



Resource: Installing Cisco Secure ACS 3.0 and greater for Windows 2000

Cisco Secure ACS 3.0 for Windows 2000 is easy to install and configure. This section presents a brief overview of the essential installation steps.

The Cisco Secure ACS installation can be condensed to the following steps:

- Step 1** Configure the Windows NT or Windows 2000 server to work with Cisco Secure ACS.
- Step 2** Verify a basic network connection from the Windows 2000 server to the network access server (NAS) using ping and Telnet.
- Step 3** Install Cisco Secure ACS on the Windows 2000 server following the Windows 2000 installation shield.
- Step 4** Initially configure Cisco Secure ACS via the web browser interface.
- Step 5** Configure the network access server for AAA.
- Step 6** Verify correct installation and operation.

Configure the 2000 Server

The first step to follow when installing Cisco Secure ACS is to configure Windows 2000 for Cisco Secure ACS by doing the following:

- Ensure the latest Service Pack is installed
- Configure Windows 2000 User Manager.
- Use Windows 2000 services to control ACS.

Cisco does not recommend that you install Cisco Secure ACS for Windows on primary domain controllers (PDC) or backup domain controllers (BDC).

Verify Connections Between 2000 Server and Other Network Devices

Verify that the NAS (router, pix, access point or switch) can ping the Windows 2000 server that will host Cisco Secure ACS. This verification will simplify installation and eliminate problems when configuring Cisco Secure ACS and devices that interface with it.

Cisco Secure ACS is easy to install from a CD-ROM or the Trial version download.

<http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des>

It installs like any other Windows application, using an InstallShield template. Before installing, ensure the network access server information such as host name, IP address, and TACACS+ key is available.

Install Cisco Secure ACS on the Server

Follow the InstallShield instructions as listed below:

- Select and configure the database.
- Configure Cisco Secure ACS for NAS using the web browser.
- Configure the NAS (router, pix, access point or switch) for Cisco Secure ACS.

Configure Cisco Secure ACS Using the Web Browser

After successfully installing Cisco Secure ACS, an ACS Admin icon appears on the desktop. Continue the initial configuration of Cisco Secure ACS with the web browser interface as follows:

- Cisco Secure ACS on Windows 2000 supports only HTML; a web browser is the only way to configure it. Cisco Secure ACS 3.0 for Windows supports the following browsers:
 - Microsoft Internet Explorer version ≥ 5.5 for Microsoft Windows
 - Netscape Communicator version ≥ 7.0 for Microsoft Windows
- Selecting the icon launches the browser with the address `http://127.0.0.1:2002/`.
- `http://<ip address>:2002/` and `http://<host name>:2002/` also works.

After Cisco Secure ACS is installed, configuration and management is through the web-based GUI. Make sure java and javascript are enabled in the web browser.

Configure Remaining Devices for AAA

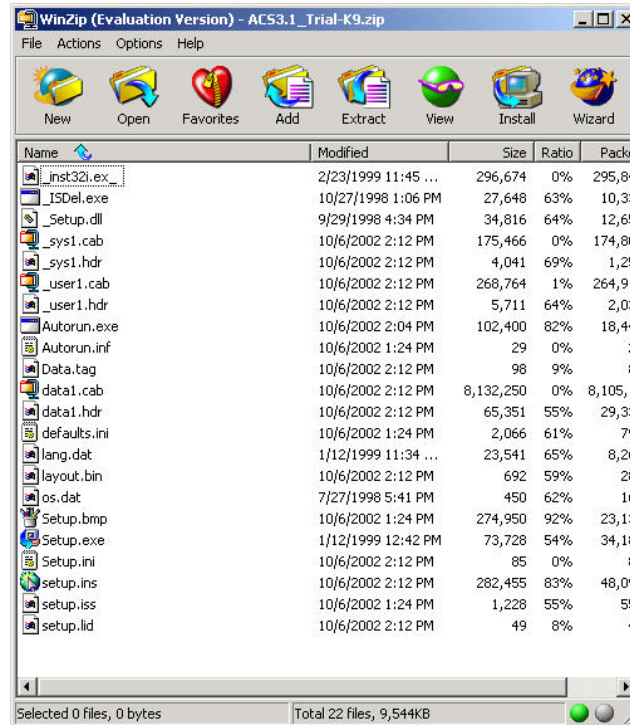
The NAS (router, pix, access point or switch) must be configured to work with Cisco Secure ACS.

Here are some of the possible configuration combinations where Cisco Secure ACS is used to perform AAA. In each configuration, each of the devices must be configured to work with Cisco Secure ACS:

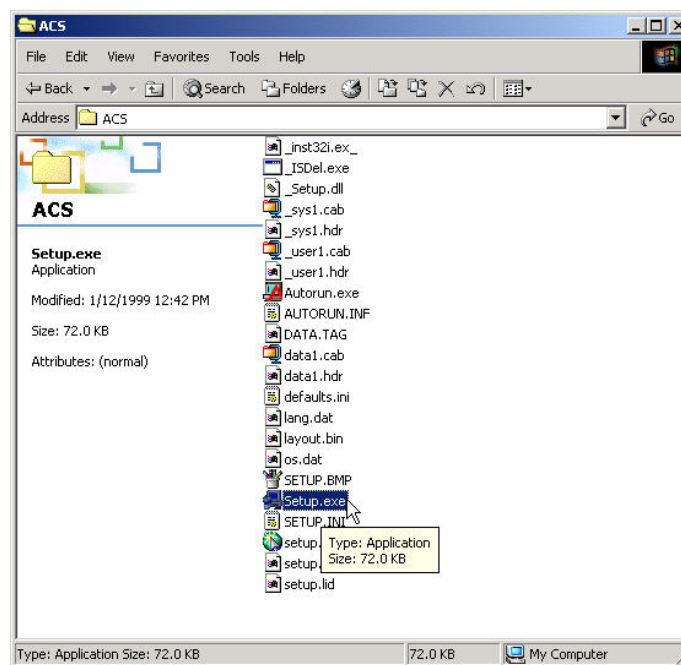
- Dialup using the Windows NT or Windows 2000 user database with TACACS+
- Dialup using the Cisco Secure ACS user database with TACACS+
- Dialup using a token card server with TACACS+
- Dialup using the Cisco Secure ACS user database with RADIUS (Cisco)
- Dialup for an ARAP client using the Cisco Secure ACS user database with TACACS+
- Device management using the Cisco Secure ACS user database with TACACS+
- User authentication for wireless access
- User authentication for switch port access
- PIX or router authentication/authorization using the Windows 2000 user database with TACACS+

