CHAPTER 7

Managing User Accounts and Authentication

Note User authentication and authorization by Prime Network is disabled if Prime Network is installed with Cisco Prime Central. If you want to prevent users from managing tickets from the Prime Network clients, see Disabling Ticket Management in the Prime Network Vision and Events Clients, page 9-24.

User account settings determine the actions users can perform in Prime Network. Each user has an access role that determines the GUI-based tasks they can perform. Device-based tasks are determined by the device scopes that are applied to a user's account, and the privileges they have for that scope. You can also control which maps users can access.

These topics explain how to create and manage user accounts. These topics also explain how to change global password rules and how to change the default access role required to log into the Events GUI client.

If you want to find out who is logged into the gateway (and disconnect them, if necessary), see Managing Client and User Sessions, page 3-21.

User Authentication and Authorization Overview

Note Most user authentication and authorization features by Prime Network are disabled if Prime Network is installed with Cisco Prime Central. See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6 for the exceptions.

In Prime Network, user authentication and authorization is controlled by a combination of device scopes, user roles, and other settings in a user's account. While device scopes determine which devices a user can access and what they can do to those devices, user roles and account settings determine the GUI tasks a user can perform.

User Authentication

User authentication is managed either 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 into Prime Network. If you use Prime Network for authentication, user information and passwords are stored in the Prime Network Oracle database. If you use an external LDAP application for authentication, passwords are stored on the external LDAP server. (User authorization information—that is, roles and scopes—is always stored in the Prime Network Oracle database. The external LDAP server, if used, only stores passwords.) The external authentication method has a special user called the *emergency user*. In Prime Network, root is designated as the external authentication emergency user. This means if Prime Network loses communication with the LDAP server, Prime Network will allow root (and only root) to log in. The root user can then change the authentication method to local, and edit user accounts so that those users can subsequently log in. Prime Network uses LDAP version 3.

Other User Account Settings that Affect Authentication

When you create a user's account, you can also specify the intervals at which users must change their passwords. Prime Network also has authentication settings that are controlled at the global level, such as how many login attempts are permitted before the user is locked out, and when to lock the account due to user inactivity. If a user account is locked, you can easily reenable it from their user account dialog box.

Change the Authentication Method

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

- Perform the necessary installation prerequisites. Refer to the *Cisco Prime Network 4.1 Installation Guide*.
- Configure Prime Network so that it can communicate with the LDAP server. See Using an External LDAP Server for Password Authentication, page 7-14.

If you want to change 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 Changing from External to Local Authentication, page 7-21.

User Authorization

User authorization is controlled by a combination of user roles, device scopes, and other user account settings.

User Roles

Prime Network provides five predefined security access roles that you can assign to a user when you create their account: Viewer, Operator, OperatorPlus, Configurator, and Administrator. These roles determine which actions a user is permitted to perform in the Prime Network GUI clients. Table 7-1 describes the five user roles.

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

User 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 working with existing maps, viewing network-related information, and managing business attachments.
OperatorPlus	Creates new maps, and manages tickets and the alarm life cycle.
Configurator	Performs tasks and tests related to configuration and activation of services.
Administrator	Manages the Prime Network system and its security using the Prime Network Administration GUI.

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).

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.

Device Scopes

Device scopes control which devices a user can access, and the actions they can perform on those devices. When you create the user account, you assign one or more device scopes to the user's account, along with a security level for that scope. Detailed information about device scopes and security levels is provided in Controlling Device Access and Authorization Using Device Scopes, page 6-1. You can add device scopes to a user account Changing User Accounts and Device Scope Access, page 7-11.

Other Settings that Affect Authorization

These settings also affect authorization:

