Appendix 8.4.4b Configuring Cisco ACS

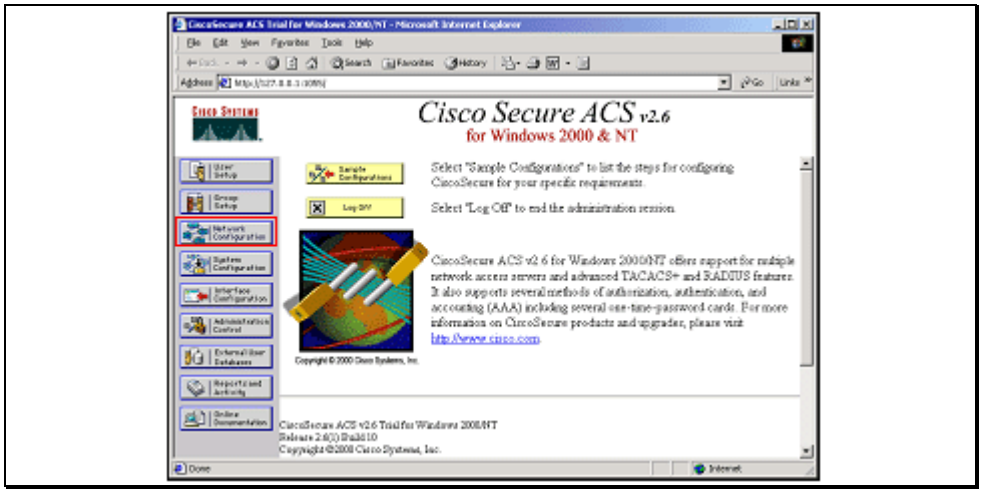

Figure [1]: Cisco ACS Main Screen

To begin configuring Cisco Access Control Server (ACS) to work with Cisco Aironet Access Points as network access servers (NASs), open the Cisco ACS main screen. From the navigation bar click the **Network Configuration** button. This will launch the Network Configuration screen.

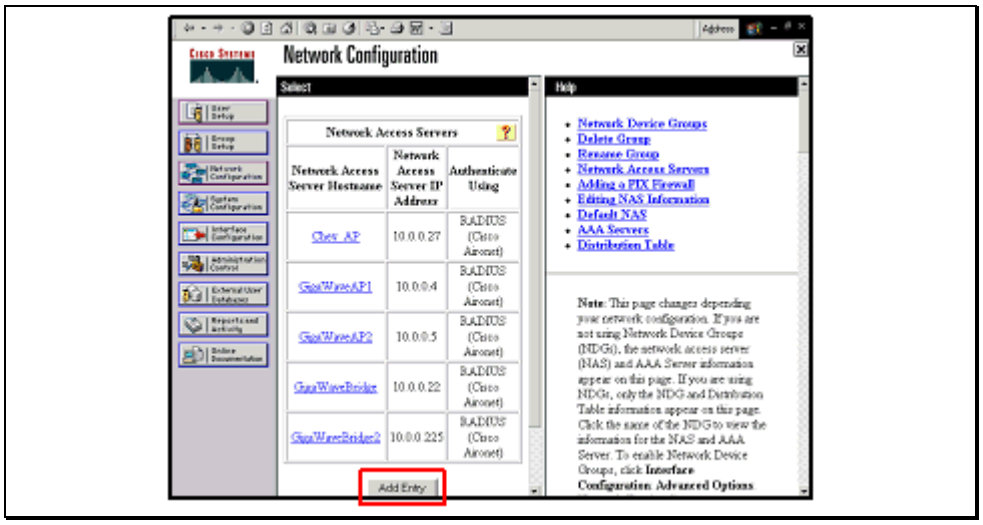

Figure [2]: Network Configuration

The Network Configuration screen lists all NASs that are currently configured. To add a NAS, click the **Add Entry** button. This will launch the Add Access Server screen.

