



User Management

This chapter provides an overview of the Cisco PTC user authentication and authorization procedures and also describes how system administrators can use the User Manager application to add, delete, and modify user information in the Cisco PTC system. The User Manager services are provided through the Cisco Networking Services (CNS) Security Services Administration server. See the [“Accessing the User Manager”](#) section on page 6-3 for a detailed description of the User Manager services that are provided through the CNS Security Services Administration server.

This chapter is organized into the following sections:

- “User Management Overview”
 - “Cisco PTC User Groups”
 - “Security Services”
- “Accessing the User Manager”
 - “Logging In to the CNS Security Services Administration Server”
 - “CNS Security Services Administration Welcome Window”
- “CNS Security Services Administration Tasks”
 - “Creating a User”
 - “Adding a User to a Group”
 - “Deleting a User”
 - “Modifying User Attributes”
 - “Changing a User Password”
 - “Changing Your Own Password”

User Management Overview

User *authentication* is the verification of the credentials of a user. User *authorization* determines the user's privileges and provides access control to the managed resources. User privileges essentially define the scope of managed resources upon which a user has the right to perform a set of operations upon successful authentication.

Cisco PTC provides user authentication and authorization as part of its overall security management.

For Cisco PTC, user privileges are classified into the following categories:

- system management privileges:
 - system startup and shutdown
 - system configuration and tuning
- user management privileges:
 - create, change, remove, and view users
- network resource management privileges:
 - create, change, remove, and view logical network entities, such as, regions, zones, virtual gateways, signal paths, and dial plans
 - create, change, remove, and view physical network entities, such as, network elements, cards, and voice ports.

A user can be given the network resource management privileges to one or more management scopes. In Cisco PTC, a management scope can be the H.323 voice network and a region.

Cisco PTC User Groups

All Cisco PTC users belong to one of the following user groups:

- System administrators
- Regional network operators
- Non-administrative users



Note

When Cisco PTC is installed for the first time, a default System Administrator (**DemoSysAdmin1**) is available. As a system administrator, the **DemoSysAdmin1** user can create additional users of various types through the CNS Security Services Administration Server window.

System Administrators

A user with system administrator privileges has *control over all aspects of the network and has write privileges in all groups*. The system administrator can:

- add system administrators, regional network operators, and non-administrative users to the system
- remove system administrators, regional network operators, and non-administrative users from the system
- add regional network operators to different security groups in different regions
- change the user password of system administrators, regional network operators, and non-administrative users.

Regional Network Operators

A user with regional network operator privileges has no user management capabilities. A regional network operator *can read, write, and provision only in the regions where they are authorized*.

The regional network operator *cannot*:

- add new system administrators and non-administrative users to the system
- remove system administrators and non-administrative users from the system
- change the user password of system administrators and non-administrative users.

Non-Administrative Users

A non-administrative user has *read only* privileges which allows them to view the network topology and device configurations of all regions. Therefore, a non-administrative user cannot add, delete, or change the passwords of system administrators, regional network operators, or other non-administrative users.

Security Services

Cisco PTC is integrated with the CNS Security Services Administration server. The CNS Security Services Administration server provides an authentication and authorization framework based upon the Role Based Access Control (RBAC) model. This framework provides features such as authentication, authorization, and security administration. The CNS Security Services Administration server processes the policy rules represented in an LDAP v3 directory to determine the entitlements and privileges granted to various roles (and role occupants).

The Cisco PTC Topology Manager, Provisioning Manager, and AutoDiscovery process all use the security services provided by the CNS Security Services Administration server.

**Note**

The CNS Security Services Administration server is installed as part of the Cisco PTC installation process.

Accessing the User Manager

You obtain access to the User Manager by clicking on the **User Management** button in the Cisco PTC Launch Pad window. The User Management functionality is provided through the CNS Security Services Administration server.

