

Initializing Management Center

Authorization on Cisco Secure ACS v.3.1

When CiscoWorks Common Services Software is installed as a standalone server, CiscoWorks Common Services uses the local authentication and authorization method. This method can, however, be changed to use a Cisco Secure Access Control Server (ACS) server for authentication and authorization. Using a Cisco Secure ACS server allows the user to assign preconfigured and custom administrator profiles for the CiscoWorks Management Center for PIX[®] Firewall, the CiscoWorks Management Center for VPN Routers, the Authentication Update Server, and other VMS Management Center applications.

Note: Even when Cisco Secure ACS authentication is used, CiscoWorks Common Services Software uses local authorization for CiscoWorks Common Services-specific utilities, such as backup and restore. To perform these actions, the user must be defined locally and be given the appropriate privilege level.

Before You Begin: Verify that your Cisco Secure ACS server is running version 3.1 or later. CiscoWorks Common Services Software is not compatible with earlier versions of Cisco Secure ACS. If your Cisco Secure ACS server is running a software version earlier than 3.1, upgrade your Cisco Secure ACS server before continuing.

Until the first Management Center to Cisco Secure ACS is registered, the Cisco Secure ACS server will only show the conventional Shared Profile Component (Figure 1).

Figure 1
 Shared Profile Component Prior to Management Center Registration





- Step 1. Create an administrator account on the Cisco Secure ACS server for CiscoWorks Common Services Software.

This is the administrator account that CiscoWorks Common Services uses to update Cisco Secure ACS settings for each client application. You can view the audit data for this administrator account to see what actions CiscoWorks Common Services Software is performing on the Cisco Secure ACS server. Refer to the *Cisco Secure ACS 3.1 for Windows User Guide* for instructions on configuring a Cisco Secure ACS administrator.

- Step 2. Configure the CiscoWorks Common Services server as a AAA client on the ACS server.

The CiscoWorks Common Services server must be configured as a client of the ACS server for authentication and authorization to occur. In the ACS graphical user interface (GUI), select Network Configuration and add an AAA client. In the example in Figure 2 the client is configured in the network device group name mc-group and is configured to use the TACACS+ AAA protocol.

Figure 2
Adding the CiscoWorks Common Services Server as an AAA Client

CISCO SYSTEMS Network Configuration

Edit

**AAA Client Setup For
pix-mc-test**

AAA Client IP Address: 192.168.79.236

Key: cisco

Network Device Group: mc-group

Authenticate Using: TACACS+ (Cisco IOS)

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

Submit Submit + Restart Delete Delete + Restart Cancel

- Step 3. Set the CiscoWorks Common Services Login Module to TACACS+.

To view the existing AAA server configuration, select VPN/Security Management Solution > Administration > Configuration > AAA Server from the navigation tree (Figure 3). This will bring up the AAA Server Information window (Figure 4). In this example, the AAA Server Information window shows the default configuration of CiscoWorks2000 local.



Figure 3
View AAA Server Selection in the Navigation Tree



Figure 4
AAA Server Information Window Configuration

The screenshot shows the 'AAA Server Information' window. At the top, there is a title bar and a Cisco Systems logo. Below the logo, a message says: 'Use this screen to enter the AAA Server information.' The main content area is titled 'AAA Server Info' and contains two radio buttons: 'ACS' and 'CiscoWorks2000 Local'. The 'ACS' radio button is selected. Below the radio buttons, there is a section titled 'Server Details' with two input fields: 'ACS Server' and 'ACS Port Number'. Below this, there is a section titled 'Login' with three input fields: 'Administrator Name', 'Password', and 'ACS Shared Secret'. At the bottom, there is a section titled 'Register/Unregister Applications' with two buttons: 'Register' and 'Unregister'. At the very bottom, there are three buttons: 'Finish', 'Synchronize', and 'Help'.



To select set the login module to TACACS+, follow these steps:

1. Select Server Configuration > Setup > Security > Select Login Module (Figure 5) from the navigation tree. The Select Login Module page appears (Figure 6).