Installing Cisco Secure ACS

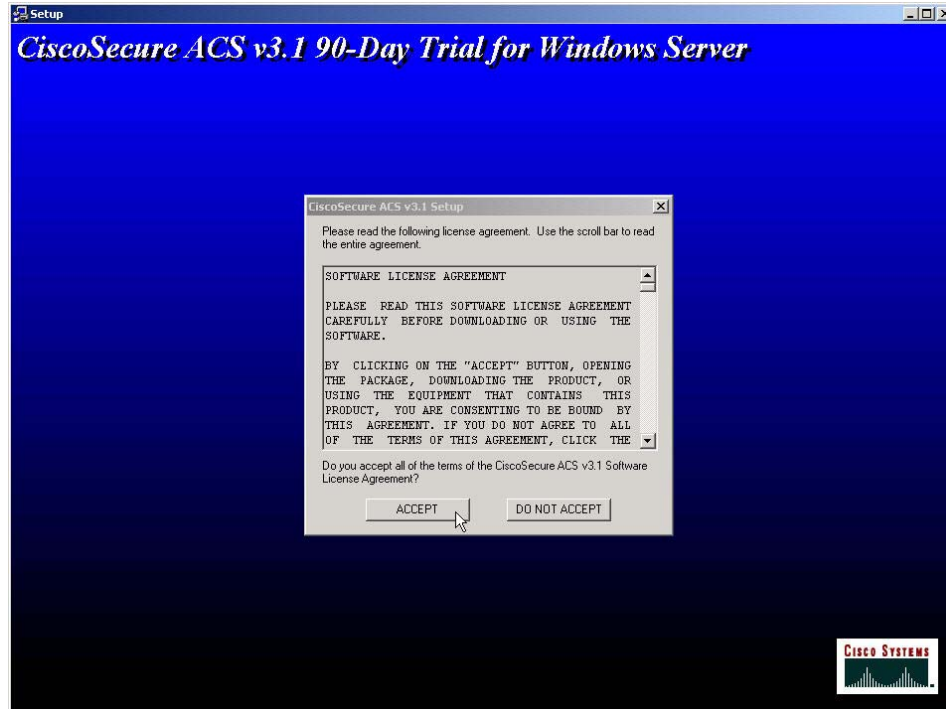
Step 1 Uncompress the packaged CSACS zip file.



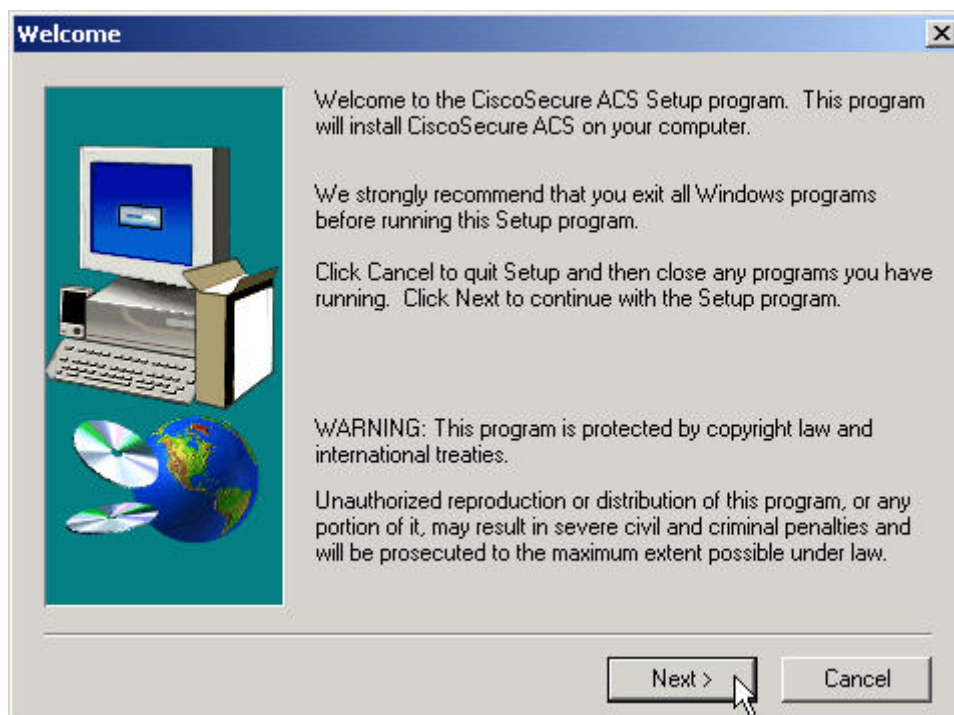
Step 2 After the CSACS zip file is uncompressed, launch the **Setup.exe** file.



Step 3 Press **ACCEPT** to agree the Software License Agreement.



