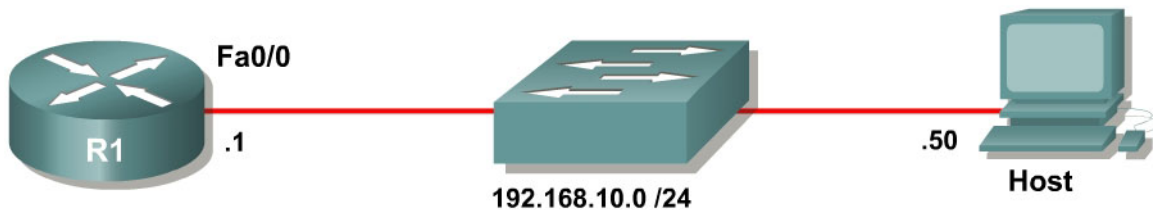


Lab 5.6b Configuring AAA and RADIUS

Learning Objectives

- Install CiscoSecure ACS
- Configure CiscoSecure ACS as a RADIUS server
- Enable AAA on a router using a remote RADIUS server

Topology Diagram



Scenario

In this lab, you will set up CiscoSecure ACS as a RADIUS server. You will also set up R1 to use authentication, authorization, and accounting (AAA) with reference to the RADIUS server. Because RADIUS is an open, standards-based protocol, many implementations are available. This lab shows how to configure CiscoSecure ACS. However, you could use a different RADIUS software solution. If you are using another RADIUS solution, configure the server similarly to the configuration used for ACS. The router configuration is the same regardless of the software server used.

Step 1: Configure the Interface

Configure the router interface shown in the topology diagram.

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

Configure the IP address of 192.168.10.50/24 on the host.