Figure 5

Navigation Tree: Select Login Module

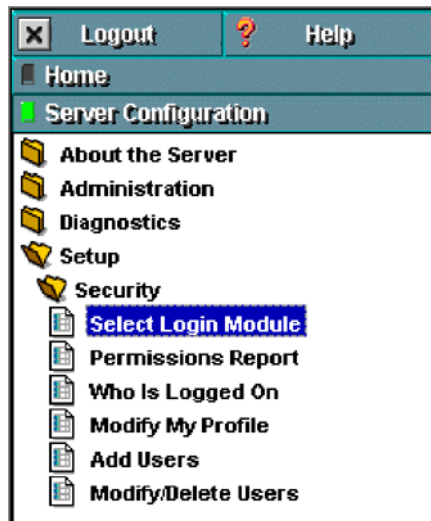
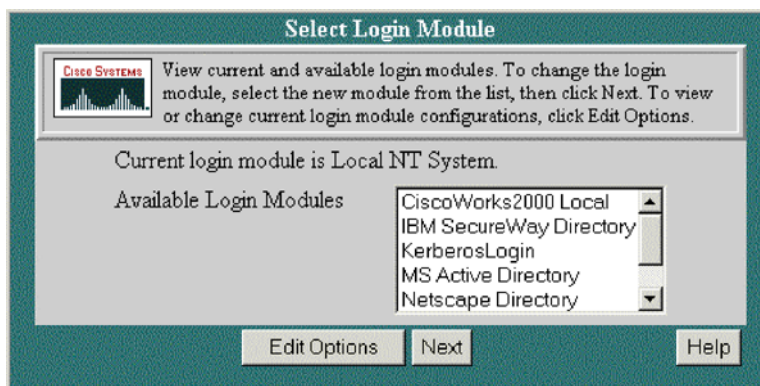


Figure 6

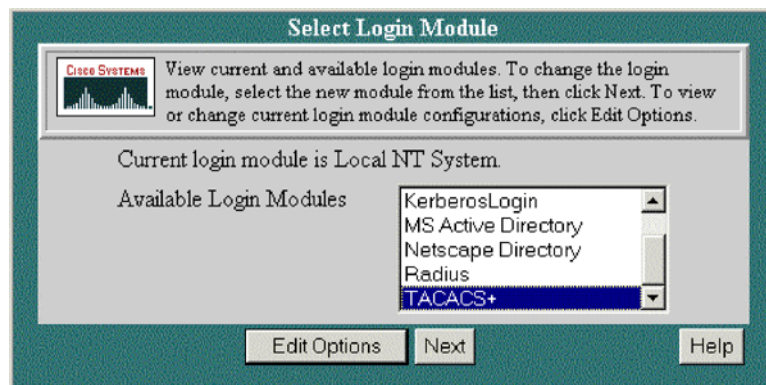
Select Login Module Window





- Click TACACS+ in the Available Login Modules field (Figure 7) and click Next.
The Login Module Options page appears (Figure 8).
- In the Server field, enter the server name or IP address of your ACS server.
- In the Port field, enter the ACS service port number (49 for TACACS+).
- In the Key field, enter the shared secret that was entered when you configured ACS to accept CiscoWorks Common Services as a client (see Figure 2).
- Select the False radio button next to Debug.

Figure 7
Selecting TACACS+ in the Select Login Module Window



- Select a login fallback option:

