

Resource: How to Add Users to CSACS-NT

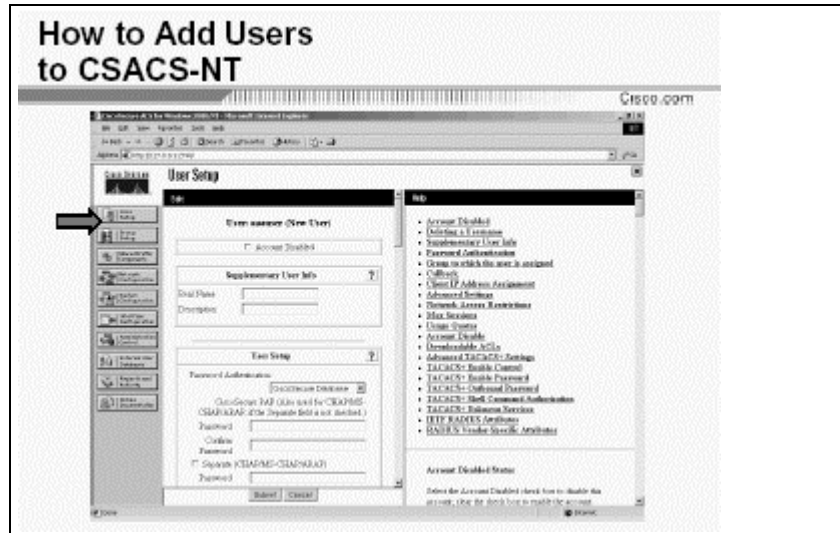


Figure [1] Users setup screen on Windows version of Cisco Secure ACS

The following process illustrates how to add users to the CSACS. An explanation of each of the windows where that account can be edited is then provided.

Step 1 Click **User Setup** from the navigation bar. The Select window opens.

Step 2 Enter a name in the User field.

Note The username can contain up to 32 characters. Names cannot contain the following special characters: #, ?, ", *, >, and <. Leading and trailing spaces are not allowed.

Step 3 Click **Add/Edit**. The Edit window opens. The username being added or edited appears at the top of the window.

The Edit window contains the following sections:

- Account Disabled

- Supplementary User Info
- User Setup
- Account Disable

Account Disabled

If you need to disable an account, select the Account Disabled check box in the Account Disabled section to deny access for this user.

Note You must click Submit to have this action take effect.

Supplementary User Info

In this section, you can enter supplemental information to appear in each user profile. The fields shown below are available by default. However, additional fields may be inserted by clicking **Interface Configuration** in the navigation bar and then click **User Data Configuration** (configuring supplemental information is optional):

- **Real Name**—If the username is not the real name of the user, enter the real name here.
- **Description**—Enter a detailed description of the user.

User Setup

In the User Setup group box, you can edit or enter the following information for the user as applicable:

- **Password Authentication**—From the drop-down menu, choose a database to use for username and password authentication. Select the Windows NT user database or the Cisco Secure database. The Windows NT option authenticates a user with an existing account in the Windows NT user database located on the same machine as the CSACS server. The Cisco Secure database option authenticates a user from the local CSACS database. If you select this database, enter and confirm the Password Authentication Protocol (PAP) password to be used. The separate CHAP/MS-CHAP/ARAP option is not used with the PIX Security Appliance.

Note: The Password and Confirm Password fields are required for all authentication methods except for all third-party user databases.

- Group to which the user is assigned—From the Group to which the user is assigned drop-down menu, choose the group to which to assign the user. The user inherits the attributes and operations assigned to the group. By default, users are assigned to the Default Group. Users who authenticate with the Unknown User method who are not found in an existing group are also assigned to the Default Group.
- Callback—This is not used with the PIX Security Appliance.
- Client IP Address Assignment—This is not used with the PIX Security Appliance.

Account Disable

The Account Disable group box can be used to define the circumstances under which the user account will become disabled.

Note: This is not to be confused with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

- Never radio button—Select to keep the user's account always enabled. This is the default.
- Disable account if radio button—Select to disable the account under the circumstances you specify in the following fields:
 - Date exceeds—From the drop-down menu, choose the month, date, and year on which to disable the account. The default is 30 days after the user is added.
 - Failed attempts exceed—Select the check box and enter the number of consecutive unsuccessful login attempts to allow before disabling the account. The default is 5.
 - Failed attempts since last successful login—This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.
- Reset current failed attempts count on submit—If an account is disabled because the failed attempts count has been exceeded, select this check box and click **Submit** to reset the failed attempts counter to 0 and reinstate the account.

If you are using the Windows NT user database, this expiration information is in addition to the information in the Windows NT

user account. Changes here do not alter settings configured in Windows NT.

When you have finished configuring all user information, click **Submit**.