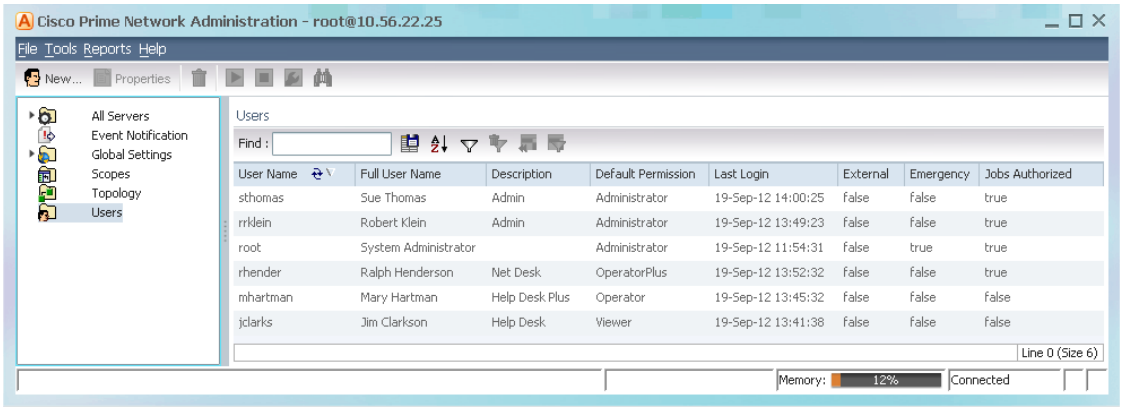
- When you create a user's account, you can also specify whether the user is permitted to create public (shared) reports and manage jobs. See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.
- Ticket actions can be disabled from the Global Settings branch. This disallows both Vision and Events client users from ticket operations such as clearing, acknowledging and deacknowledging, clearing, adding notes, and so forth. By default, ticket actions remain enabled when you are using Prime Network with Cisco Prime Central. If you want to disable ticket operations in Prime Network, see Disabling Ticket Management in the Prime Network Vision and Events Clients, page 9-24.

Checking Existing User Accounts

To check existing user accounts, click Users in the navigation area. Figure 7-1 shows an example of the Prime Network Administration window with Users selected.

Note If Prime Network is installed with Cisco Prime Central, you can view user properties but you cannot add or change them.

Figure 7-1 Users Window



The following describes the columns that are displayed in the Users table.

Column	Description
User Name	The unique username defined for the current client station.
Full User Name	(Optional) Full username.
Description	A description of the user.
Default Permission	The default permission of the user, such as Viewer or Administrator. For example, a user with the default permission Viewer can view maps and the Device List. **Note** The default permission applies only at an application level; that is, it applies to all activities that are related to GUI functionality and not the activities related to devices. Device access is controlled through the device scopes mechanism.

Column	Description
Last Login	The date and time that the user last logged in.
External	Indicates whether an external authentication server is used for account and password verification.
Emergency	Indicates that a user is designated as an emergency user for the external authentication server, in case the external server goes down.
Jobs Authorized	Indicates whether the user can schedule jobs when the global Job Scheduling setting is enabled. (See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.

Configuring Global User Password Settings

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

To change the global user password settings listed in Table 7-2, choose **Global Settings > Security Settings > Password Settings**. Changes are applied after you click **Apply**.

Table 7-2 Global Password Settings

Item	Description	Default
Password Validity Period	Number of days after which users must reset their password.	30
Number of Attempts Before Lockout	Number of attempts before a user's account is disabled. (Administrators can reenable accounts as described in Changing User Accounts and Device Scope Access, page 7-11.)	5
Password Strength	The last ___ passwords cannot be repeated (1 to 15)	5
	Password must contain four different character types	Enabled
	No character can be repeated more than twice consecutively	Enabled
	Password cannot contain more than ___ consecutive characters from the previous passwords	4
	Cannot contains replication or reversal of user name	Enabled
	Cannot contain the following words (comma-separated list)	Cisco
Days to alert before password expires	Number of days before the password expires. User will receive a warning during the login that his password is about to expire in x days.	7

Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling

The global User Account Settings page allows you to configure the following features that affect all Prime Network users:

- When users accounts should be disabled due to account inactivity (30 days by default)
- Whether users must enter device credentials before executing any features that user command scripts (disabled by default)
- Whether users can schedule jobs only if they have been granted this privilege in their user account (disabled by default)

To change these settings, choose **Global Settings > Security Settings > User Account Settings**. Changes are applied to new users; for existing users in active sessions, the changes are applied the next time they log in.

Table 7-3 Global User Account Settings

Item	Description	Default
Account Inactivity	Changes the timer for when Prime Network should disable a user account due to inactivity. To disable this setting (so that accounts are never disabled), enter 0.	30 days

Table 7-3 Global User Account Settings (continued)