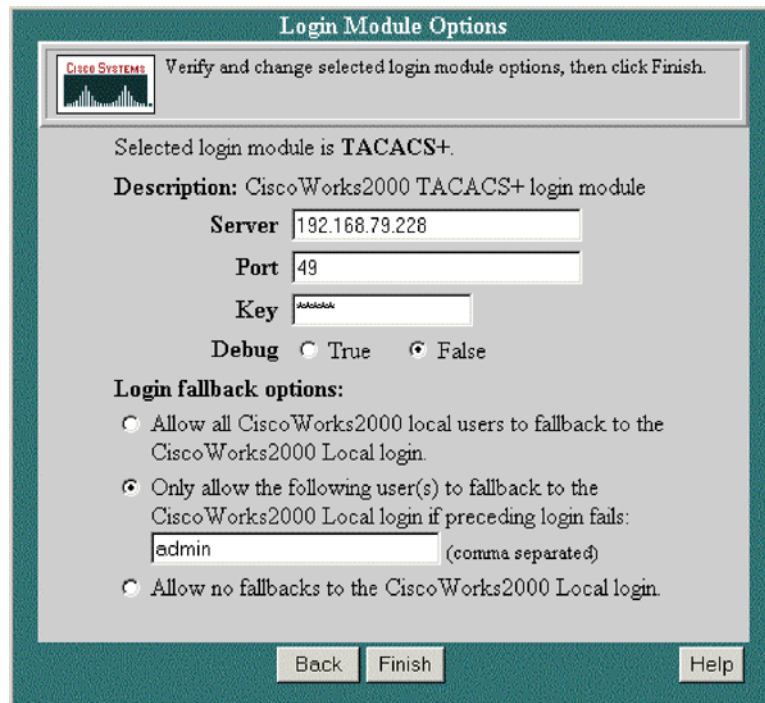
Fallback Option	Description
Allow all CiscoWorks2000 local users to fallback to the CiscoWorks2000 Local login	If the user cannot be authenticated against ACS, the system attempts to authenticate the user against the local user database. This requires a local account with the same name and password as the ACS user account.
Only allow the following user(s) to fallback to the CiscoWorks2000 Local login if preceding login fails:	This is the default setting. A list of users can be specified that will fall back to local authentication if ACS authentication fails. By default, the "admin" user appears in this field. Additional user names can be added by separating them with a comma. This requires a local account with the same name and password as the ACS user account.
Allow no fallbacks to the CiscoWorks2000 Local login	If the user cannot be authenticated against ACS, the login attempt fails.

In this example the default option is selected, as shown in Figure 8.

- Click Finish and the Select Login Module page appears once again (Figure 9), but now the current module is specified as TACACS+



Figure 8
Configuring TACACS+ in the Login Module Options



Login Module Options

Verify and change selected login module options, then click Finish.

Selected login module is **TACACS+**.

Description: CiscoWorks2000 TACACS+ login module

Server 192.168.79.228

Port 49

Key [masked]

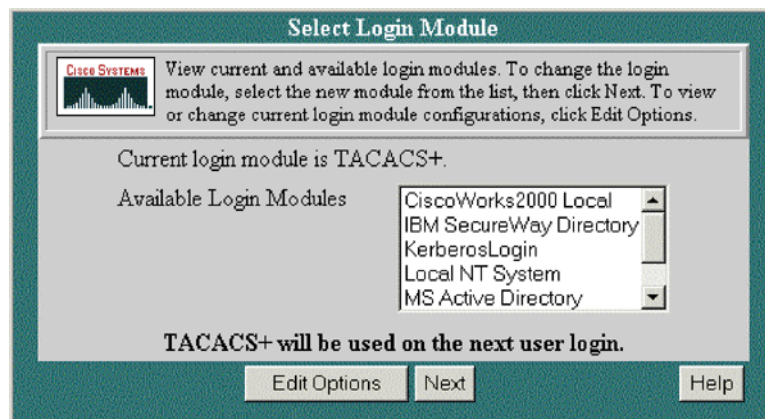
Debug ☐ True ☒ False

Login fallback options:

- ☐ Allow all CiscoWorks2000 local users to fallback to the CiscoWorks2000 Local login.
- ☒ Only allow the following user(s) to fallback to the CiscoWorks2000 Local login if preceding login fails:
admin (comma separated)
- ☐ Allow no fallbacks to the CiscoWorks2000 Local login.

Back Finish Help

Figure 9
TACACS+ Selected in the Select Login Module Window



Select Login Module

View current and available login modules. To change the login module, select the new module from the list, then click Next. To view or change current login module configurations, click Edit Options.

Current login module is **TACACS+**.

Available Login Modules

CiscoWorks2000 Local
IBM SecureWay Directory
KerberosLogin
Local NT System
MS Active Directory

TACACS+ will be used on the next user login.

Edit Options Next Help



Step 4. Synchronize the authentication server.

To specify the ACS Server information, follow these steps:

1. Select VPN/Security Management Solution > Administration > Configuration > AAA Server from the navigation tree.

The AAA Server Information page appears (Figure 10). The current authentication and authorization server, ACS, is selected.