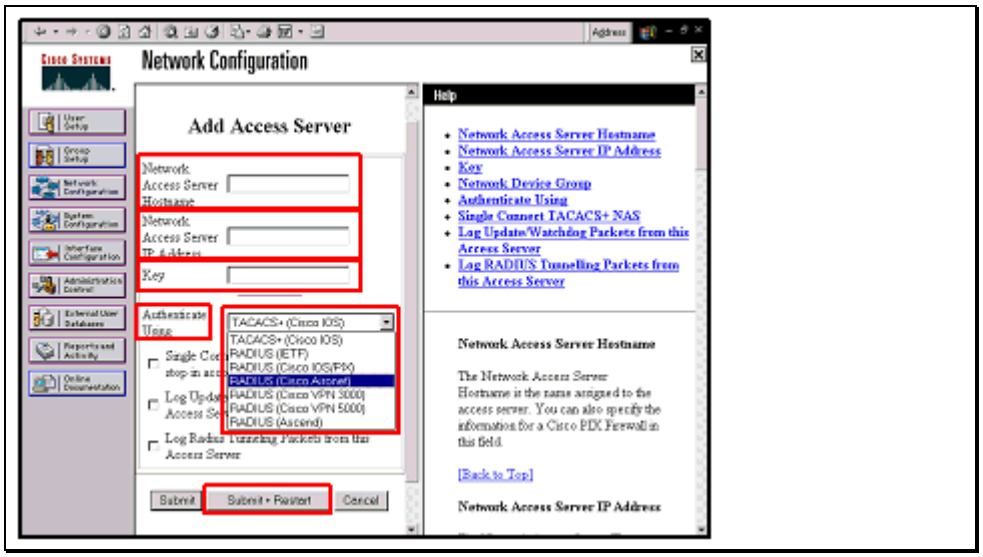

Figure [3]: Access Server Setup Example

To configure Cisco ACS for use with the Cisco Aironet product as a NAS, perform the following.

On the left side of screen of the ACS menu, click on the **Network Configuration** button, then click **ADD Access Server**. This will bring up the Add Access Server screen.

Each individual access point is considered a network access server (NAS). To configure a NAS, enter the following:

- **Network Access Server Hostname -** Domain Name System (DNS) name of the specified access point
- **Network Access Server IP Address -** IP address of the specified access point
- **Key -** Shared secret between the server and this individual access point
- **Authenticate Using -** Must select “RADIUS (Cisco Aironet)”

Each key can be different on a per access point basis but must match the setting in the specified access point.

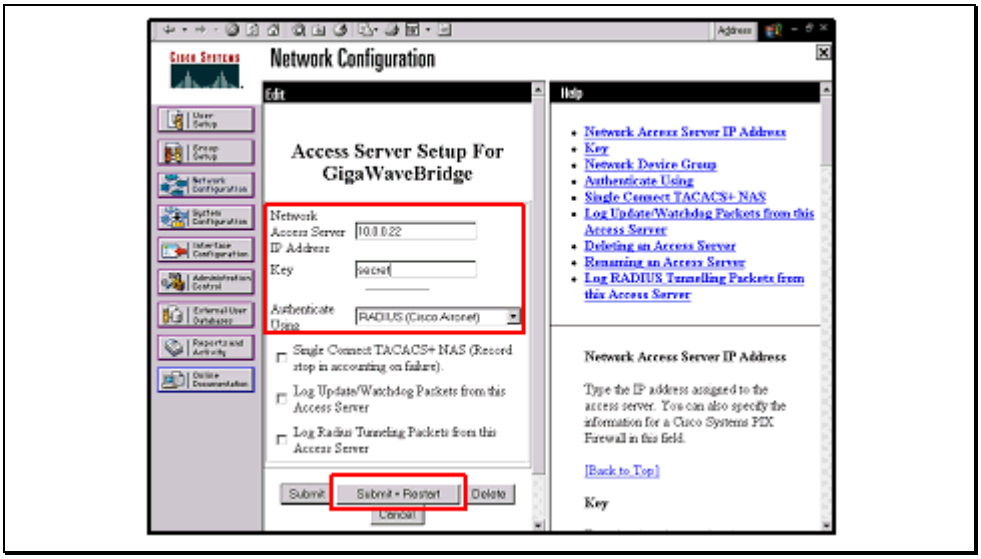

Figure [4]: Access Server Setup Example (Cont.)

When finished configuring the NAS, click the **Submit+Restart** button. Cisco ACS is now ready to receive authentication requests through the NAS.

Figure [5]: External User Database

Configuring a Windows NT/2000 External User Database

Perform the following to configure Cisco Secure ACS to authenticate users against the Windows NT/2000 user database in a network trusted domains.

In the navigation bar click **External User Databases**.