Item	Description	Default
Execution of Commands	Requires users to enter their device credentials when they execute command scripts from these features: • A device's right-click **Commands** menu in the Vision GUI client (applies only to commands that are immediately executed; does not apply to scheduled commands) • Transaction Manager • Change and Configuration Management (includes Compliance Audit) If the feature is enabled, users are prompted for their username and password when they run a command. Provisioning and Audit events display an additional column that lists the user name. Prime Network Vision instances must be restarted after enabling and disabling the execution of commands. You must logout and then login again for the changes to take effect. For transactions (activation workflows), users must have the same credentials for all devices in the transaction because Prime Network propagates the credentials to *all* command scripts in the transaction. Once the credentials are entered, they are used throughout the current GUI client session for all subsequent commands. This feature is not available for scheduled commands or for SNMP commands. In those cases, the VNE credentials will be used (this is the Prime Network default behavior). VNE credentials are not exposed; events will display the device username as **From VNE login**. **Note** You can also configure Prime Network to generate a warning message whenever a user executes a command script. See Adding a Warning Message to Command Scripts, page 10-2. (If Prime Network is used with Prime Central, this is enabled by default.)	Disabled (standalone) Enabled (suite mode)
Job Scheduling	Enables global per-user authorization for any Prime Network features that use jobs. This feature works in concert with the job setting in individual user accounts (see Creating a New User Account and Viewing User Properties, page 7-9). If global Job Scheduling is enabled, job privileges are controlled by the settings in individual user accounts: • If users have job scheduling privileges, they can run and schedule jobs. • If users do not have privileges, all job scheduling features in their GUI client are disabled. If global Job Scheduling is disabled (which is the default), the setting in individual user accounts is ignored. (If Prime Network is used with Prime Central where Job Scheduling is enabled by default, job privileges are controlled by the settings in individual user accounts.)	Disabled (standalone) Enabled (suite mode)

Configuring Global Report Security Settings (Public Reports)

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

To change the global report setting listed in Table 7-4, choose **Global Settings > Report Settings**.

Table 7-4 Global Report Settings

Item	Description	Default
Security Settings	Allows all users to create shared (public) reports. When a report is public, all users can view the contents; reports are *not* filtered according to scopes or security privileges.	Disabled (no users can create public reports)
Purge reports after ___ days	Specifies how long to save a report. (For information on Prime Network data purging, see Purging Reports, page 8-12.)	90 days
Store reports up to ___ MB	Specifies the maximum disk size, in MB, at which reports should be purged. (For information on Prime Network data purging, see Purging Reports, page 8-12.)	Disabled

Changing GUI Client User Passwords

Note This feature is disabled if Prime Network is installed with Cisco Prime Central. If Prime Network is using an external LDAP server for authentication, do not use this procedure; instead, change the password in the LDAP server.

Users can change their own password when they are logged into any GUI client and they select **Tools > Change User Password**. The password will be changed across all Prime Network GUI clients: Vision, Events, Administration, Change and Configuration Management, and the BQL client.

Administrators can change user passwords by editing a user's account settings; see Changing User Accounts and Device Scope Access, page 7-11.

To change the root password, see Changing System Passwords (Oracle Database, Graphs Tool, root, bos* Users), page 11-9.

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**.

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.

Before You Begin

Check the global security settings to see the current system defaults. You might also want to check the device scopes that are currently available.

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

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.
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 7-14.) 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 Oracle database. Passwords must adhere to the global password rules set by the administrator (see Configuring Global User Password Settings, page 7-5). This field is disabled if you are using LDAP (external user) for authentication.
Confirm Password	Reenter the new Prime Network password.
User is authorized to schedule jobs	**Note** To use this feature, global Job Scheduling must be enabled (it is disabled by default). See Table 7-3 on page 7-6.) Gives the user authority to schedule jobs across the product. If the global authorization mode is disabled, this setting is ignored. If global Job Scheduling is *enabled* and: • This check box is activated, the user is permitted to schedule jobs. • This check box is *not* activated, the job scheduling features in the user's GUI clients will be disabled.

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 User Authentication, page 7-2. For information on the special All Managed Elements scope, see What Are Device Scopes?, page 6-1.
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 What Are Device Scopes?, page 6-1. 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 disables 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 Re-enabling User Accounts, page 7-23); 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.

Field	Description	Default
Limit Connections:	Maximum number of Prime Network client sessions that a user can be running at any one time (to protect performance). This includes BQL sessions and workflow invocations. Leaving this field blank means the user can have *unlimited* connections.	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 Configuring Global User Password Settings, page 7-5.

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.

Changing 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 System Security, page 11-1.

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	
User Name	User ID of the user logged in to the system.
Full Name	(Optional) Full name of the user.
Description	(Optional) Free text description of the user.
External User only	Select this option if the user is an external user.
User is authorized to schedule jobs	Select this option if the user can schedule jobs.
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 Configuring Global User Password Settings, page 7-5.