Note: If the Login Module has been changed, the Synchronize button is active. If the Login Module has not been changed, the actions on this page cannot be performed.

Figure 10
AAA Server Information Data Entry

AAA Server Information

Use this screen to enter the AAA Server information.

AAA Server Info

☒ ACS ☐ CiscoWorks2000 Local

Server Details

ACS Server: 192.168.79.228

ACS Port Number: 49

Login

Administrator Name: superuser

Password: *****

ACS Shared Secret: *****

Register/Unregister Applications

Register Unregister

Finish Synchronize Help

2. Click Synchronize.

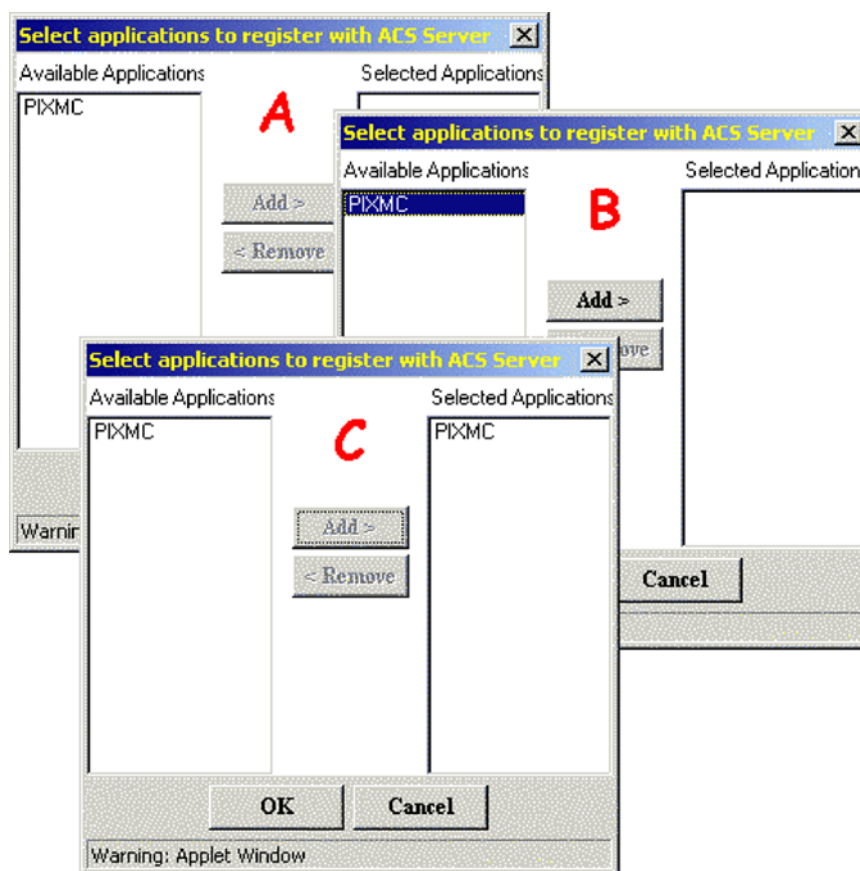
The selected authentication and authorization server changes to match the selection made on the Available Login Modules page. If the new authentication and authorization server is Cisco Secure ACS, the Server Details section is populated with the ACS server information that was entered on the Login Modules Options page and the Login and Register/Unregister Applications sections becomes available for input.



3. In the User Name field, enter the name of the administrative account that was set up in ACS for use by CiscoWorks Common Services.
4. In the Password field, enter the password for the administrative account.
5. In the ACS Shared Secret field, enter the shared secret that was created when specifying CiscoWorks Common Services as an ACS client.
6. Click Register.

The Select applications to register with ACS server dialog box appears (Figure 11-A).

Figure 11
Application Registration Selection Window



7. Select the client applications names in the Available Applications field that you want to register with Cisco Secure ACS (Figure 11-B), and then click Add.

The client application names move to the Selected Applications field (Figure 11-C).

8. Click OK.

The installed client applications register their roles and privileges with the ACS server. When the roles and privileges have been registered, a status message appears.