Verify that you have connectivity between R1 and the host with the **ping** command.

```
R1# ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Step 2: Install CiscoSecure ACS

If you have already installed CiscoSecure ACS, go to step 3.

This step guides you through installing the 90-day trial version of CiscoSecure ACS. After you download the trial and extract it, run Setup.exe.

Note: At the time of this writing, CiscoSecure ACS only runs on Microsoft Windows Server Editions. You cannot run CiscoSecure ACS on Microsoft Windows XP.

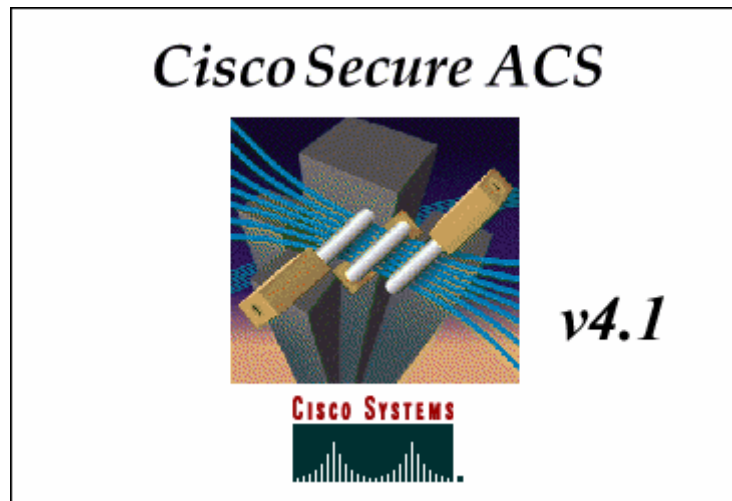


Figure 2-1: CiscoSecure ACS Splash Screen

After reading the terms of the license agreement, click **ACCEPT**.

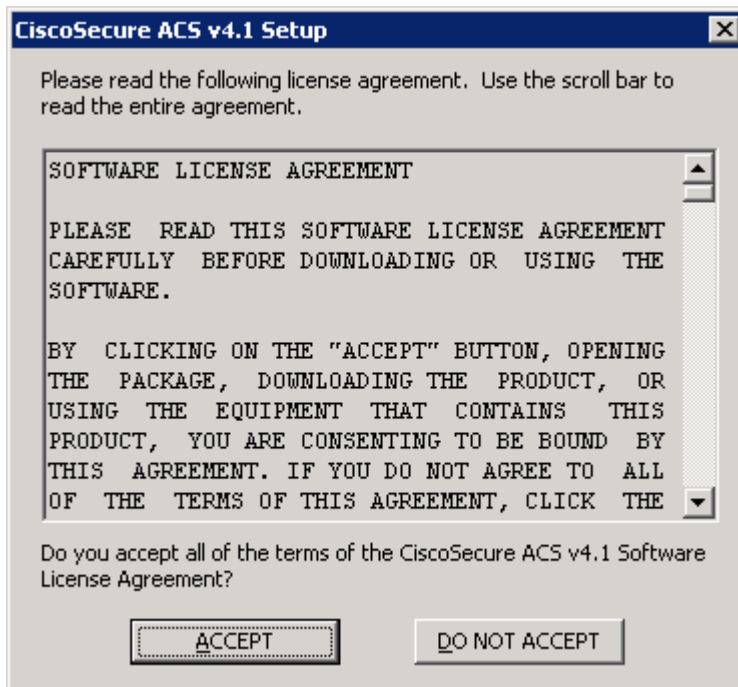


Figure 2-2: CiscoSecure ACS License Agreement

Click **Next** to continue the installation process.

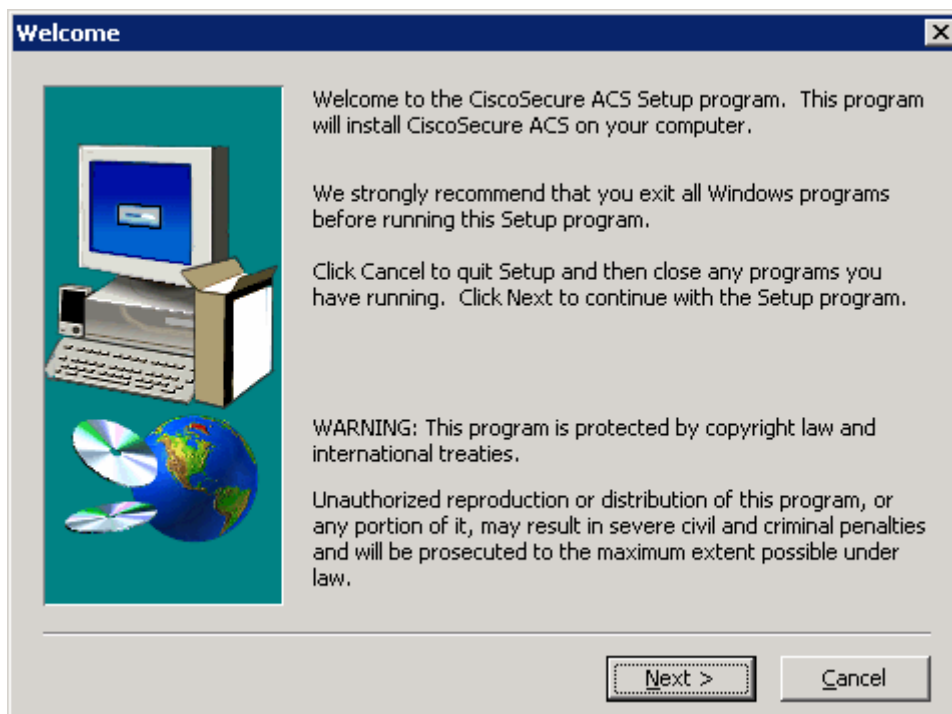


Figure 2-3: CiscoSecure ACS Installation Wizard