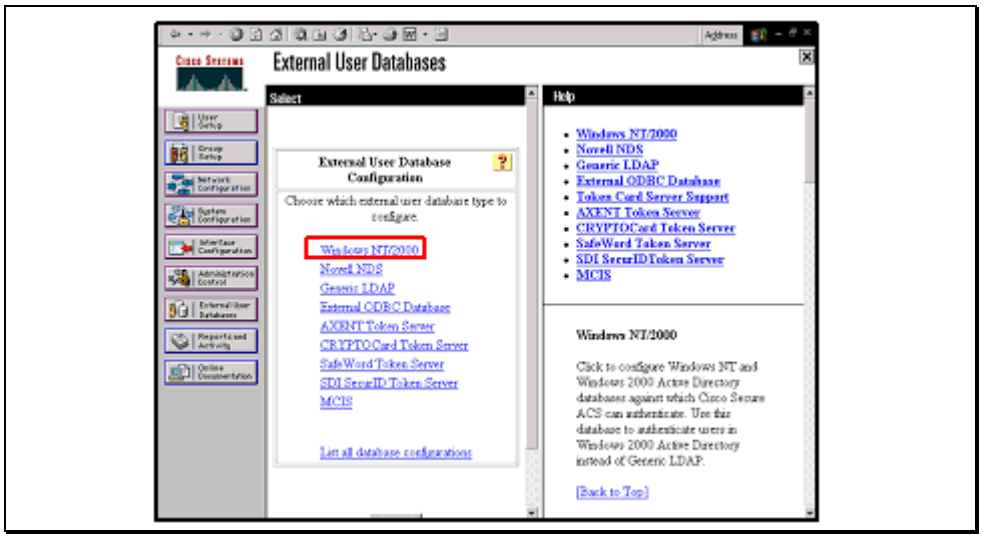

Figure [6]: External User Database: Windows NT/2000

Click on the **Windows NT/2000** link. This will launch the External User Database Configuration screen.

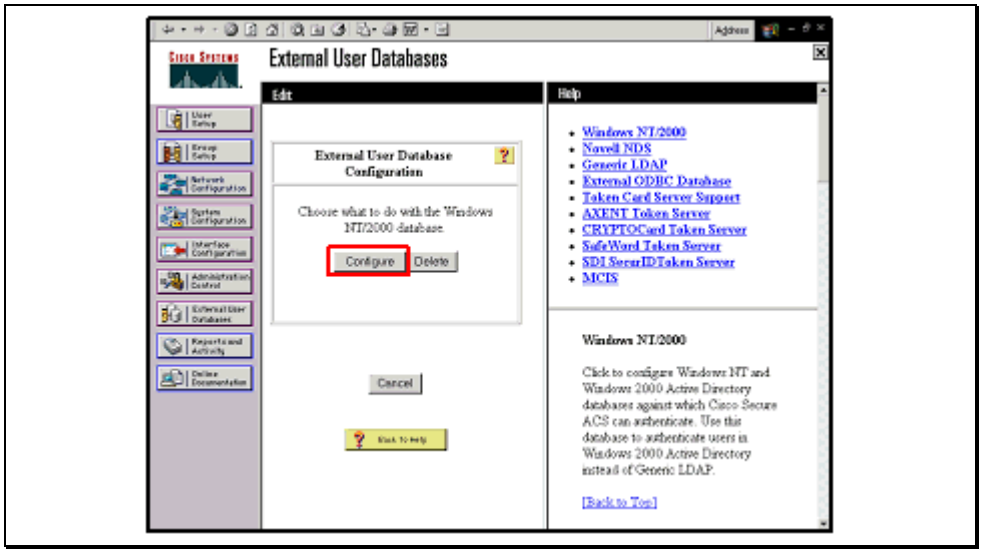

Figure [7]: Windows NT/2000 Database (Cont.)

Click the **Configure** button. This will launch the Windows NT/2000 User Database Configuration screen.