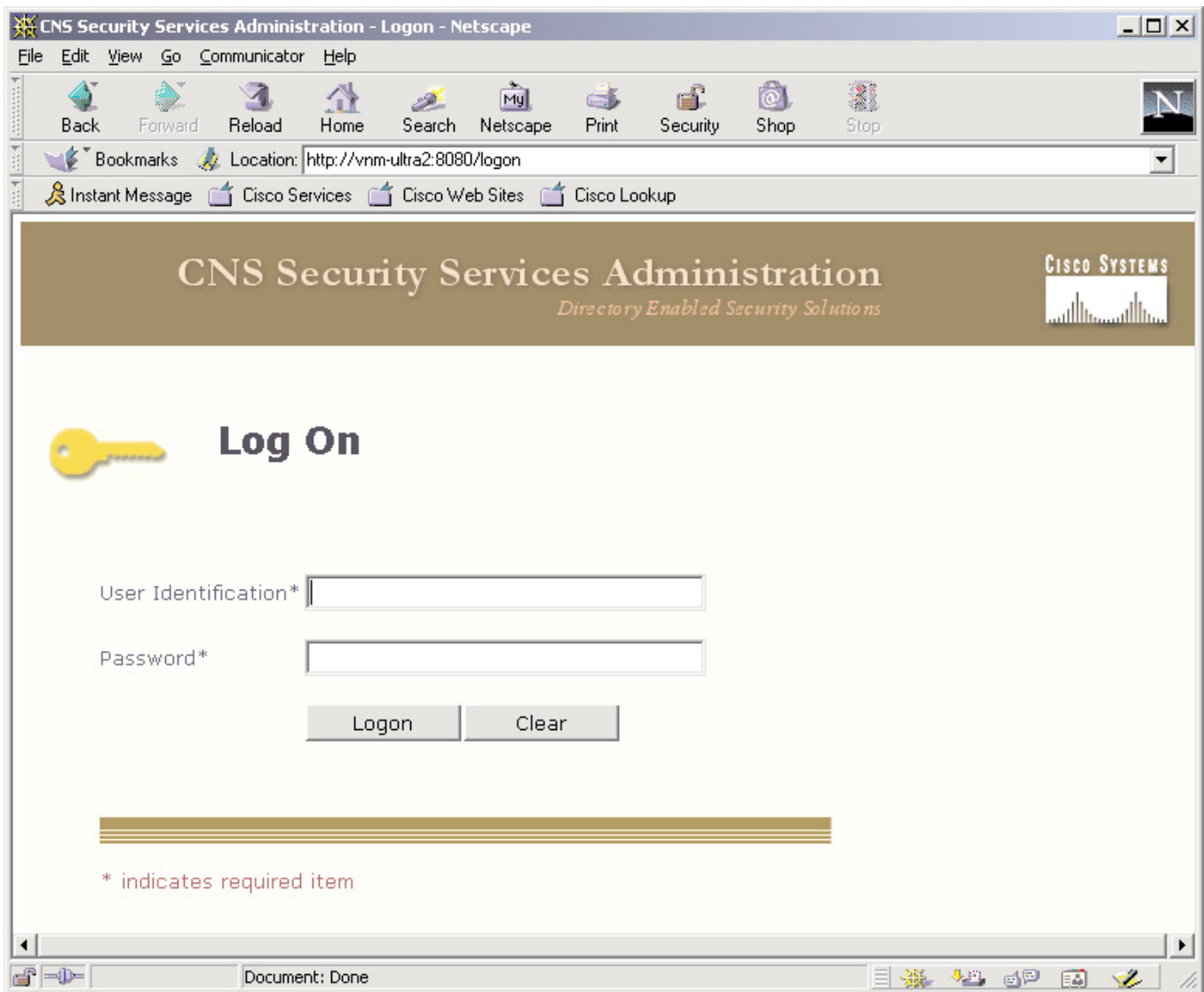
The CNS Security Services Administration server allows you to:

- create a new user
- clone a user
- delete a user
- add a user to one or multiple user groups
- delete a user from one or multiple user groups
- change user passwords.

Logging In to the CNS Security Services Administration Server

To obtain access to the CNS Security Services Administration server, you must first login through the CNS Security Services Administration Logon window, shown in Figure 6-1. You are prompted to enter a username and password. The username and password are then authenticated by the CNS Security Services Authentication Service.

Figure 6-1 CNS Security Services Administration Logon Window



75358

CNS Security Services Administration Welcome Window

Upon successfully logging in to the CNS Security Services Administration server, a CNS Security Services Administration Welcome window appears. By default, the CNS Security Services Administration server is started in *Normal* mode. Using this tool in normal mode is sufficient for Cisco PTC's needs. This CNS Security Services Administration Welcome window provides:

- version, product, and copyright information
- menu options that allow you to navigate through different user-interfaces.



Note

You can use the CNS Security Services Administration server in either *Expert* or *Normal* mode. Expert mode provides additional features and functionality that are beyond the needs of Cisco PTC. You are in expert mode when the **Normal Mode** link is displayed in the upper right corner of the CNS Security Services Administration Welcome window, as shown in Figure 6-2. If you see an **Expert Mode** link displayed in this window, click on the link to enter expert mode.