Verify that all the requirements in the checklist are satisfied and check all the options before clicking **Next**.

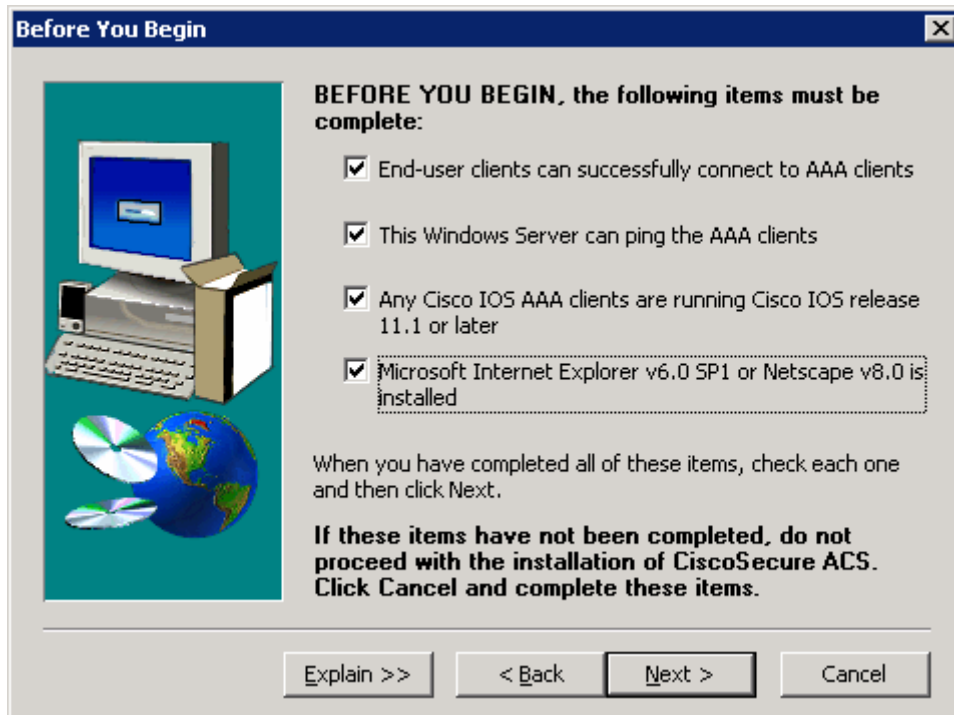


Figure 2-4: CiscoSecure ACS Pre-Installation Checklist

Use the default installation folder and click **Next**.

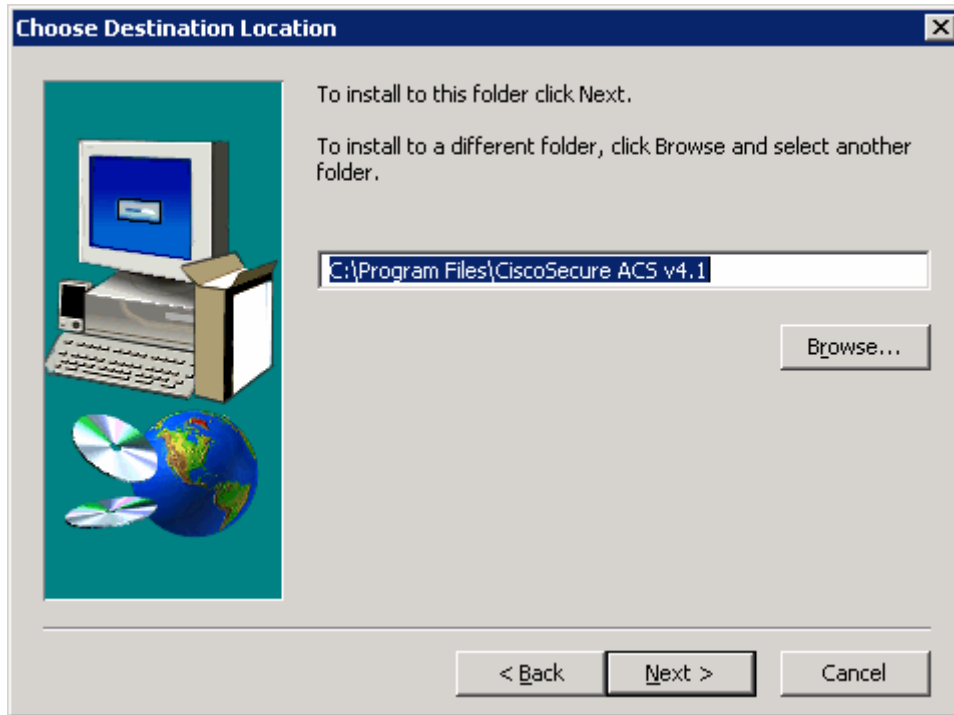


Figure 2-5: CiscoSecure ACS Installation Location

CiscoSecure has the ability to check the Windows User Database. However, for this lab, choose to authenticate using the internal database only. Click **Next**.

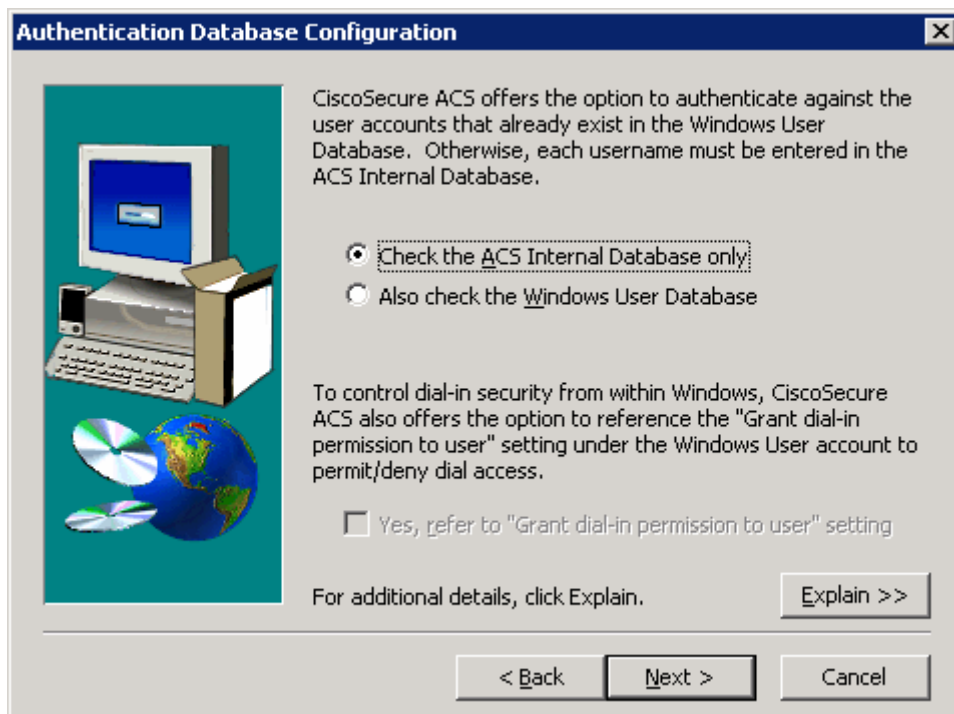


Figure 2-6: CiscoSecure ACS Authentication Database Options

The installer will then begin copying files and registry keys. This process may take a few minutes.

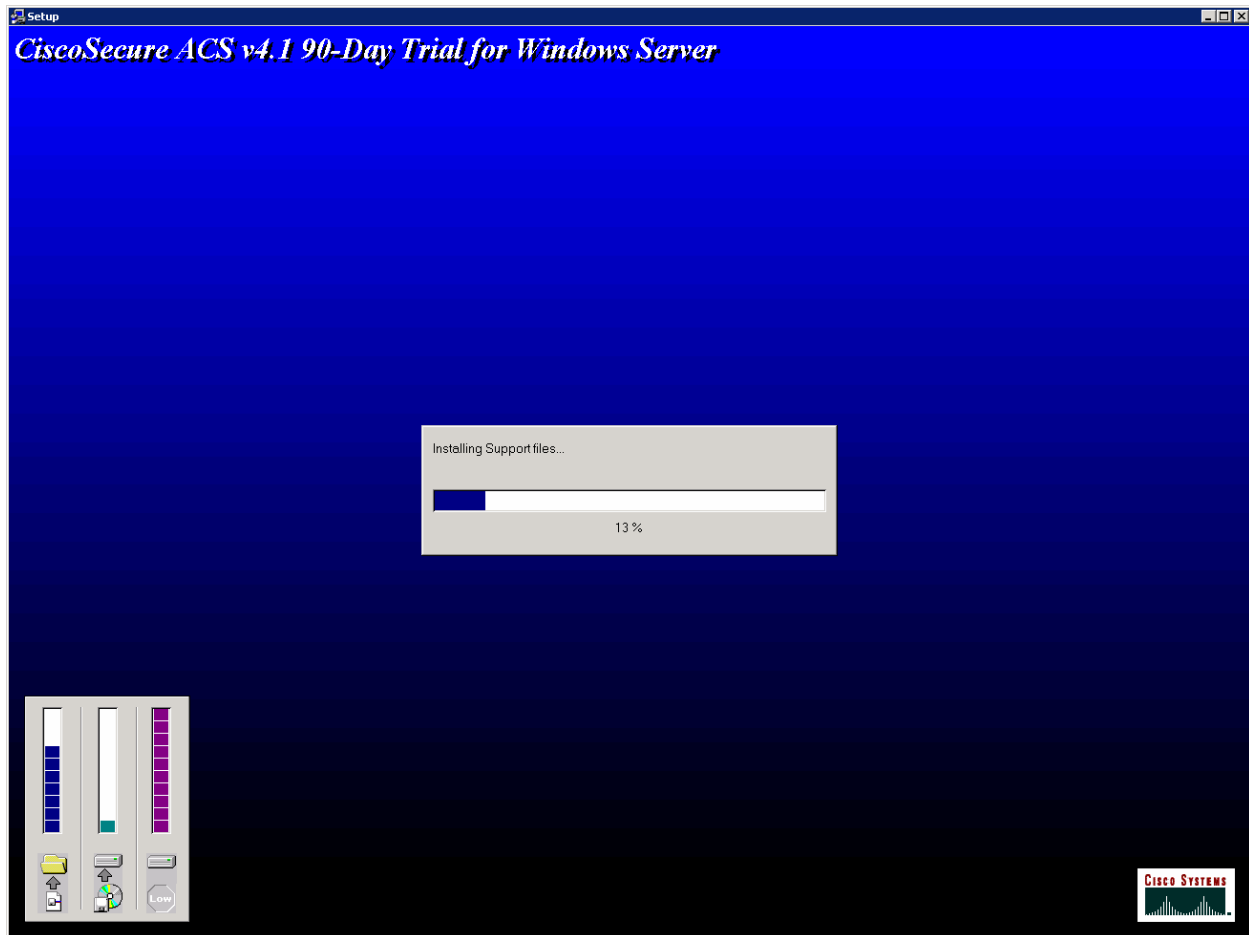


Figure 2-7: CiscoSecure ACS Installation Progress Indicator