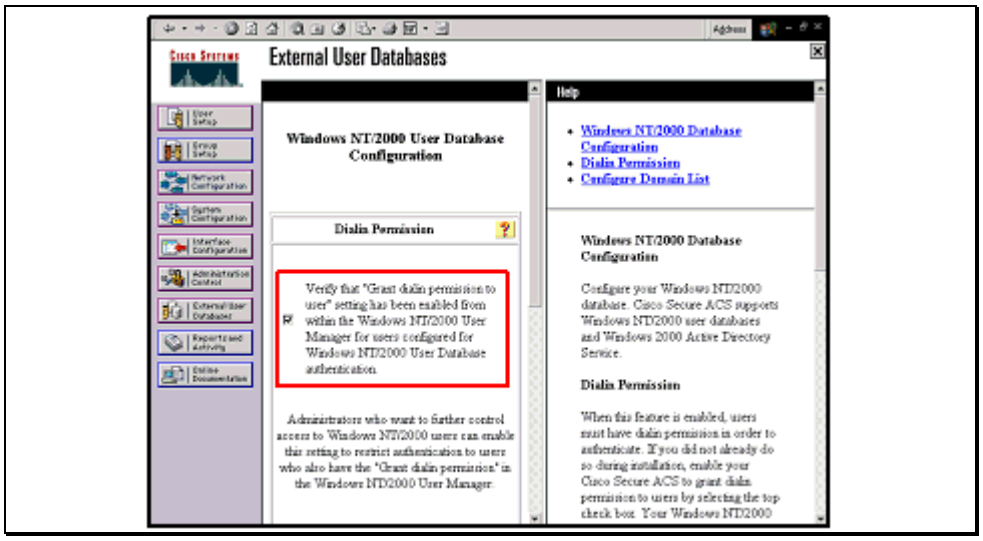

Figure [8]: Windows NT/2000 Database Configuration

To restrict network access to users who have Windows dial-in permission, select the "**Verify that Grant dial in permission**…" check box.

Note	Windows dial-in permission is enabled in the Dial-in section of user properties in Windows NT and on the Dial-in tab of the user properties in Windows 2000.

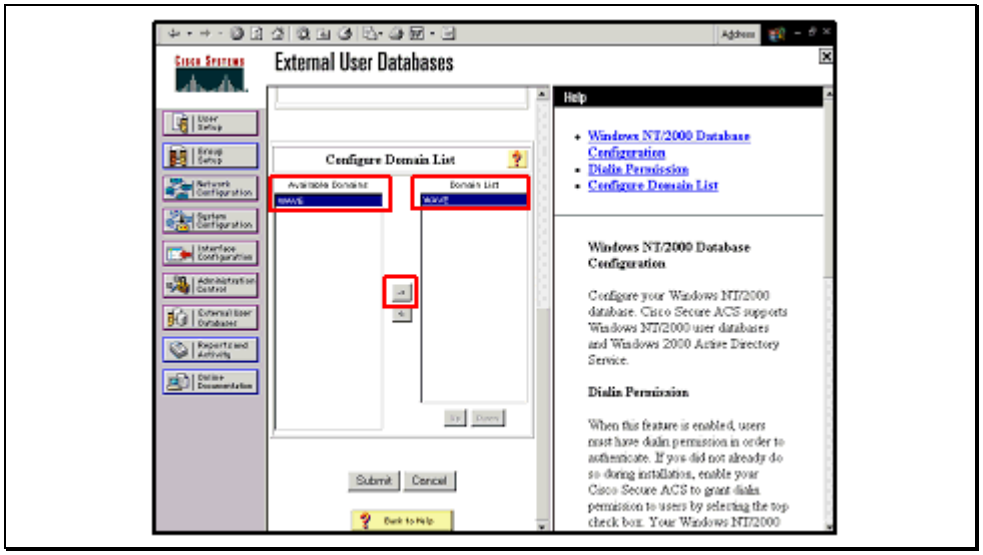

Figure [9]: Windows NT/2000 Database, Configure Domain List

It is important that Cisco Secure ACS authenticates the use of each trusted Windows domain for usernames that are not domain-qualified. Perform the following steps as shown in the Figure [9], to authenticate unqualified usernames:

- In the **Available Domains** list select or highlight the domains
- Click the arrow button to move the selected domains to the **Domain List** box.
- Click the **Submit** button.

The Cisco Secure ACS will then save the Windows NT/2000 user database configuration that was created. It is then possible to add it to the **Unknown User Policy** or assign specific user accounts to use this database for authentication.