Field	Description
Device Security	Scopes and security levels that will control the actions the user can perform on devices. For information on how to make changes, see Configuring Global User Password Settings, page 7-5.
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.
User Last Login	Displays date and time of the last login.

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

Changing the Minimum User Access Role for the Events and Administration Clients

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

By default, only users with Administrator privileges can log into the Administration and Events clients. You can adjust Prime Network to allow users with lower privileges to log into these clients.

When you change the required role to a lower role, the higher roles inherit the access. For example, if you change the required security level to Operator, then users with Operator, OperatorPlus, Configuration, and Administrator privileges will be permitted to log into the Events GUI client.

Note This procedure requires a gateway restart.

Change the Minimum Role for the Events Client

Step 1 Choose **Tools > Registry Controller > User Accounts** from the main menu of the Administration GUI client.

Step 2 In the User Access Role for Events GUI Client drop-down list, select a role and click **Apply**.

Step 3 Restart the gateway for your changes to take effect. See Stopping and Restarting Prime Network Components, page 3-17.

Change the Minimum Role for the Administration Client

To change the minimum user access role for the Administration client, you must use the registry editor CLI. This example shows how to change the minimum role to Configurator.

If you want this user to have the same privileges as the default Administrator role, you must also grant the user access to the AllManaged Elements device scope (when you create the user's account).

Step 1 Log into the gateway server as *pnuser*.

Step 2 Run the following commands to change the minimum access role from Administrator to Configurator:

```
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0
site/plugin/BOSPlugin/commands/com.sheer.metromission.plugin.bos.commands.UpdateDeviceP
ackageName
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.GetSuiteUseStatus
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1
avm11/services/plugin/ClientPlugin/isConfiguratorEnabledForAnaManage true
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/plugin/ClientPlugin/eventVisionRole
configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.commands.U
pdateBosManage/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.CreateDevice/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.DeleteDevice/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.CreateAvm/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.DeleteAvm/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.UnloadAvm/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.CreateMC/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.DeleteMC/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BosManagePlugin/commands/com.sheer.metromission.plugin.bosmanage.oldcommand
s.GetSuiteUseStatus/default plugin/default_roles/configurator
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/plugin/BOSPlugin/commands/com.sheer.metromission.plugin.bos.commands.UpdateDeviceP
ackageName/default plugin/default_roles/configurator
```

Step 3 Restart the gateway for your changes to take effect. See Stopping and Restarting Prime Network Components, page 3-17.

Configuring External User Authentication (LDAP)

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.

User authentication is managed either 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 into Prime Network. If you use Prime Network, user information and passwords are stored in the Prime Network Oracle database. If you use an external LDAP application, passwords are stored on the external LDAP server. (User authorization information (roles and scopes) is always stored in the Prime Network Oracle database. The external LDAP server, if used, only stores passwords.) The external authentication method has a special user called the *emergency user*. In Prime Network, root is designated as the external authentication emergency user. This means if Prime Network loses communication with the LDAP server, Prime Network will allow root (and only root) to log in. The root user can then change the authentication method to local, and edit user accounts so that those users can subsequently log in. Prime Network uses LDAP version 3.

User authorization is managed through a combination of user access roles and scopes. For detailed information on these topics, see User Authentication, page 7-2, and What Are Device Scopes?, page 6-1.

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 Oracle database. If you want to use external authentication, these topics will guide you through the process.