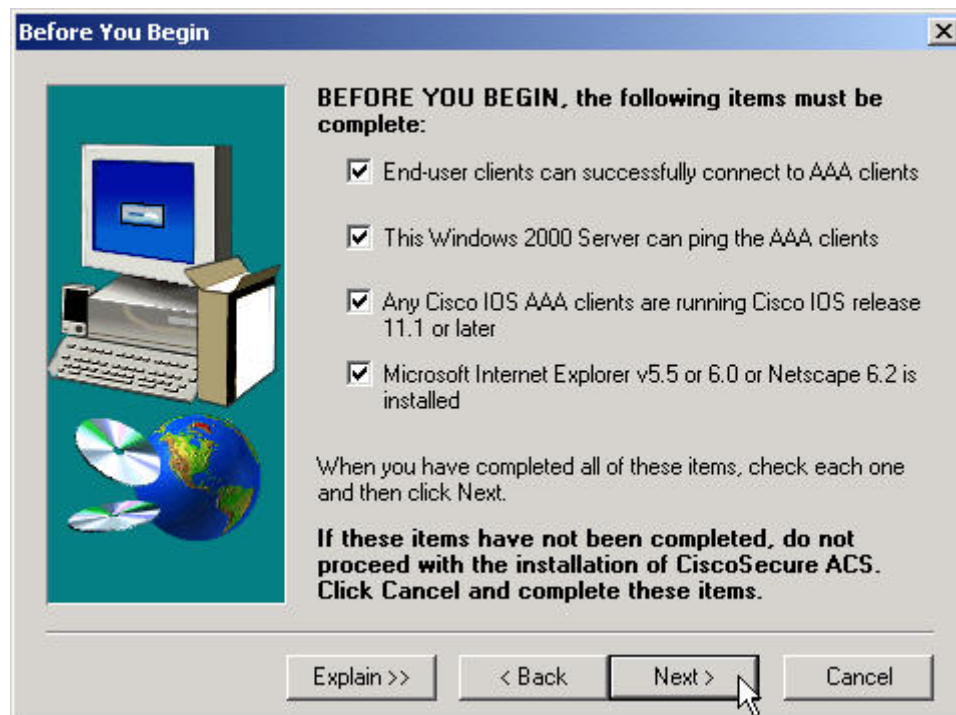
Step 4 If there are any Windows programs running, exit out of them and proceed with the CSACS installation. Press **Next>** to continue.



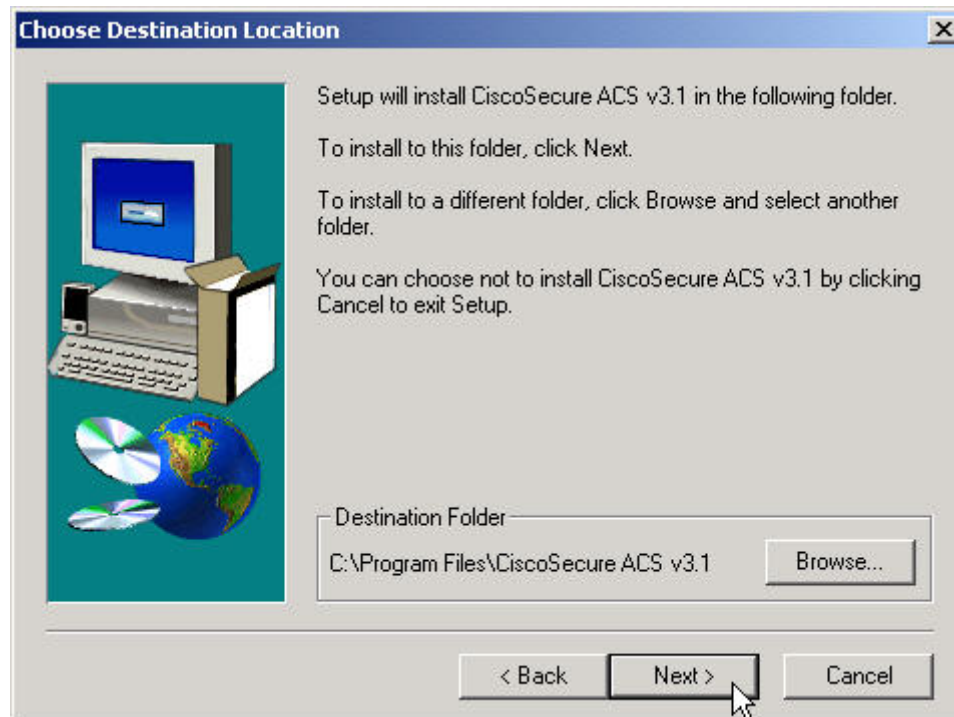
Step 5 If IAS is running, the setup utility will recommend disabling this service. To avoid any issues, disable IAS and press **Next>** to continue.



Step 6 Verify all the CSACS requirements have been met and proceed with the installation by clicking **Next>**.



Step 7 Choose the desired destination folder and press **Next>** to continue.