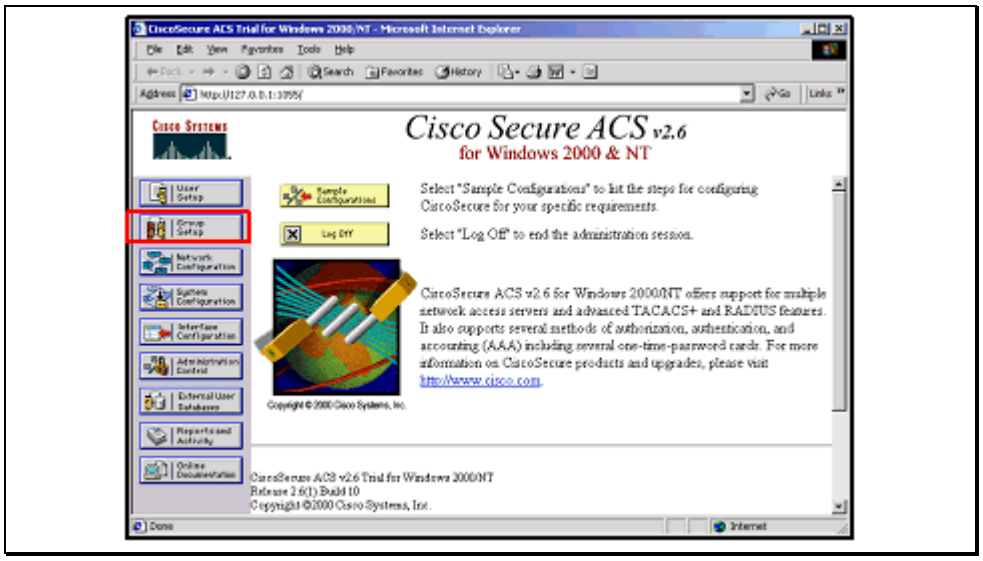

Figure [10]: Session Policy Setup

To adjust the timeout value for the client session requiring re-authentication and new Wired Equivalent Privacy (WEP) key derivation, click the **Group Setup** button form the ACS main screen. This will launch the Group Setup screen.

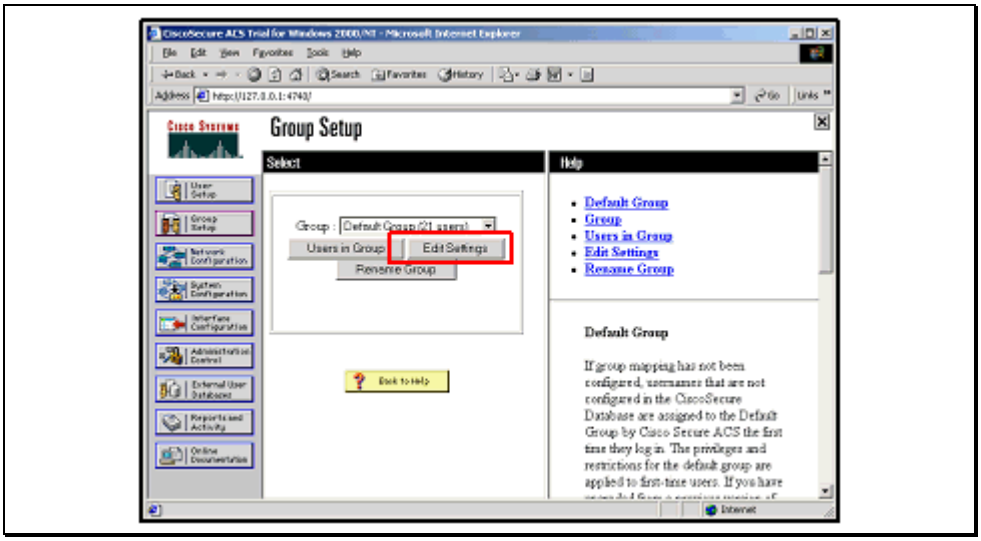

Figure [11]: Session Policy Setup

From the Group Setup screen, choose a group, usually the default group, and click the **Edit Settings** button.