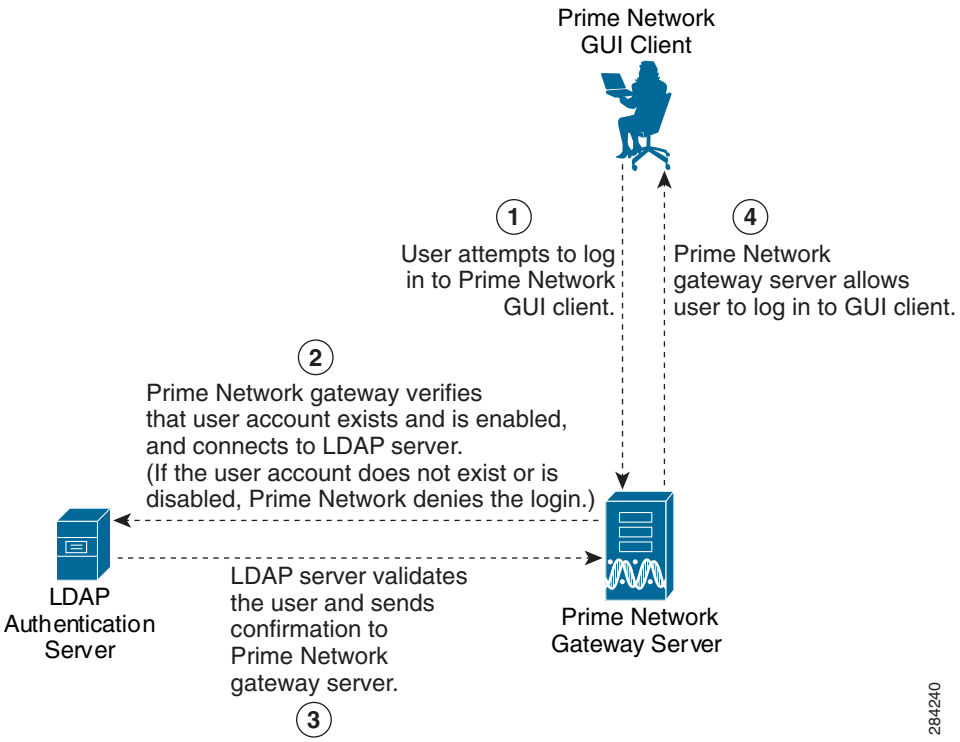
How Does External Authentication Work?

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 Oracle database). The external authentication server only stores login and password information; information pertaining to user roles and scopes is stored in the Prime Network Oracle database.

As illustrated in Figure 7-2, 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 into Prime Network. From that point on, the user can perform functions and access network elements as specified by their roles and scopes (see Changing a User's Device Scope Security Level, page 6-5).

Figure 7-2 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 7-16
- 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 7-17.

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.

Note This procedure requires a gateway restart.

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
```

Step 6 Restart the prime network gateway:

```
# anactl restart
```

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 4.1 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.

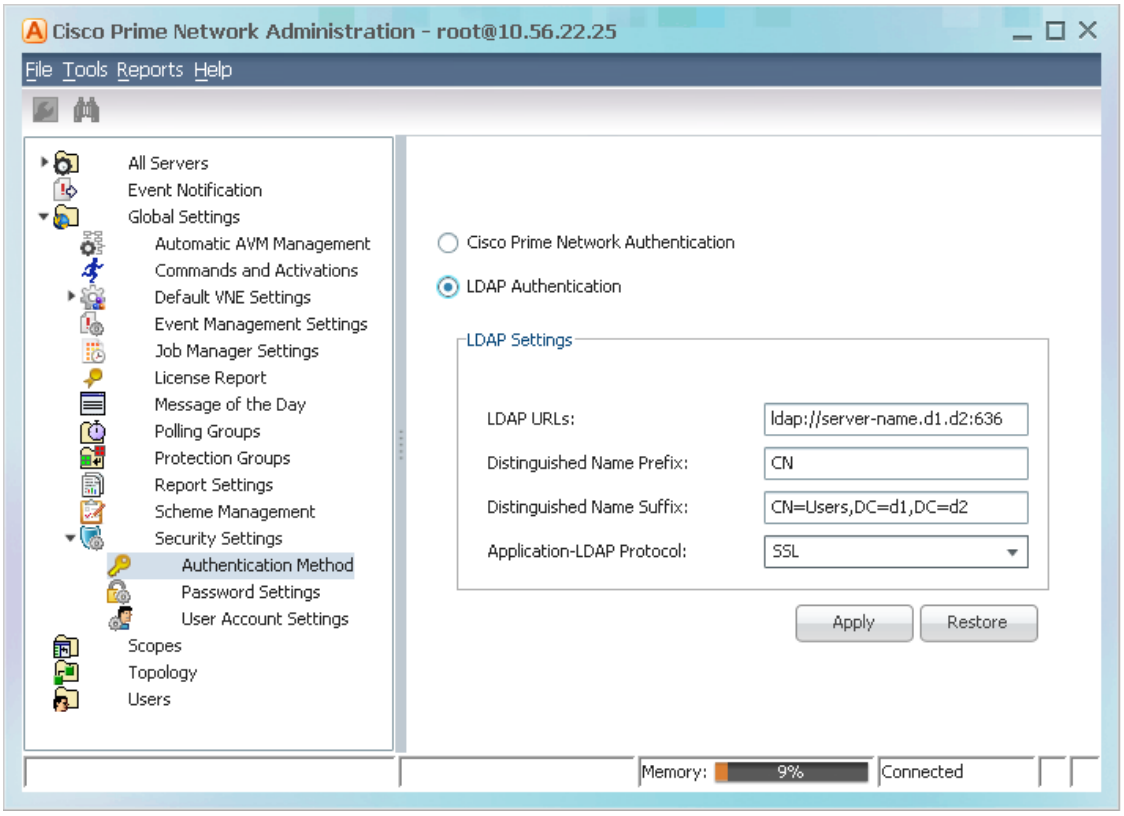
You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Note This procedure requires a gateway restart.

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

Step 1 Choose **Global Settings > Security > Authentication Method**. Figure 7-3 provides an example of the Authentication Method window.

Figure 7-3 Authentication Method Window



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 7-5 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.)
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**

Table 7-5 LDAP Authentication Method Settings (continued)

Field	Description
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 (refer to the *Cisco Prime Network 4.1 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 Stopping and Restarting Prime Network Components, page 3-17.

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.

To import users from an LDAP server into Prime Network, you must first create and LDAP Data Interchange Format (LDIF) file using the **ldifde** command, and then import the file into Prime Network using the **import_users_from_LDIF_file.pl** command.

This command produces an LDIF file for a Windows LDAP server:

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

The following shows sample contents of an LDIF file named **users.LDF**:

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

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

dn: CN=zzz,CN=Users,DC=ldapsj,DC=com
changetype: add
```

```
description: description
displayName: zzz
email: zzz@mail.com
userPrincipalName: zzz@acme.com
```