Figure 6-2 CNS Security Services Administration Welcome Window



75360

User Management Menu Options

This menu provides the following options:

- **User Configuration**
- **User Group Configuration**

**Note**

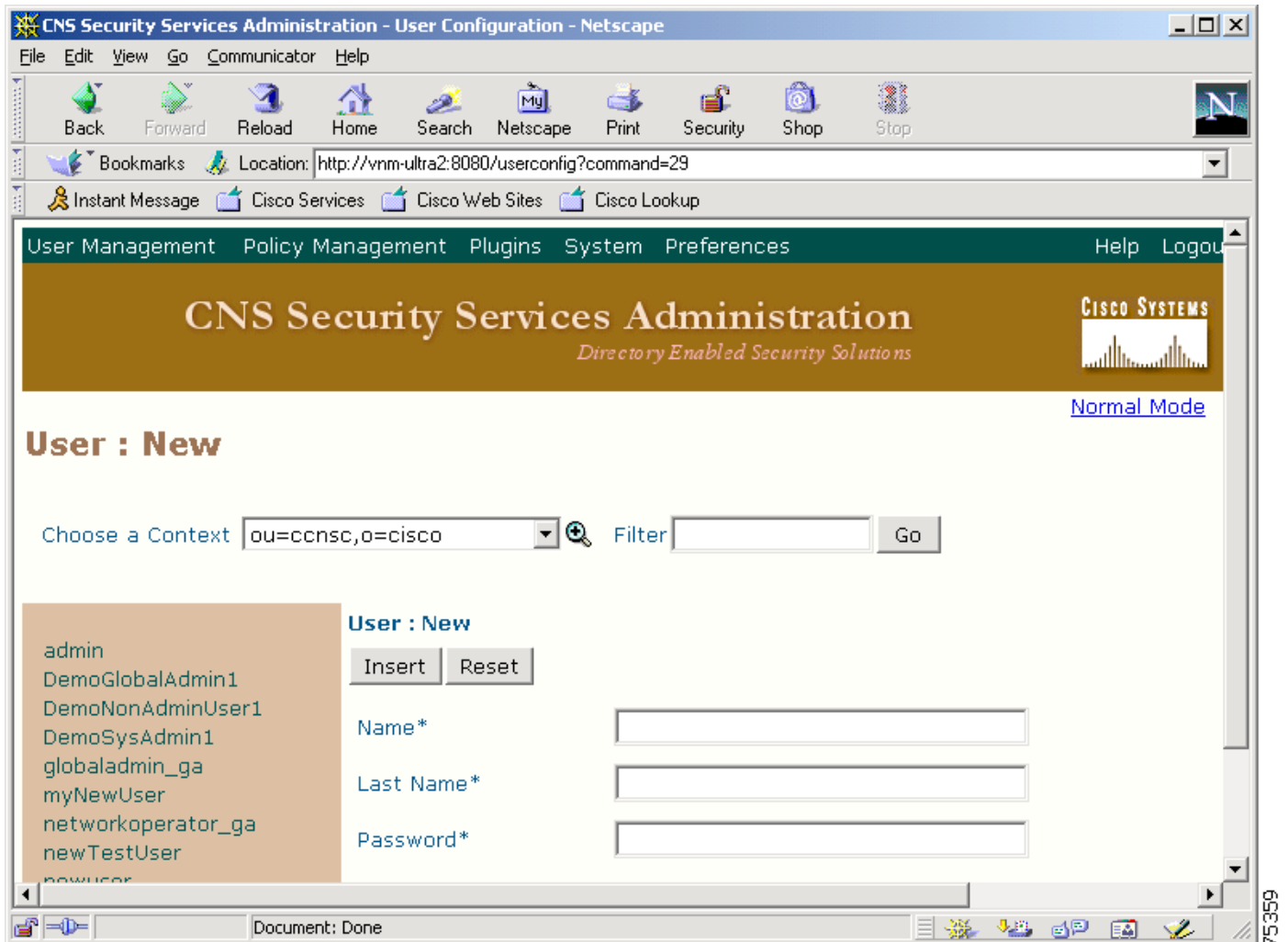
The **User Group Configuration** option has no relevance to Cisco PTC. Therefore, it is strongly recommended that you do not invoke this option when using Cisco PTC.

User Configuration Option

When you choose the **User Configuration** menu option, a list of known users is displayed in a pane on the left side of the window, as shown in [Figure 6-3](#). When you select a user from this list, the window is populated with the details (name, password, E-mail address, and home phone number) about the selected user. With the proper permissions, you can modify the user profile, clone the user configuration parameters under a new unique username, and delete the user, from this window.

You can also add a new user through this window. You must enter a unique username, the user's last name, and a password in their respective text fields.

Figure 6-3 CNS Security Services Administration User Configuration Window



User Group Configuration Option

The **User Group Configuration** option has no relevance to Cisco PTC. Therefore, *it is strongly recommended that you do not invoke this option* when using Cisco PTC.

Policy Management Menu Options

The **Policy** menu options have no relevance to Cisco PTC. Therefore, *it is strongly recommended that you do not invoke these options* when using Cisco PTC.

Plug-ins Menu Options

The **Plug-ins** menu option has no relevance to Cisco PTC. Therefore, *it is strongly recommended that you do not invoke this option* when using Cisco PTC.