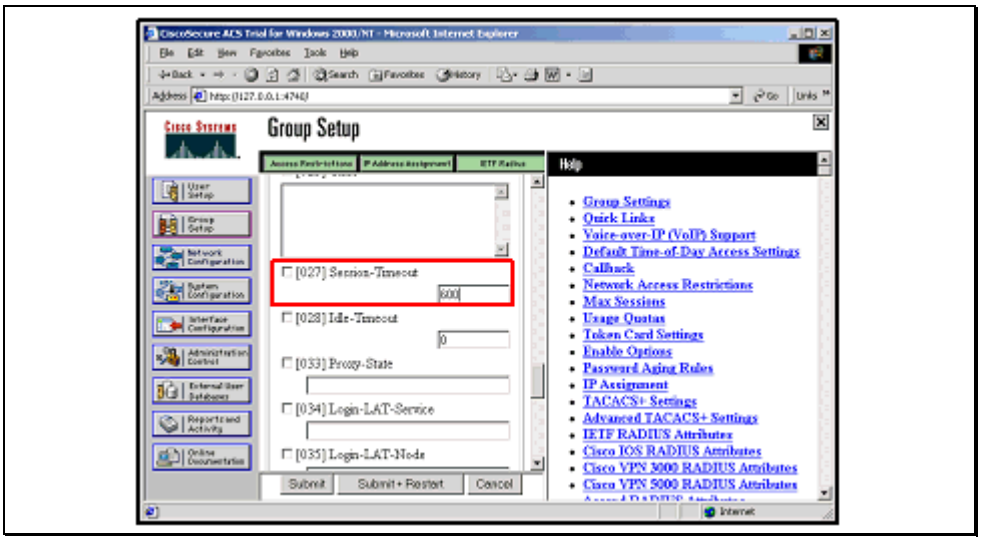

Figure [12]: Session Policy Setup (Cont.)

Scroll down through the setup menu and find the **[027] Session Timeout** entry. Enter the timeout value in seconds. The timeout value will depend upon the number of users typically attached to the access point, as well as the amount of traffic the clients will typically be sending. The larger the number of users, or the more traffic the users are sending, the smaller the value needs to be to ensure that the wireless LAN (WLAN) is protected. By setting smaller values it is possible to prevent a hacker from being able to capture enough packets to hack a WEP key.

The following are recommended values:

- Using WEP only with 802.1X, key rotation time of 15 minutes
- Using WEP and TKIP with 802.1X key rotation time of 240 minutes

Note	These values apply to both session keys and broadcast key.

When finished click the **Submit+Restart** button.

For help in determining the best session key timeout value, consult *Cisco Product Bulletin 1515: Cisco Wireless LAN Security Bulletin.*

Figure [13]: User Setup in ACS

Cisco ACS can use the Cisco Radius server as the user database or an external user database.

Note	If using the Windows NT/2000 database, all users who should have wireless access must have 'remote access' enabled under their user profile.

To configure accounts on Cisco ACS, click the **User Setup** button from the main screen. This will launch the User Setup screen.

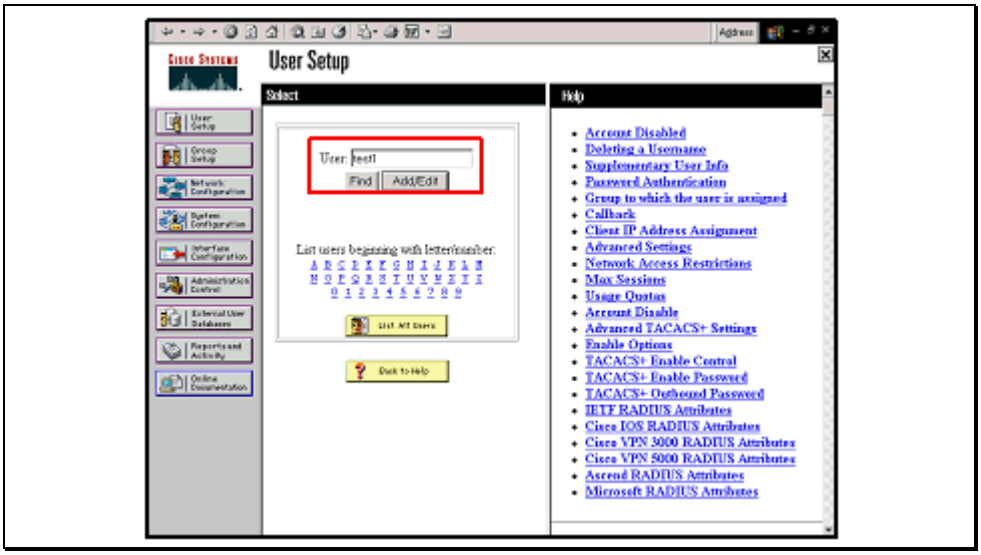

Figure [14]: User Setup in ACS (Cont.)