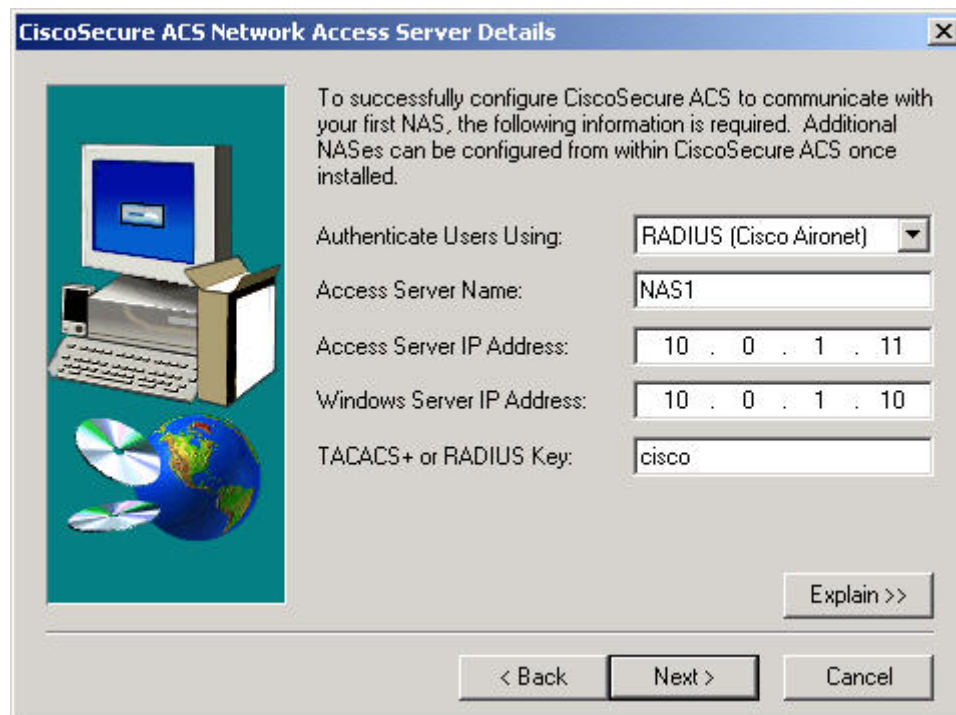


Step 8 In the Network Security courses, students will authenticate against the CiscoSecure ACS database. Select the CSACS database checkbox and press **Next>** to continue.



Step 9 Initially, a NAS must be configured to install the CSACS. In this example, NAS1 is being configured. Press **Next>** to continue. In the FWL course, users will be authenticated using **RADIUS (Cisco Aironet)** and the RADIUS key is **cisco**. In the Network Security courses, users will be authenticated using **TACACS+ (Cisco IOS)**

TACACS+ (Cisco IOS)
RADIUS (Cisco Aironet)
RADIUS (Cisco BBSM)
RADIUS (Cisco IOS/PIX)
RADIUS (Cisco VPN 3000)
RADIUS (Cisco VPN 5000)
RADIUS (IETF)
RADIUS (Ascend)
RADIUS (Juniper)
RADIUS (Nortel)
RADIUS (iPass)



The screenshot shows the 'CiscoSecure ACS Network Access Server Details' window. On the left is an illustration of a computer system with a monitor, keyboard, and tower unit, along with a CD-ROM and a globe. The main text area contains instructions: 'To successfully configure CiscoSecure ACS to communicate with your first NAS, the following information is required. Additional NASes can be configured from within CiscoSecure ACS once installed.' Below this are several configuration fields: 'Authenticate Users Using:' with a dropdown menu set to 'RADIUS (Cisco Aironet)'; 'Access Server Name:' with a text box containing 'NAS1'; 'Access Server IP Address:' with a dotted IP address box containing '10 . 0 . 1 . 11'; 'Windows Server IP Address:' with a dotted IP address box containing '10 . 0 . 1 . 10'; and 'TACACS+ or RADIUS Key:' with a text box containing 'cisco'. At the bottom right is an 'Explain >>' button. At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

CiscoSecure ACS Network Access Server Details

To successfully configure CiscoSecure ACS to communicate with your first NAS, the following information is required. Additional NASes can be configured from within CiscoSecure ACS once installed.

Authenticate Users Using: RADIUS (Cisco Aironet)

Access Server Name: NAS1

Access Server IP Address: 10 . 0 . 1 . 11

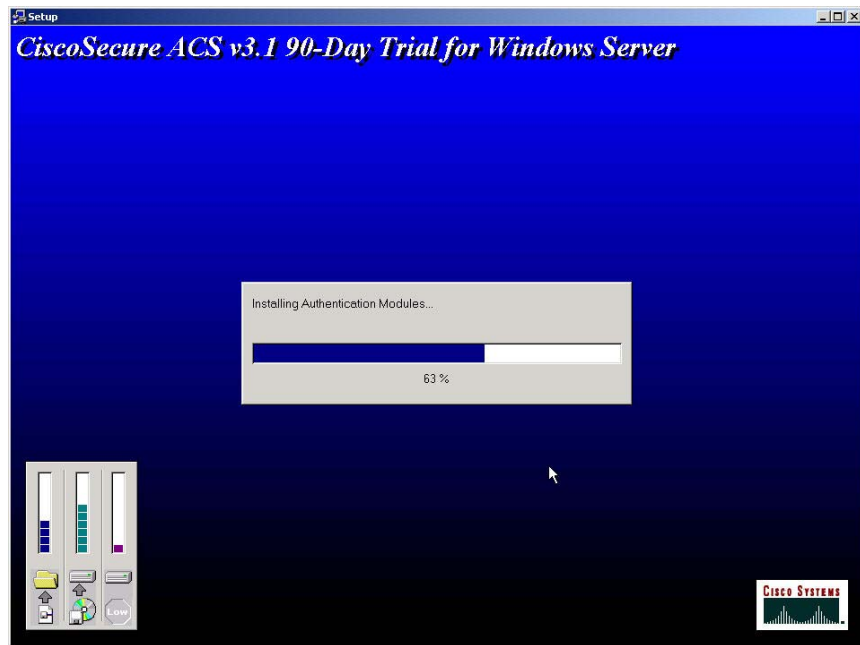
Windows Server IP Address: 10 . 0 . 1 . 10