At the end of the installer, you are prompted whether you want to see any advanced configuration options in the user interface. You do not need to select any of these. Click **Next** after reviewing the options.

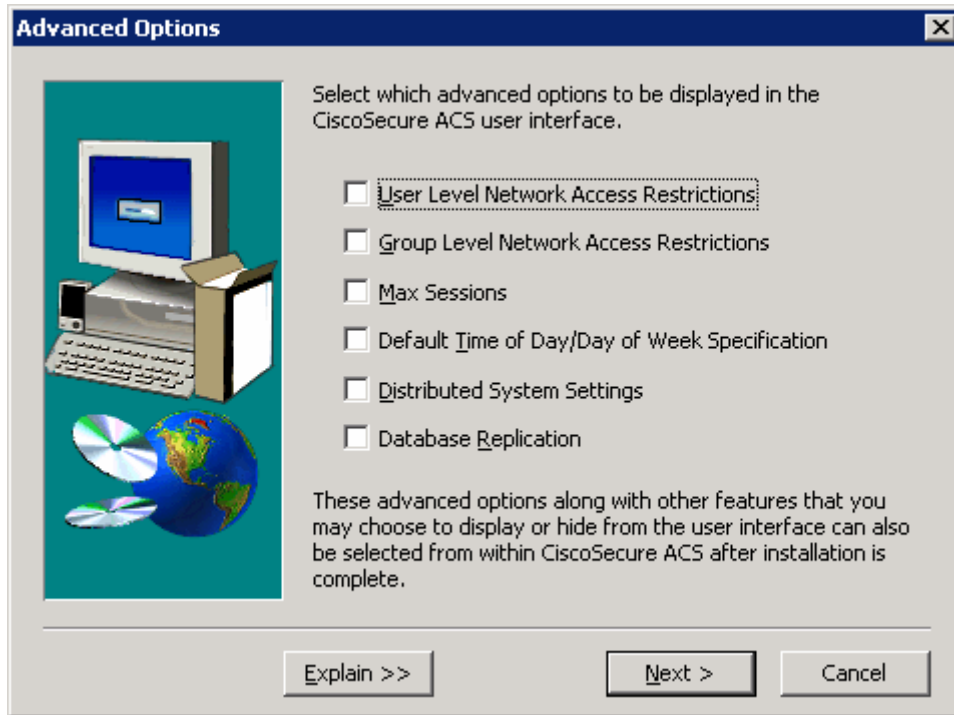


Figure 2-8: CiscoSecure ACS Advanced Configuration Options

Keep the default settings in the next step of the installation wizard and click **Next**.

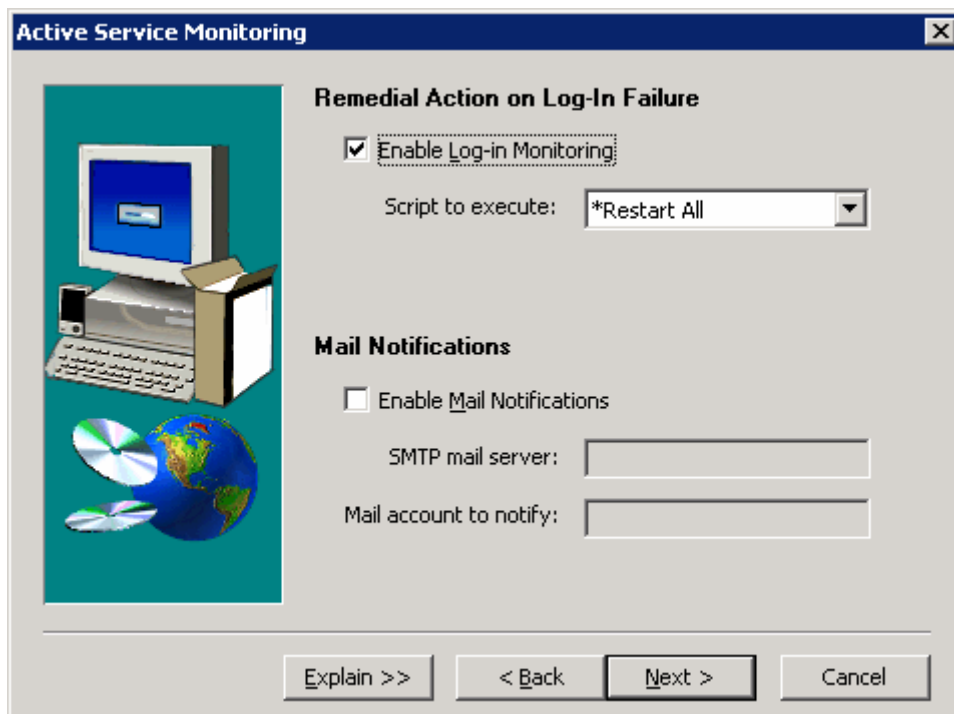


Figure 2-9: CiscoSecure ACS Log-In

You must create a password for ACS internal database encryption. It must be at least eight characters and contain both letters and numbers. In the example below, "ciscoacs4" is used as the password. After configuring the password, click **Next**.

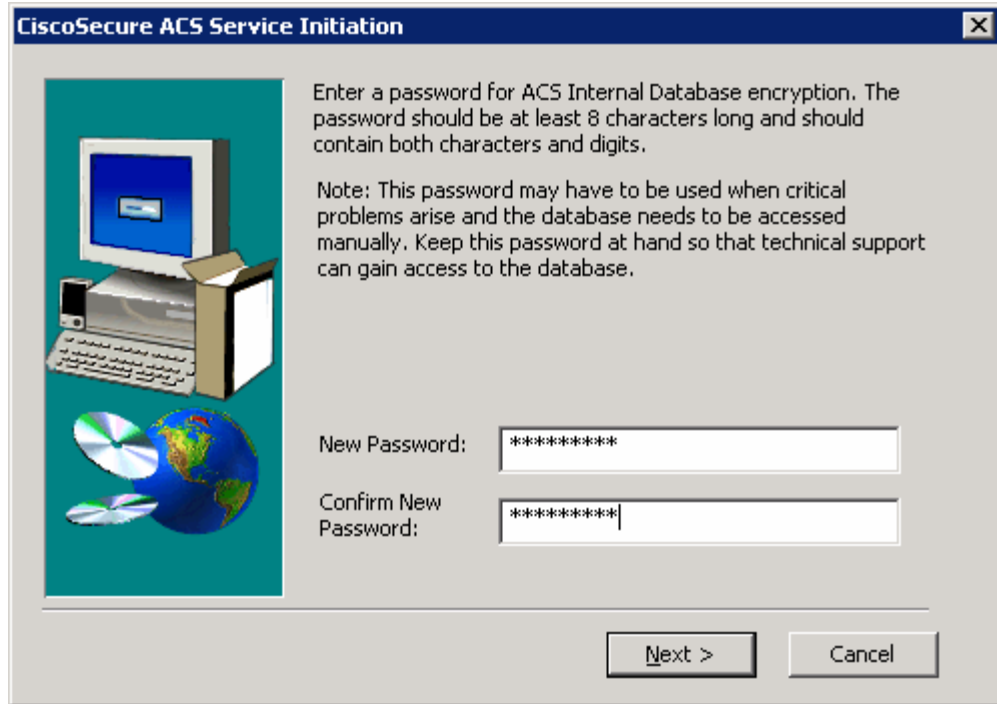


Figure 2-9: CiscoSecure ACS Password Configuration

Choose to start the ACS service on the host now. You should also select the option to start the administration window after the installer ends to verify the installation. Click **Next** after selecting the options.

