in Changing Passwords: bosenable, bosconfig, and bosusermanager, and root, page 15-4.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Changing Passwords—Procedure for Administrator

Administrators can change any user's password using the following procedure.

Step 1 Select **Users** in the navigation pane.

Step 2 Right-click the users account, then choose **Change Password**.

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

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

Step 5 Click **OK**.

Changing Passwords—Procedure for Users

Users can change their own passwords using the following procedure.

Step 1 Choose **Tools > Change User Password**.

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**.