TACACS+ or RADIUS Key: cisco

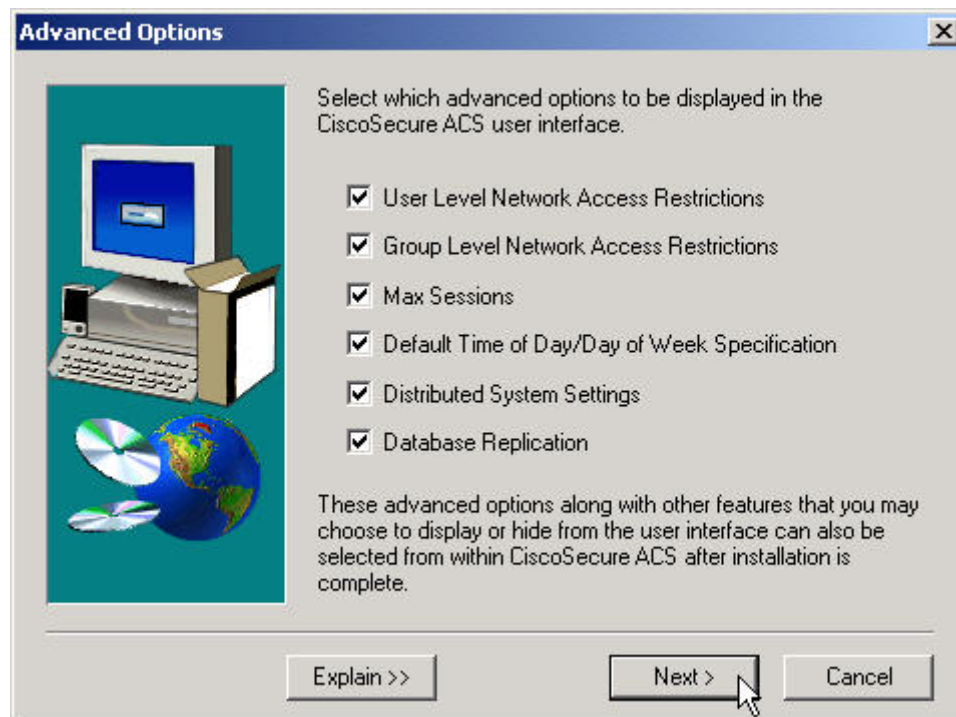
Explain >>

< Back Next > Cancel

Step 10 CSACS will begin updated the server.



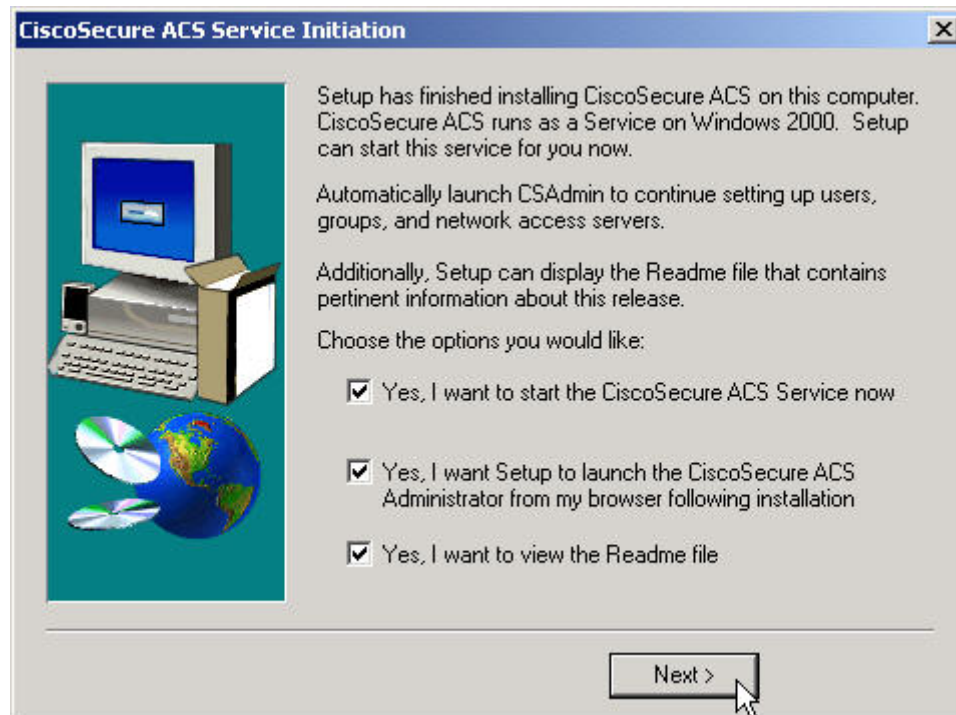
Step 11 Select all the advanced options and press **Next>** to continue.