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*] [*user-email-attribute-name*]

Where:

Argument	Description
ldif-filename	LDIF file name. It should reside in *NETWORKHOME*/Main.
roleName	Prime Network user role: Administrator, Configurator, Operator, OperatorPlus, and Viewer (default=Viewer)
username-attribute-name	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). Mandatory for each user.
user-desc-attribute-name	Attribute name as it appears in the LDIF file. Optional for each user.
full-name-attribute-name	Attribute name as it appears in the LDIF file. Optional for each user.
user-email-attribute-name	Attribute name as it appears in the LDIF file. Optional for each user.

The following command imports the LDAP users listed in the **users.LDF** file into Prime Network. It creates three users with a Viewer role. It is executed from the *NETWORKHOME*/Main/scripts directory.

```
# import_users_from_LDIF_file.pl users.LDF userPrincipalName description displayName
email
```

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 Changing User Accounts and Device Scope Access, page 7-11.

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

Note This procedure requires a gateway restart.

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 Stopping and Restarting Prime Network Components, page 3-17.

Step 5 Reconfigure user accounts accordingly (see Changing User Accounts and Device Scope Access, page 7-11).

Controlling Which Maps Users Can Access

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

By default, users can access any Vision GUI client maps that have been created by other users. You can control this by enabling the map assignment mechanism.

Note This procedure requires a gateway restart.

Step 1 Enable the map assignment mechanism.

a. Choose **Tools > Registry Controller > User Accounts** from the main menu of the Administration GUI client.

b. In the User Access to Existing Maps setting, select **True** from the drop-down list and click **Apply**.

c. Restart the gateway for your changes to take effect. See Stopping and Restarting Prime Network Components, page 3-17.

Step 2 Specify which maps users can access:

a. In the Users tree in the Administration GUI client, right-click a user and choose **Properties**.

b. Click the **Maps** tab. The Maps tab lists all maps saved in the Oracle database. Those that are not assigned to the user are listed on the left.

c. To assign maps to the user account, move them from the left side to the right side, and click **OK**.

Re-enabling User Accounts

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

User accounts can become locked or disabled for two reasons:

- A user entered the wrong password, exceeding the number of permitted retries. The retries setting is controlled from the Password Settings window.
- The user has not logged in, exceeding the account inactivity period.

The settings that control these actions are specified in the Global Settings; see Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.

To reenable a locked account:

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 In the Account tab, check the Enable Account check box.

Step 4 Save your changes.

Deleting a Prime Network User Account

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

If you want to disable a user account but not delete it, see Changing User Accounts and Device Scope Access, page 7-11.

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.

Tracking User-Related Events

The following table provides ways you can get historical information on user-related events. You can tailor your search or reports by specifying keywords (such as *user*).

For historical events related to:	See:
User accounts that were created, edited, or deleted Login issues such as failed logins Account inactivity events Map permission issues	Security events report, which you can launch from the main menu by choosing **Reports > Run Report > Events Reports > Detailed Non-Network Events > Detailed Security Events**