Cisco ACS can use the Cisco Radius server as the user database or an external user database.

Note	If using the Windows NT/2000 database, all users who should have wireless access must have 'remote access' enabled under their user profile.

To configure accounts on Cisco ACS, click the **User Setup** button from the main screen. This will launch the User Setup screen.

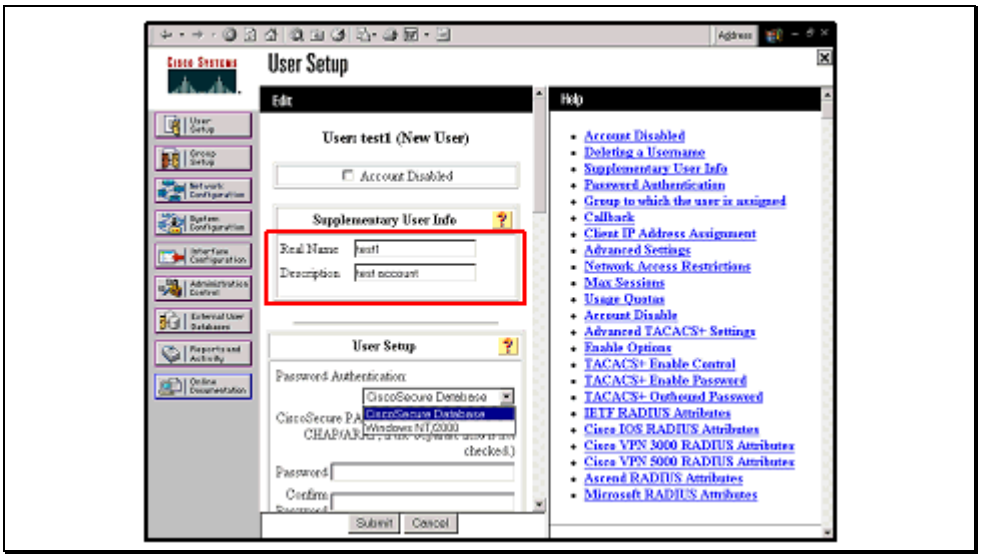

Figure [15]: User Setup in ACS: New User

Enter information about the user as shown in Figure [15]. Enter the real name of the user in the **Real Name** box. Enter a description of the account in the **Description** box.

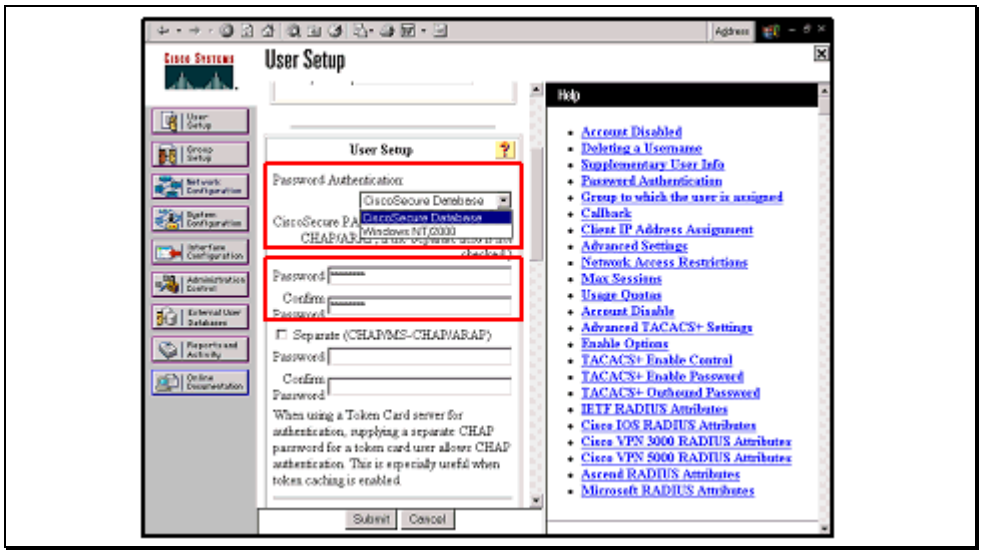

Figure [16]: User Setup in ACS: New User (Cont.)

Scroll down to the **Password Authentication** entry and choose **Cisco Secure Database** form the drop down menu. This indicates that the user account will be stored on Cisco ACS.

Type the password in the **Password** box. Retype the password in the **Confirm Password** box.