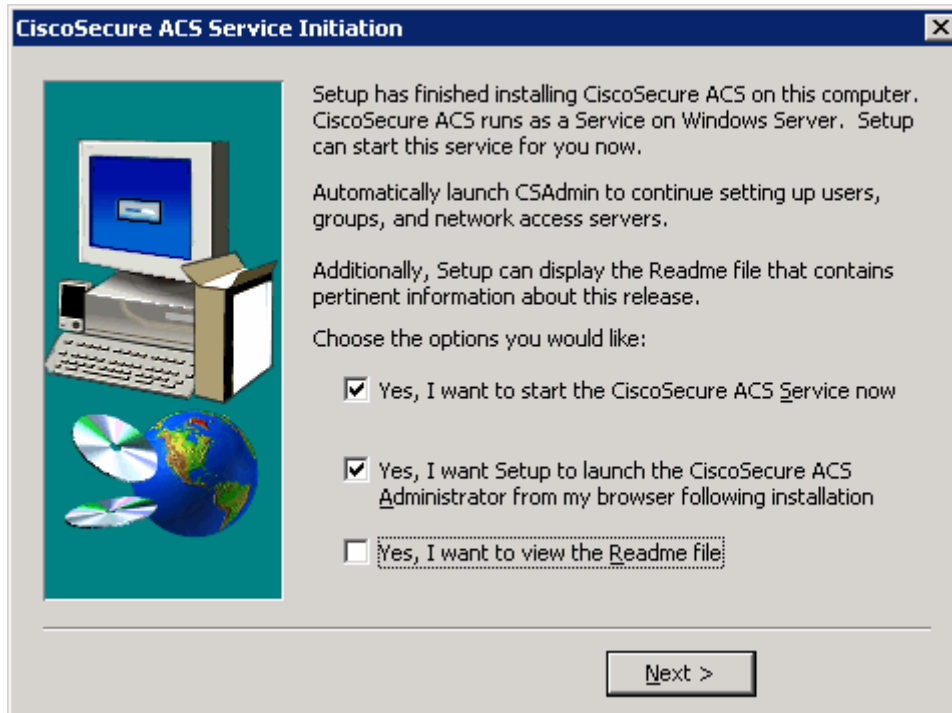


Figure 2-10: CiscoSecure ACS Service Configuration

Read the instructions and click **Finish**. You should also make sure your computer is compliant with all ACS access requirements, complying with the supported versions of Internet Explorer and the Java Runtime Environment.

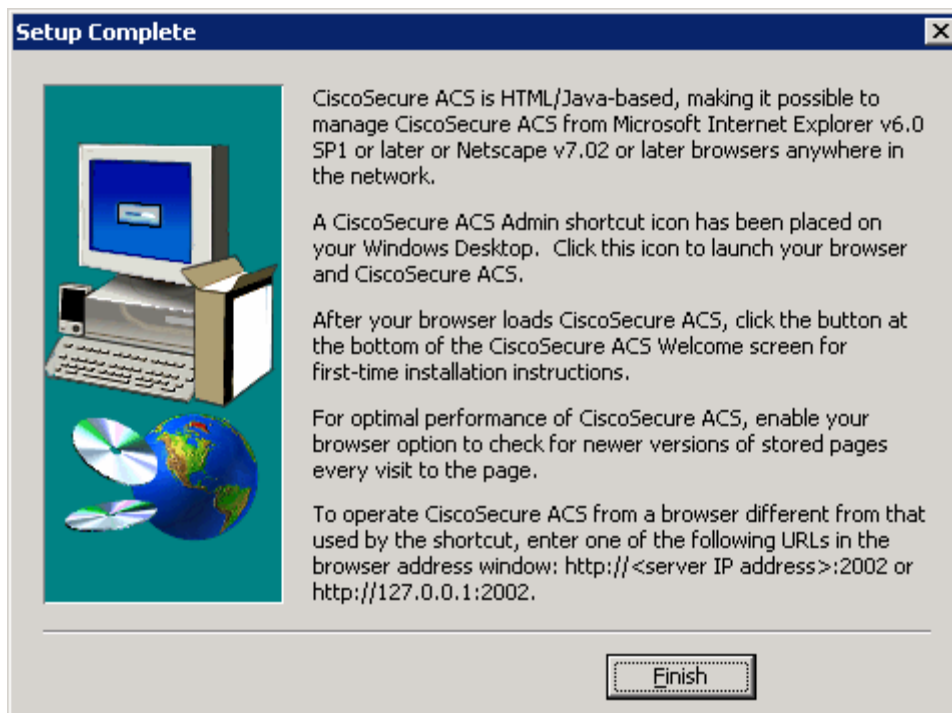


Figure 2-11: CiscoSecure ACS Installation Complete Window

If the CiscoSecure ACS administrative screen comes up when the installer ends, it was successfully installed.

Step 3: Configure Users in CiscoSecure ACS

If CiscoSecure ACS application is not open, start it by clicking the **Start** button and choosing **Programs > CiscoSecure ACS v4.1 Trial > ACS Admin**.

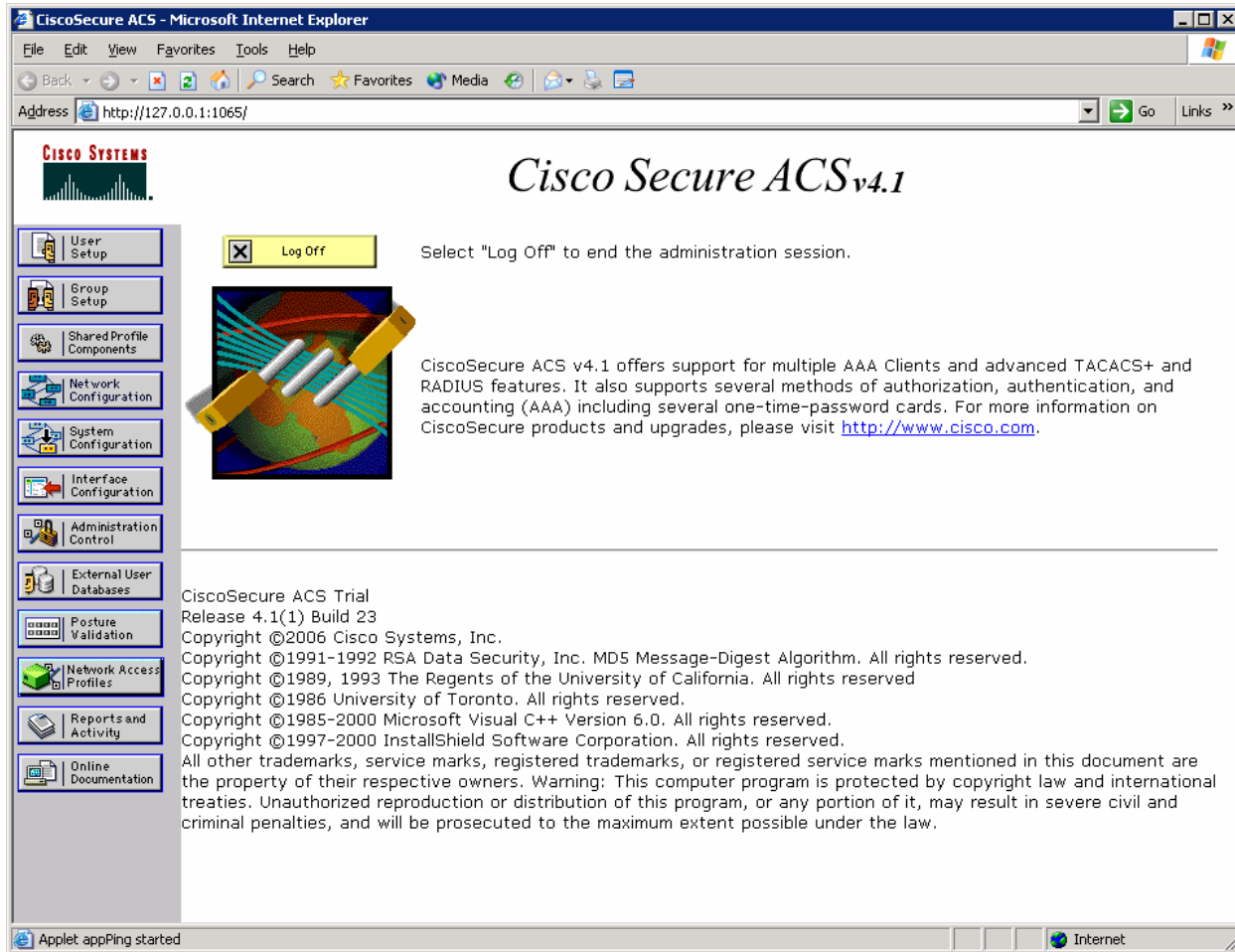


Figure 3-1: ACS Home Page