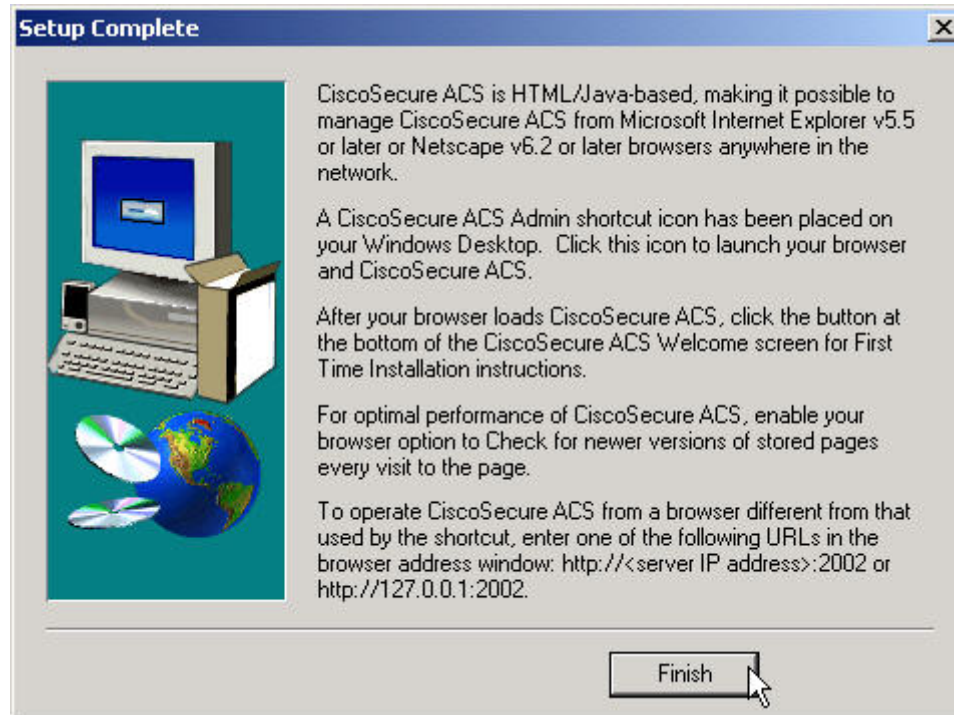
Step 12 Enable Log-in Monitoring and press **Next>** to continue.



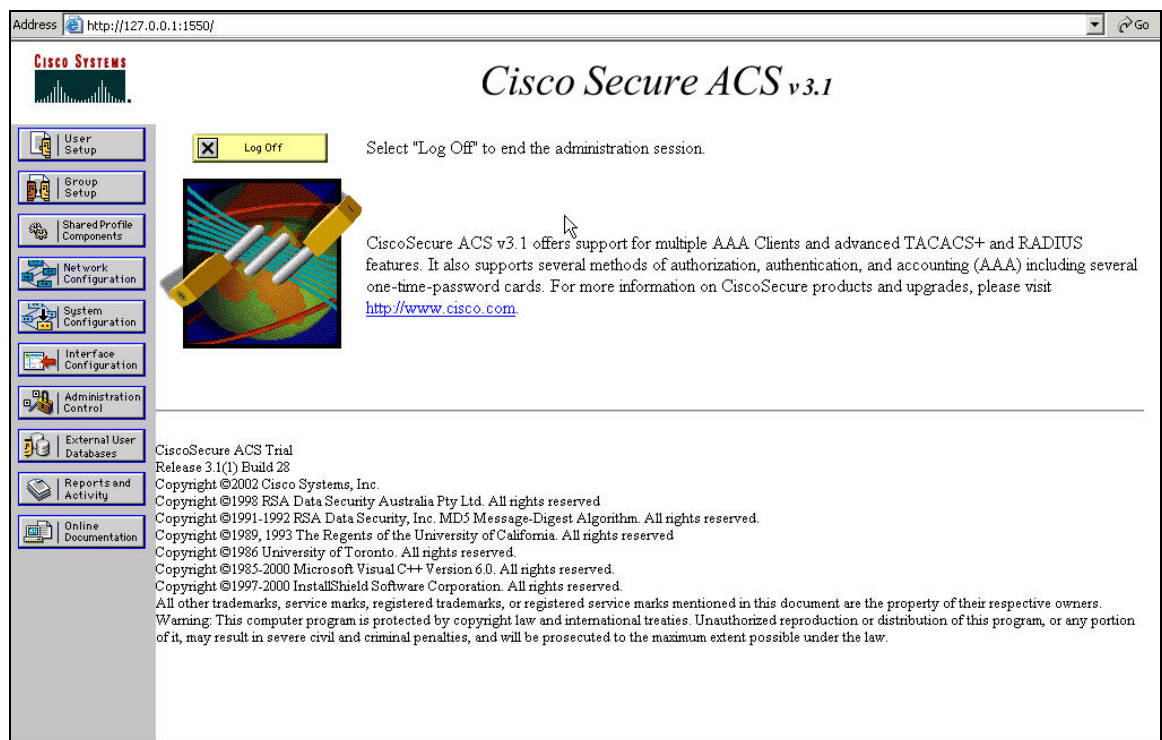
Step 13 Select the appropriate options and press **Next>** to continue.



Step 14 Click **Finish** to complete the installation of CSACS.



Step 15 The CSACS main menu will appear. CSACS has been successfully installed.



Administrative Options

The Cisco Secure ACS web browser interface makes administration of AAA features easy. It provides a navigation bar with a number of buttons, each of which represents a particular area or function that can be configured. Not all of the buttons will be used depending on the configuration that is being put in place. The following is a list of the buttons available to the administrator, as well as a brief description of each.

User Setup	Add, edit, delete user accounts, list users in databases
Group Setup	Create, edit, rename groups, list all users in a group
Network Configuration	Configure and edit network access server parameters; add and delete network access servers; configure AAA server distribution parameters
System Configuration	Start and stop Cisco Secure ACS services, configure logging, control database replication, control RDBMS synchronization
Interface Configuration	Configure user defined fields that will be recorded in accounting logs; configure TACACS+ and RADIUS options, control display of options in the user interface
Administration Control	Control administration of Cisco Secure ACS from any workstation on the network
External User Databases	Configure the unknown user policy; configure authorization privileges for unknown users; configure external database types
Reports and Activity	<p>Select Reports & Activity in the navigational bar to view the information below. It is possible to input this information into most database and spreadsheet applications.</p> <ul style="list-style-type: none">• TACACS+ Accounting Reports—Lists when sessions stop and start; records network access server messages with username; provides caller line identification information; records the duration of each session• RADIUS Accounting Reports—Lists when sessions stop and start; records network access server messages with username; provides caller line identification information; records the duration of each session• Failed Attempts Report—Lists authentication and authorization failures with an indication of the cause