System Menu Options

The **System** menu option has no relevance to Cisco PTC. Therefore, it is strongly recommended that you do not invoke this option when using Cisco PTC.

Preferences Menu Options

This menu allows you to provides the following options:

- **My Profile**
- **Change Password.**

My Profile Option

This menu option allows you to edit your personal profile. You can edit your first and last names, your E-mail address, and your home phone number. Upon completing your editing, click **Update** to have the changes take effect. Click **Reset** to discard your current modifications and return to the settings that were in effect when you chose this menu option.

Change Password Option

This menu option allows you to change your password. You are required to enter your current password in order to change it. Upon editing your current password, click **Update** to have the new password take effect. Click **Reset** to discard your current modifications and have your current password reapplied.

CNS Security Services Administration Tasks

This section describes how to use the CNS Security Services Administration window to accomplish the following tasks:

- create a new user
- add a user to a group
- delete a user
- modify an existing users profile
- change an existing user's password.

Creating a User

Only system administrators can add users (system administrators, regional network operators, and non-administrative users) to the system. See the [“Cisco PTC User Groups” section on page 6-2](#) for a detailed list of the capabilities of the various user types.

-
- Step 1** Log in to the Cisco PTC system as a system administrator.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
The CNS Security Services Administration Log On window is displayed.

- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **User Management > User Configuration** menu option.
- Step 5** Enter a unique user name, last name, and password in their respective fields, then click **Update**.
The username you specified is now added to the list of usernames displayed in the CNS Security Services Administration window.
- You can now add your E-mail address and home phone number to your user profile and modify your existing user profile settings. You can also add this username to an existing group.
-

Adding a User to a Group

Only system administrators can add users (system administrators, regional network operators, and non-administrative users) to a group.

- Step 1** Log in to the Cisco PTC system as the system administrator.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
The CNS Security Services Administration Log On window is displayed.
- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **User Management > User Configuration** menu option.
- Step 5** Select the username you want to add to a group from the list of usernames displayed in the CNS Security Services Administration window.
Information pertaining to the selected username is now displayed.
- Step 6** You can search for a specific group by entering its name in the **Filter** text field and then click **Go**, or you can click the **Add to Group** button.
The Select User Group window appears.
- Step 7** Select one or more groups from the list of group names in the left pane, then click the right arrow button.
The selected group names are added to the right pane.
- Step 8** Click the **Insert and Close** button.
The Select User Group window is closed and the username is added to the selected groups.
-

Deleting a User

Only system administrators can delete users (system administrators, regional network operators, and non-administrative users) from the system.

- Step 1** Log in to the Cisco PTC system.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
The CNS Security Services Administration Log On window is displayed.

- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **User Management > User Configuration** menu option.
- Step 5** Select the username you want to delete from the list of usernames displayed in the CNS Security Services Administration window.
- Step 6** Click **Delete**.

The user you specified is deleted and no longer has access to the Cisco PTC system.

Modifying User Attributes

Only system administrators can modify the user attributes (first name, last name, E-mail address, home phone number) of all types of users (system administrators, regional network operators, and non-administrative users). The other user types are restricted as to the types of users they can modify attributes. See the [“Cisco PTC User Groups” section on page 6-2](#) for a detailed list of the modification capabilities of the various user types.

- Step 1** Log in to the Cisco PTC system.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
The CNS Security Services Administration Log On window is displayed.
- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **User Management > User Configuration** menu option.
- Step 5** Select the username you want to modify attributes for from the list of usernames displayed in the CNS Security Services Administration window.
Information pertaining to the selected username is now displayed.
- Step 6** Modify the attributes you wish to change in their respective text fields, then click **Update**.

The modifications you specified are now in effect.

Changing a User Password

Only system administrators can change user passwords.

- Step 1** Log in to the Cisco PTC system.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
The CNS Security Services Administration Log On window is displayed.
- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **User Management > User Configuration** menu option.

- Step 5** Select the username you want to change the password for from the list of usernames displayed in the CNS Security Services Administration window.
- Information pertaining to the selected username is displayed.
- Step 6** Enter a new password in the **Password** text field, confirm the password in the **Confirm Password** text field, then click **Update**.
- The new password you specified is now in effect.
-

Changing Your Own Password

This section describes how to change your own password.

- Step 1** Log in to the Cisco PTC system.
- Step 2** Click the **User Management** button in the Cisco PTC Launch Pad window.
- The CNS Security Services Administration Log On window is displayed.
- Step 3** Enter your username and password in their respective fields, then click **Logon**.
- Step 4** Choose the **Preferences > Change Password** menu option.
- Step 5** Enter a new password in the **Password** text field, confirm the password in the **Confirm Password** text field, then click **Update**.
- The new password you specified is now in effect.
-