Click the **Network Configuration** button on the left side. On this screen, you can configure AAA clients directly. Click **Add Entry** under the heading AAA Clients.

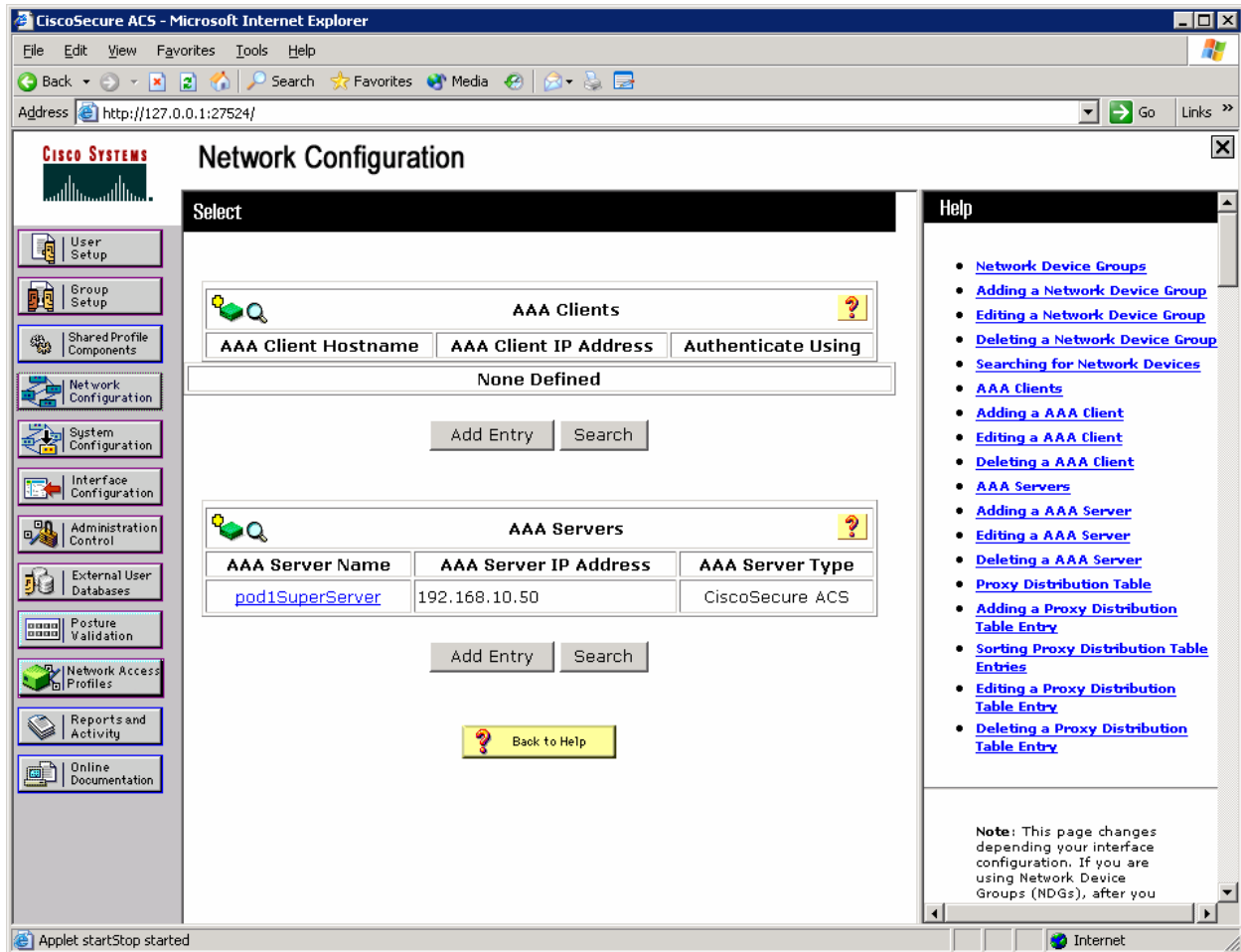


Figure 3-2: ACS Network Configuration Page

Configure R1 as a RADIUS client as shown below, and then click **Submit + Apply**.

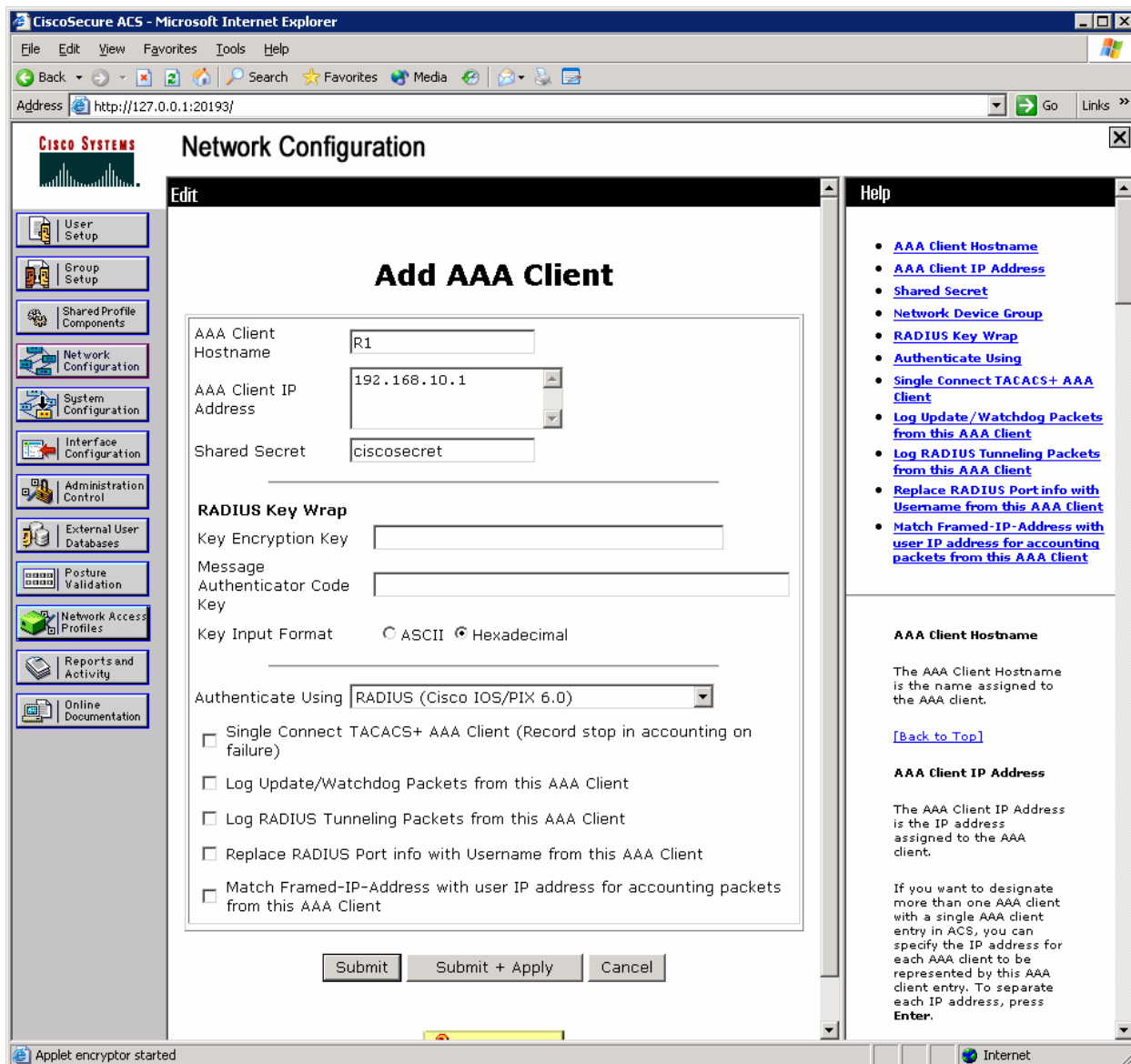


Figure 3-3: ACS AAA Client Configuration

You should now be able to see R1 listed as a AAA client on the network configuration screen.

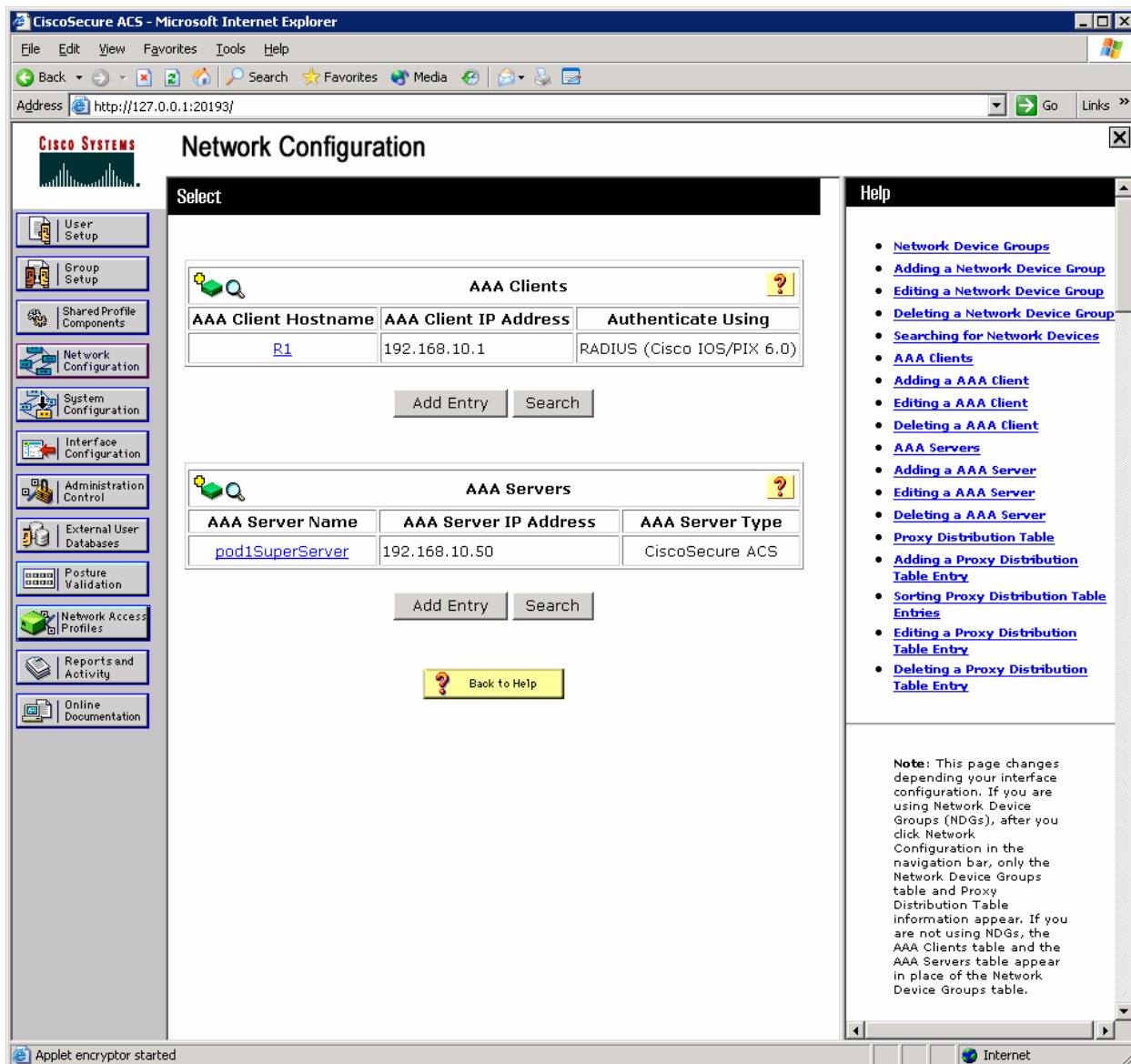


Figure 3-4: ACS Network Configuration Page, with Changes Applied

Click the **User Setup** button on the left side. Add a user named “cisco,” and then click **Add/Edit**.

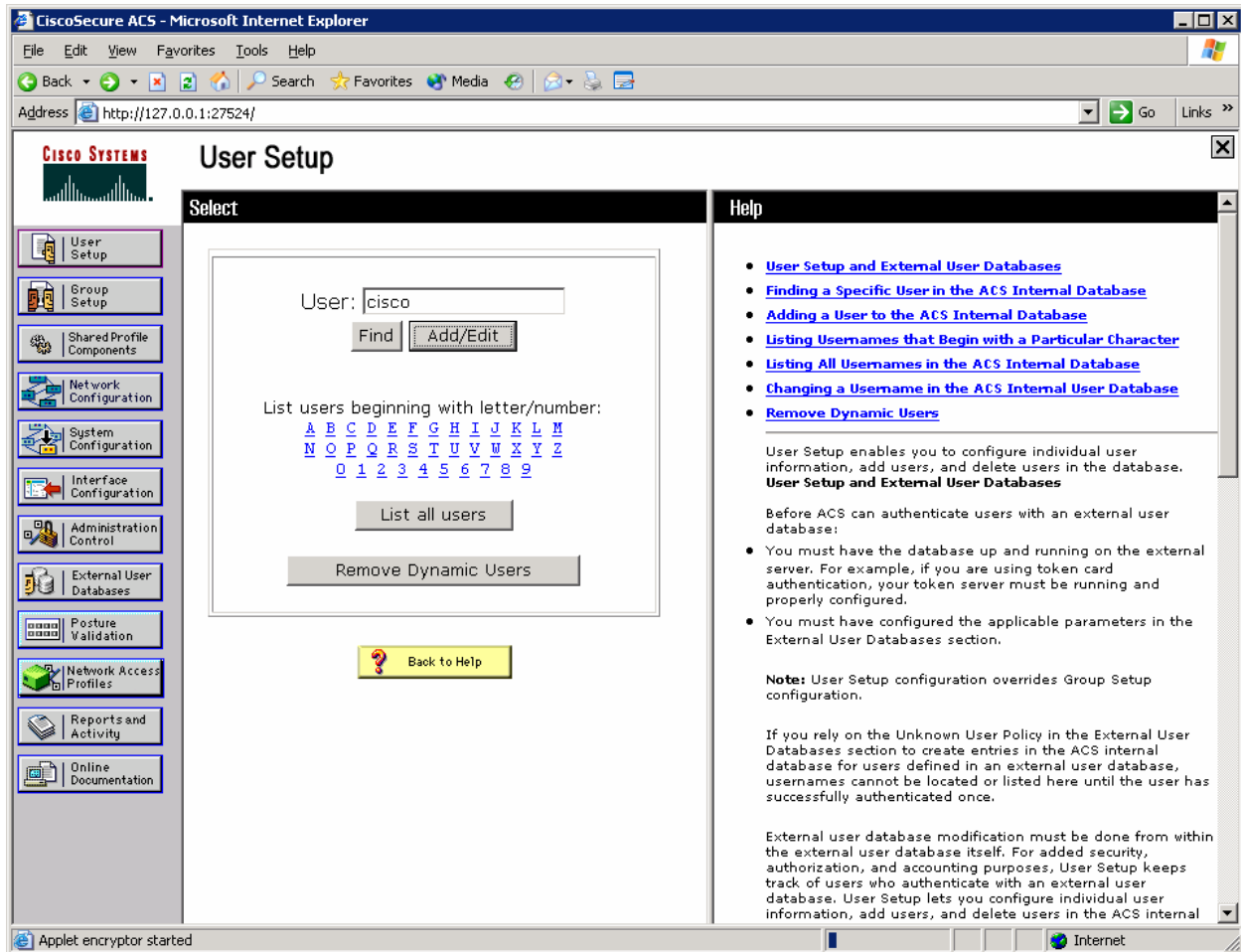


Figure 3-5: ACS User Configuration Page

Assign the real name to be your own name, and set the password to “cisco.”
Click **Submit**.

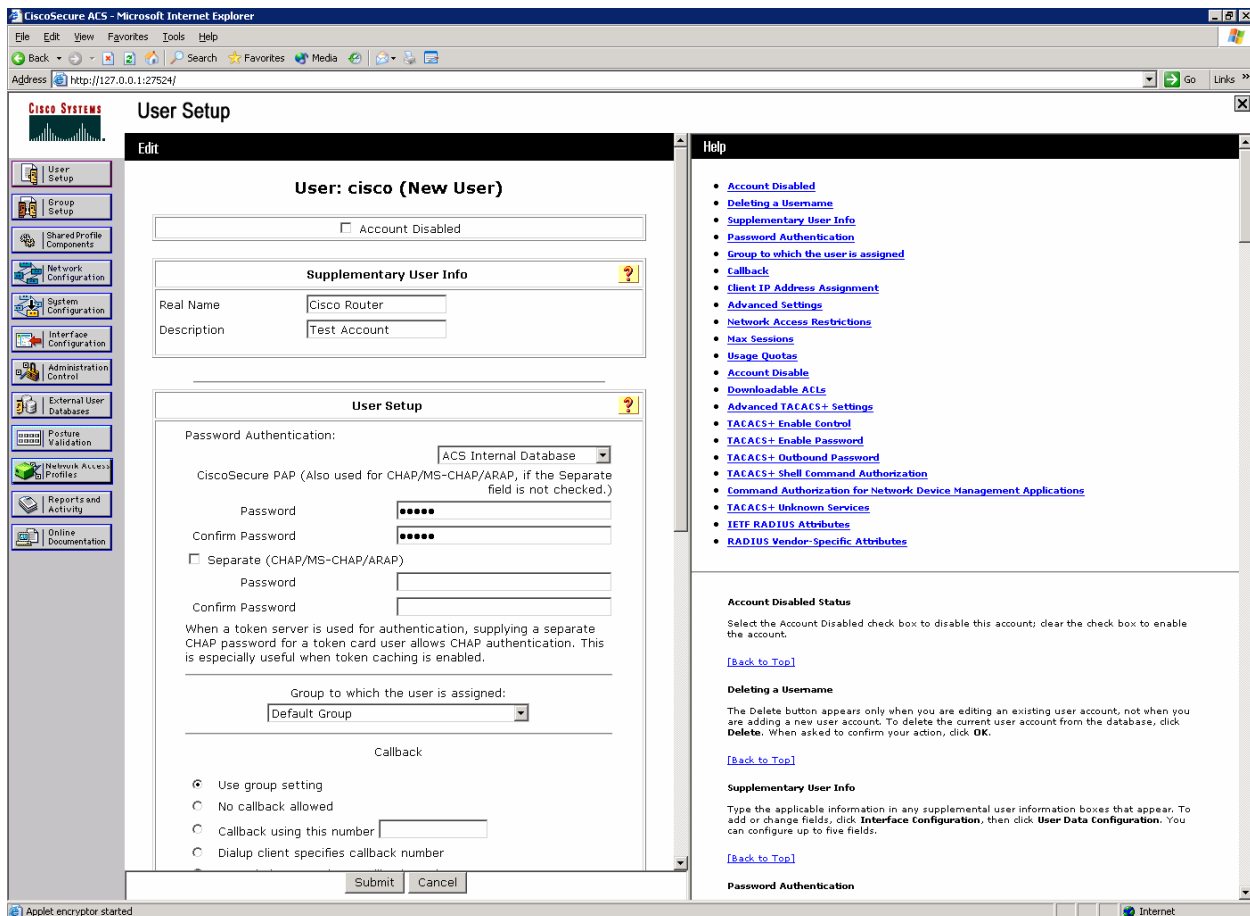


Figure 3-6: ACS Add New User Page

Why would a company want to use a centralized authentication server rather than configuring users and passwords on each individual router?

Step 4: Configure AAA Services on R1

On R1, enable AAA with the **aaa new-model** command in global configuration mode. Then set up the default login authentication list with the **aaa authentication login default method1 [method2] [method3]** command. You may create a list of authentication methods. Configure the list to first use RADIUS for the authentication service, and then enter the **none** keyword. If no RADIUS server can be reached and authentication cannot be performed, the router globally allows access without authentication. This is a safeguard measure in case the router starts up without connectivity to an active RADIUS

server. You could alternatively configure local authentication as the backup authentication method instead.