- List Logged in Users—Lists all users currently receiving services for a single network access server or all network access servers with access to Cisco Secure ACS
- List Disabled Accounts—Lists all user accounts that are currently disabled
- Admin Accounting Reports—Lists configuration commands entered on a TACACS+ (Cisco) network access server

Online Documentation

Provides more detailed information about the configuration, operation, and concepts of Cisco Secure ACS

Administrative Procedure

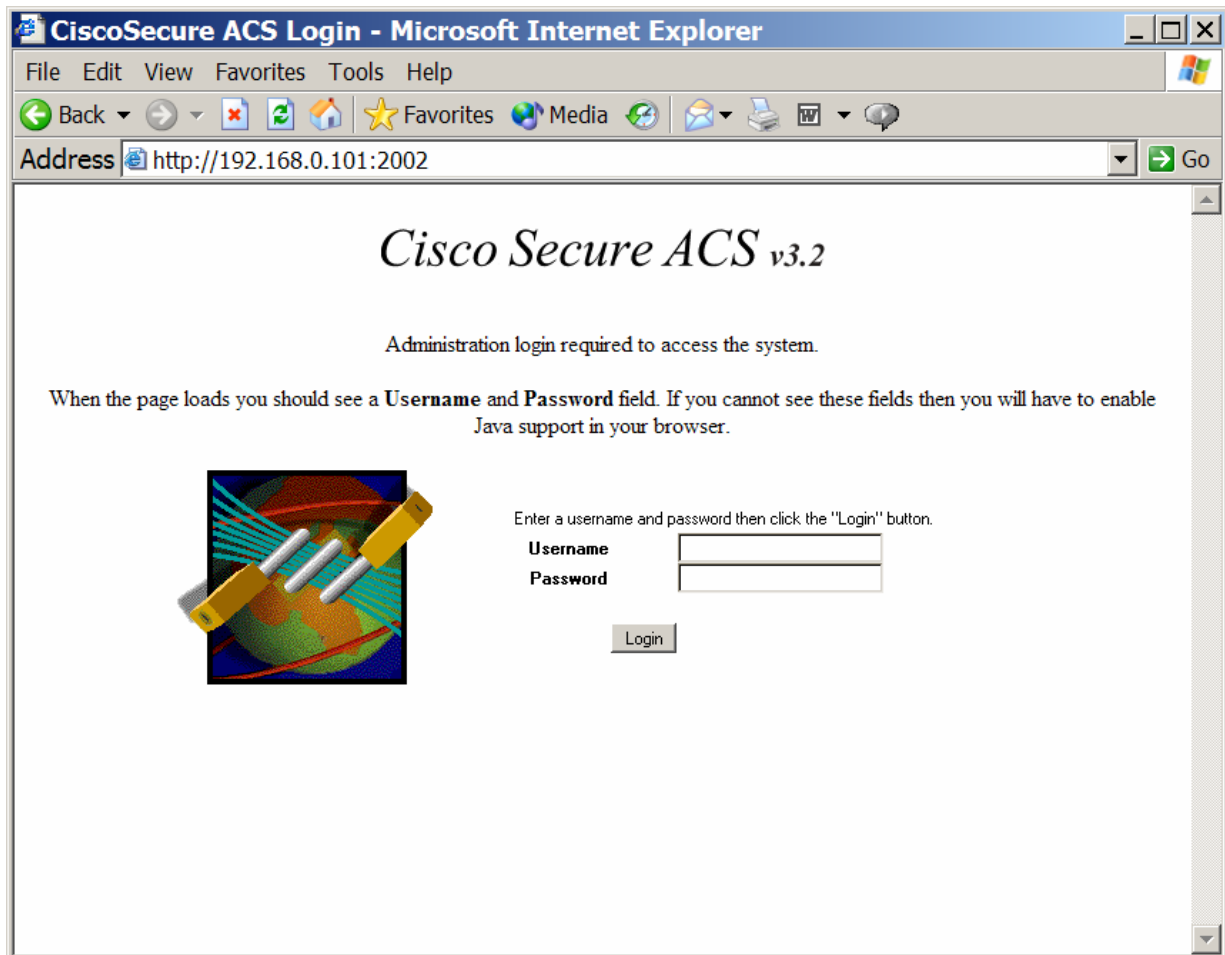
The previous list follows the order of the buttons in the navigational bar as they appear on the main administrative screen. However, this will not always be the order in which an administrator sets up the Cisco Secure ACS. The order the administrator uses will entirely depend on the needs of the network and that administrator's preferences. One typical order of configuration is as follows:

- Administration Control - Configure access for remote administrators.
- NAS Configuration - Configure and verify connectivity to a network access server.
- Group Setup - Configure available options and parameters for specific groups. All users must belong to a group.
- User Setup - Add users to a group that is configured.
- All other necessary areas.

Configure ACS for remote management

Cisco Secure ACS can be managed locally on the server or remotely via a web browser. CSACS can be managed remotely via any PC running IE 5.5 or Netscape 7 or later. From the remote PC, enter the IP address:2002 of the server running ACS in the Address field of the browser. See the example below.