9. Click OK to close the status message.

10. Click Finish (Figure 10).

The Cisco Secure ACS username, password, and shared secret are saved. A status message appears (Figure 12 or Figure 13).

11. Click OK to close the status message.

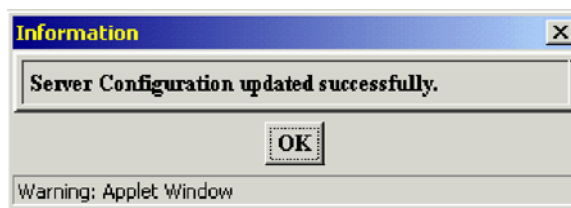
Figure 12

Application Previously Registered Message



Figure 13

Server Configuration Successful Message



Once a management center has been registered and synchronized with ACS, the appropriate entry is made available in the ACS Share Profile Components. In this example (Figure 14) the Management Center for PIX Firewalls (PIX MC) has been registered and the entry Management Center for PIX Firewalls is now available.

This option provides a set of “pre-canned” command authorization sets that are designed to look like the roles used in CiscoWorks2000 for administrators (Figure 15). ACS additionally provides the ability to configure these existing roles as well as add new user-configurable roles.

For more information concerning the application and configuration of these roles, please consult the user documentation for the PIX Management Center (*Using PIX MC 1.0 and AUS 1.0*) and the VPN Router Management Center (*Using Management Center for VPN Routers 1.0*).



Figure 14
Updated Shared Profile Components

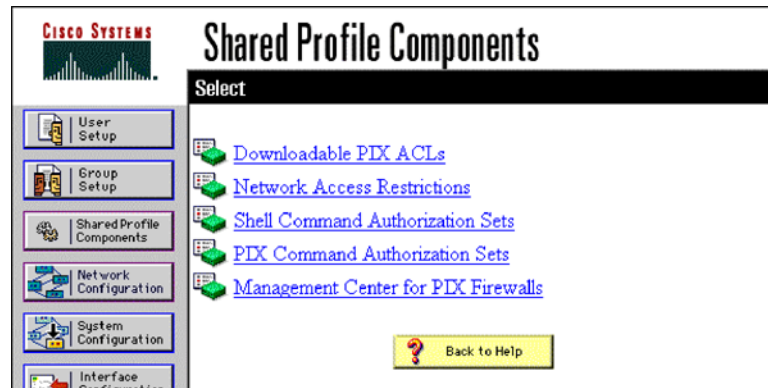
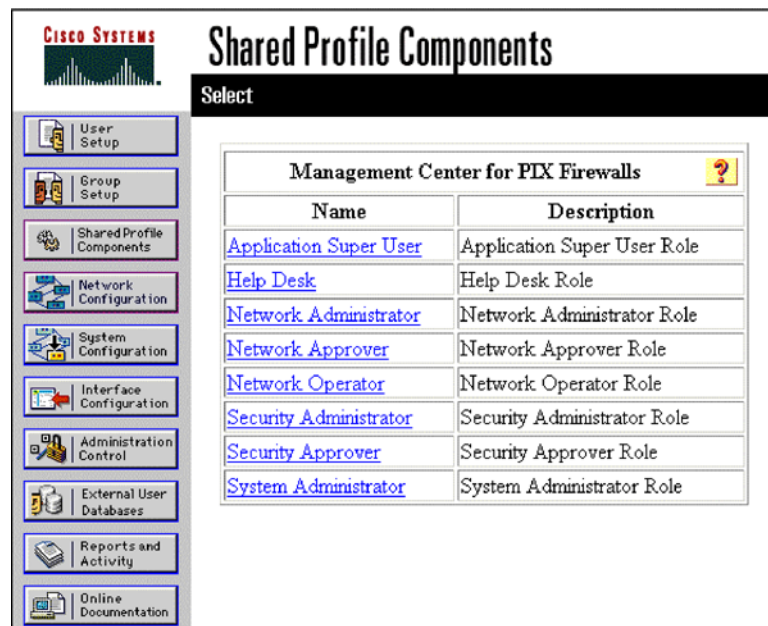


Figure 15
Shared Profile Components for the PIX Management Center





Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0208R) 202905/ETMG 11/02