```
R1(config)# aaa new-model
R1(config)# aaa authentication login default group radius none
```

Note: If you do not set up a default login authentication list, you could get locked out of the router and need to use the password recovery procedure for your specific router.

Specify a RADIUS server using the **radius-server host** *hostname* **key** *key* command. The *hostname* parameter accepts either a hostname or an IP address. The *key* is a secret password shared between the RADIUS server and the AAA client and used to authenticate the connection between the router and the server before the user authentication process takes place.

```
R1(config)# radius-server host 192.168.10.50 key ciscosecret
```

Next, create a unique authentication list for Telnet access to the router. This does not have the fallback of no authentication, so if there is no access to the RADIUS server, Telnet access is disabled. To create an authentication list that is not the default list, use the global configuration command **aaa authentication login** *name* *method1* [*method2*] [*method3*]. Name the authentication method list “telnet_lines.” To apply the list to vtys on the router, issue the **login authentication** *name* command in line configuration mode.

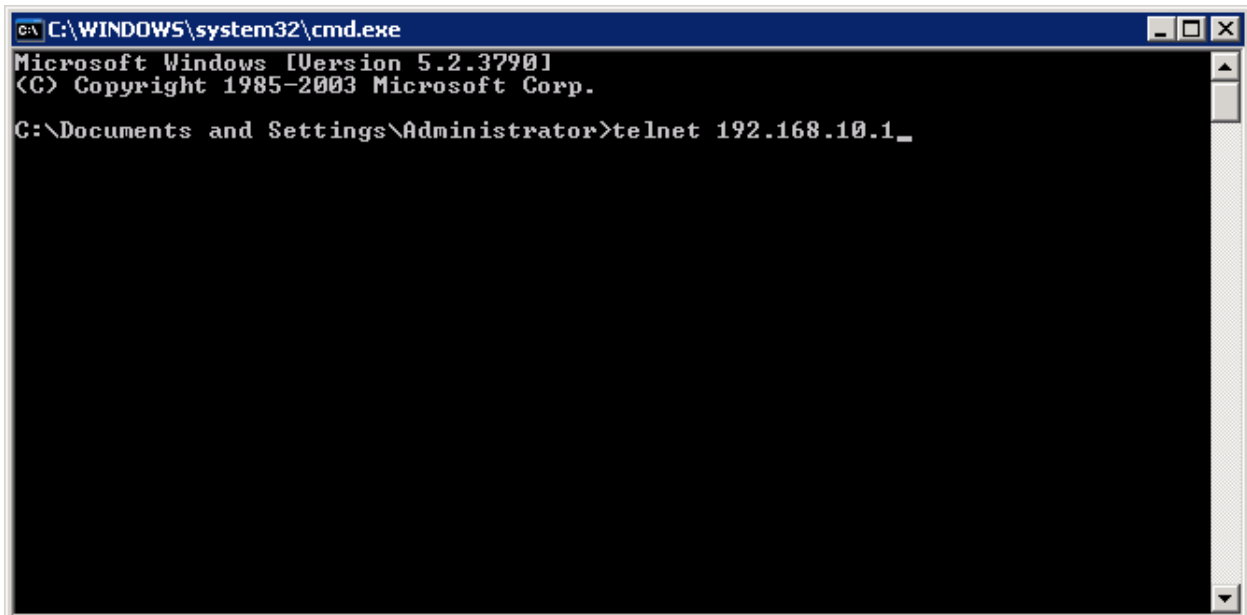
```
R1(config)# aaa authentication login telnet_lines group radius
R1(config)# line vty 0 4
R1(config-line)# login authentication telnet_lines
```

Given the configuration described above, if you enter a username and password pair stored in the ACS authentication database, and the router can reach and use the authentication methods available through RADIUS, would the user be permitted to access the router?

If you enter a username and password pair not stored in the ACS authentication database and the router can reach and use the authentication methods available through RADIUS, would the user be permitted to access the router?

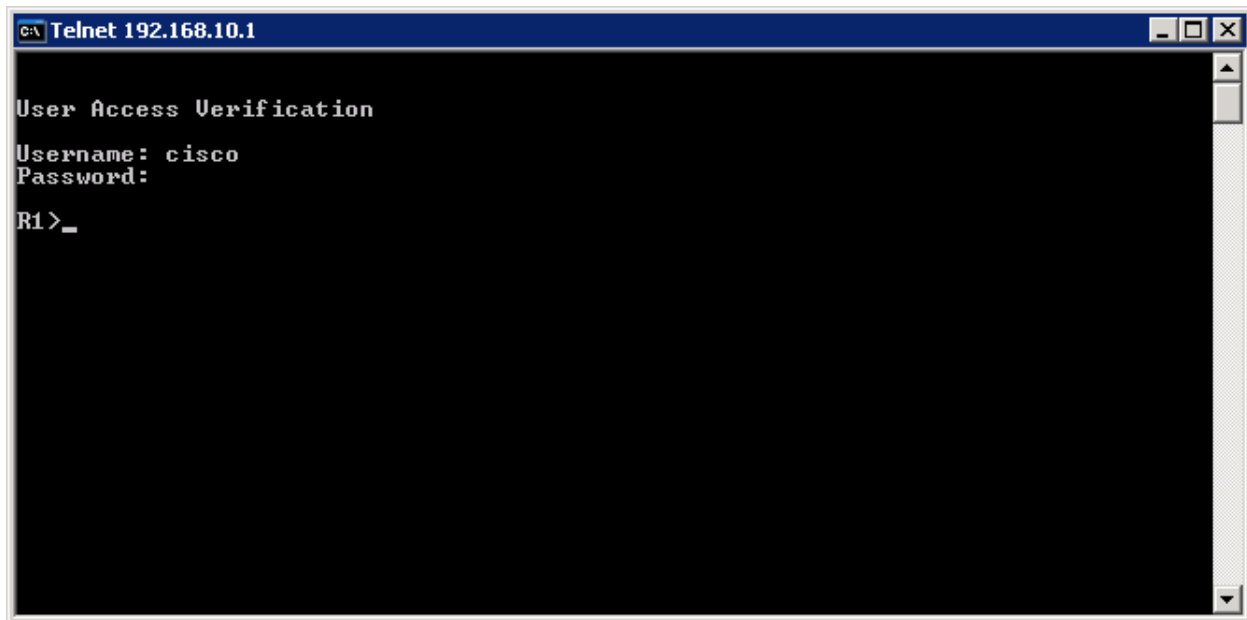
If you entered a username and password pair stored in the ACS authentication database, but the router could not reach a RADIUS server, would the user be permitted to access the router?

You can test your configuration by opening a Telnet session from the host to R1. Click the **Start** button and choose **Run**. Enter the **cmd** command in the Run dialog box, and click **OK**. At the command prompt, issue the **telnet host** command. At the login prompt, use the login credentials created earlier: the username and password are both “cisco.”



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>telnet 192.168.10.1_
```

Figure 4-1: Host Telnets to R1

A screenshot of a Telnet window titled "Telnet 192.168.10.1". The window has a black background with white text. The text shows a "User Access Verification" prompt, followed by "Username: cisco" and "Password:" on separate lines. The prompt "R1>_" is visible at the bottom left of the window.

```

c:\ Telnet 192.168.10.1
User Access Verification
Username: cisco
Password:
R1>_

```

Figure 4-2: Test AAA Authentication Using Telnet

If your session with the router console port times out, you may have to log in using the default authentication list.

Which authentication database does the current default authentication list query?

Why is it advisable to assign redundant authentication methods when using AAA?

Final Configuration

```

R1# show run
hostname R1
!
aaa new-model
!
aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown

```

```
!  
radius-server host 192.168.10.50 auth-port 1645 acct-port 1646 key ciscosecret  
!  
line vty 0 4  
  login authentication telnet_lines  
end
```