<http://192.168.0.101:2002>



The screenshot shows a Microsoft Internet Explorer browser window titled "CiscoSecure ACS Login - Microsoft Internet Explorer". The address bar contains "http://192.168.0.101:2002". The main content area displays the "Cisco Secure ACS v3.2" login page. The page has a white background with a blue header. The title "Cisco Secure ACS v3.2" is in a large, black, serif font. Below the title, the text "Administration login required to access the system." is displayed in a smaller, black, sans-serif font. Further down, a message states: "When the page loads you should see a **Username** and **Password** field. If you cannot see these fields then you will have to enable Java support in your browser." To the left of the login fields is a graphic of a globe with a yellow and blue satellite dish. To the right of the globe, the text "Enter a username and password then click the 'Login' button." is displayed. Below this text are two input fields: "Username" and "Password". Below the "Password" field is a "Login" button.

Cisco Secure ACS v3.2

Administration login required to access the system.

When the page loads you should see a **Username** and **Password** field. If you cannot see these fields then you will have to enable Java support in your browser.

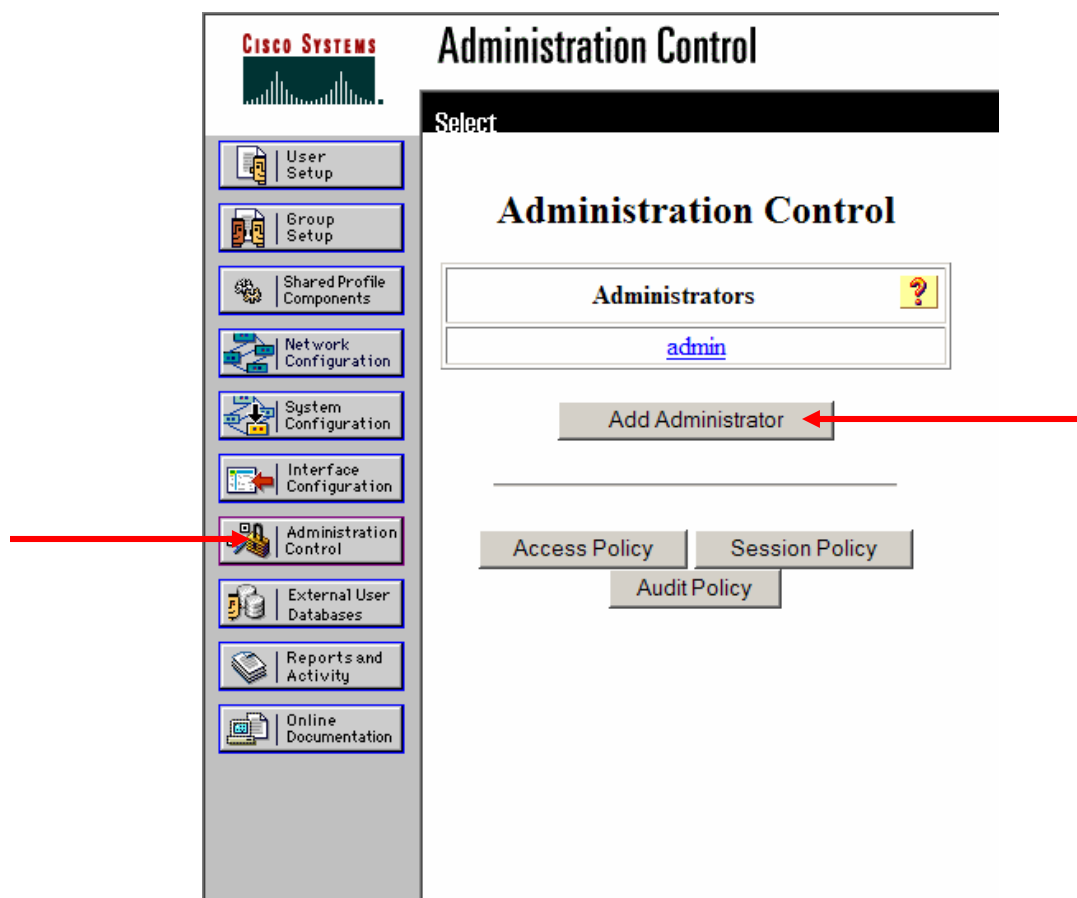
Enter a username and password then click the "Login" button.

Username

Password

Login

To enable remote management, an administrator account must be configured.



Step 1 Click on the **Administration Control** button on the left hand navigation area

Step 2 Click on the **Add Administrator** button

The screenshot shows the Cisco Systems Administration Control interface. On the left is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control (highlighted), External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Administration Control' and has a sub-header 'Edit'. The primary form is 'Add Administrator', which is divided into two sections: 'Administrator Details' and 'Administrator Privileges'. The 'Administrator Details' section contains three input fields: 'Administrator Name' with the text 'admin', 'Password' with five dots, and 'Confirm Password' with five dots. The 'Administrator Privileges' section contains two buttons, 'Grant All' and 'Revoke All', with a red arrow pointing to 'Grant All'. Below these buttons is the heading 'User & Group Setup...' followed by two unchecked checkboxes: 'Add/Edit users in these groups' and 'Setup of these groups'. At the bottom of the form are two buttons, 'Submit' and 'Cancel', with a red arrow pointing to 'Submit'. The 'Submit' button is also labeled 'Available groups' and the 'Cancel' button is labeled 'Editable groups'.

CISCO SYSTEMS

Administration Control

Edit

Add Administrator

Administrator Details

Administrator Name: admin

Password: •••••

Confirm Password: •••••

Administrator Privileges

Grant All **Revoke All**

User & Group Setup...

☐ Add/Edit users in these groups

☐ Setup of these groups

Available groups Editable groups

Submit **Cancel**

Step 3 Type in the admin name and password in the **Administrator Details** box.

Step 4 Click on the **Grant All** button in the **Administrator Privileges** box.

Step 5 Click on the **Submit** button at the bottom of the window.

Step 6 ACS can now be accessed remotely.