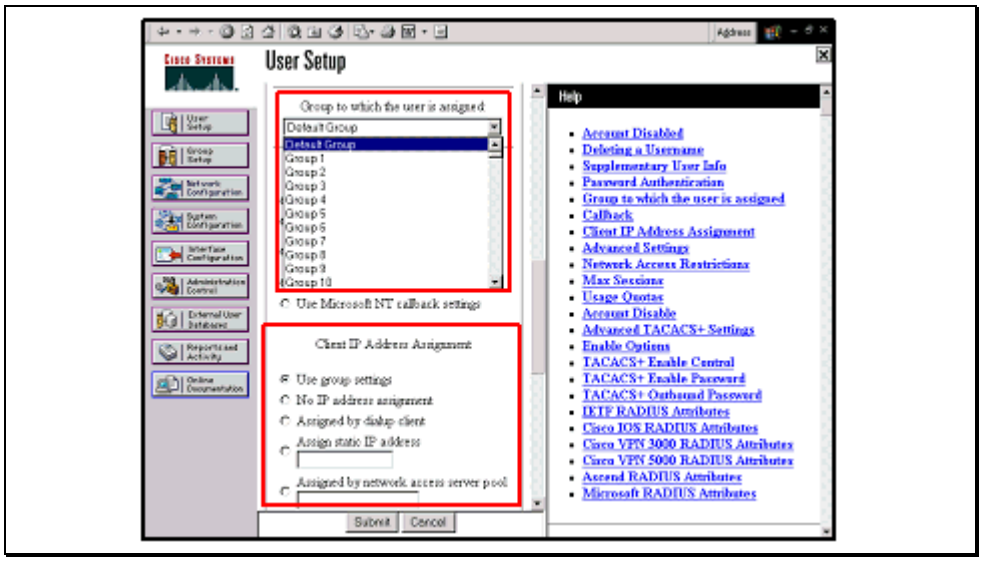

Figure [17]: User Setup in ACS: New User (Cont.)

Scroll down to the **Group to which the user is assigned** box. From the drop down menu, choose which group the user will belong to. Unless otherwise specified, all users are assigned to the **Default Group**.

Scroll down to **Client IP Address Assignment**. Choose how the user will be assigned an IP address.

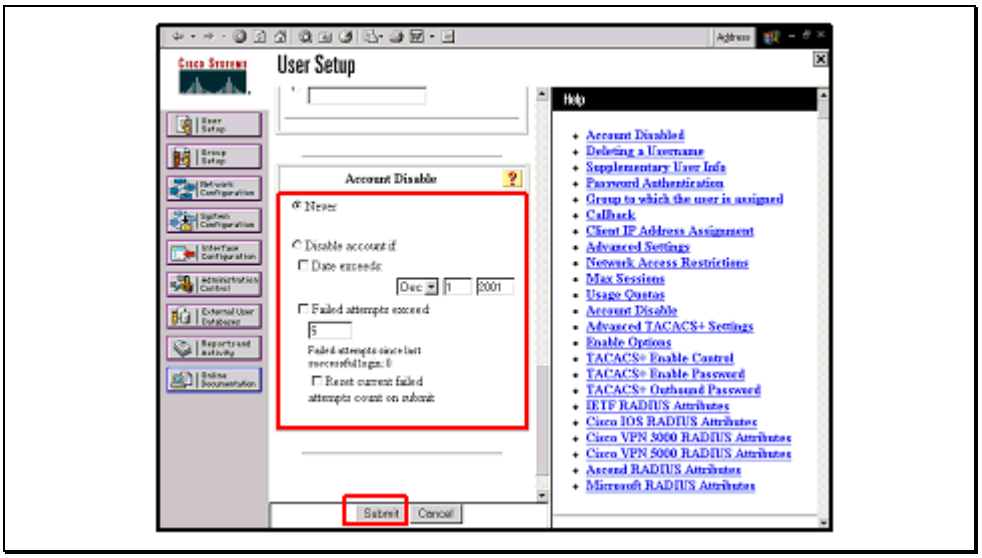

Figure [18]: User Setup in ACS: New User (Cont.)

Scroll down to the **Account Disable** box. Choose how and if the account will be disabled. By default the account is never disabled. Using this feature is possible to set up temporary accounts with an expiration date.

When finished, click the **Submit** button. The user account is now set up and ready for use.