



# CiscoWorks LMS Integration with Cisco Secure ACS

White Paper

# Contents

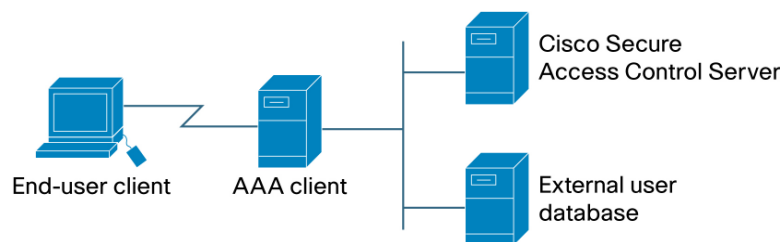
<a href="#">Introduction</a> .....	3
<a href="#">Installation of Cisco Secure ACS 4.1 Server</a> .....	4
<a href="#">Installing ACS 4.1</a> .....	4
<a href="#">Network and Port Requirements</a> .....	6
<a href="#">Verifying the ACS Installation</a> .....	6
<a href="#">Workflow for LMS/ACS Integration</a> .....	8
<a href="#">Add CiscoWorks Server as an AAA Client in ACS</a> .....	8
<a href="#">Add Network Devices as AAA Clients in ACS</a> .....	10
<a href="#">Switch CiscoWorks Server to AAA Mode</a> .....	11
<a href="#">Add the System Identity user</a> .....	14
<a href="#">Restart the Daemon Manager from the Command Line</a> .....	16
<a href="#">Verify the Integration</a> .....	16
<a href="#">Use Cases for LMS/ACS Integration</a> .....	17
<a href="#">Secure View: Limit the Device Access per User Group Level</a> .....	17
<a href="#">Role-Based Access Control: Edit Predefined User Roles and Create New Custom User Roles</a> .....	23
<a href="#">Appendix A: Generating Certificates in ACS for SSL Mode</a> .....	27
<a href="#">Appendix B: FAQ on Troubleshooting CiscoWorks LMS Integration with Cisco Secure ACS30</a> .....	
<a href="#">Appendix C: Export to ACS Server Using the CLI</a> .....	33

## Introduction

CiscoWorks LAN Management Solution (LMS) Common Services provides a robust security mechanism to manage identity and access to the CiscoWorks applications and data in a multiuser environment. As CiscoWorks has powerful network management tools for device configuration and software image management, unintended operations carried out by unauthorized users can cause disruptions to your network and in turn have a severe impact on the business-critical activities. CiscoWorks addresses this requirement by integrating with Cisco® Secure Access Control Server (ACS) to provide improved access control by means of authentication, authorization, and accounting (AAA).

ACS is a scalable, high-performance Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+) security server. As the centralized control point for managing enterprise network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco intelligent information networks. ACS provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a router, switches, network access server, PIX Firewall, and even the CiscoWorks server (Figure 1).

**Figure 1.** AAA Client Model



CiscoWorks can be integrated with an ACS server to address the following tasks:

- Provide centralized user management for a group of CiscoWorks servers.
- Provide device-level authorization. Device-level authorization restricts user access to perform certain tasks such as configuration updates and software image updates by authorizing the user for the task.
- Provide editable user roles. The user roles are mapped to tasks that the user is authorized to perform on the devices. ACS allows for the modification of the existing CiscoWorks user roles and for the creation of a new user role.
- Using ACS, groups of users can be assigned user roles per group of devices on a per application basis for the ultimate in authorization control.

The CiscoWorks server will be defined as an AAA client, just like network devices are. When a user tries to log in to the CiscoWorks server, the CiscoWorks server (AAA client) sends a request to the ACS server (AAA server) to authenticate the user, check the authorization, and audit the activities of the user.

This document provides a detailed explanation and step-by-step procedures for setting up CiscoWorks LMS to integrate with Cisco Secure ACS server. The versions of the software used in this white paper are:

- CiscoWorks LMS 3.0 with Common Services 3.1
- Cisco Secure ACS Server 4.1

**Note:** If multiple LMS or CSM servers are integrating with one ACS server, the Common Services modules on these servers must be of the same version.

### Installation of Cisco Secure ACS 4.1 Server

Before integrating your CiscoWorks Common Services with Cisco Secure ACS, you need to have completed the installation of CiscoWorks Common Services and Cisco Secure ACS on the appropriate servers and make sure that network connectivity exists between the two.

Cisco Secure ACS comes in two configurations:

- **Cisco Secure ACS for Windows:** Software for installation on Windows servers
- **Cisco Secure ACS Solution Engine:** A 1-rack-unit (1RU) hardware appliance with a preinstalled Cisco Secure ACS license

Cisco Secure ACS for Windows is suitable for customers who prefer to control their operating environment (this may include the type of hardware servers, OS, and installed services). In many cases, where security operations and server/OS operations are different departments in an IT organization, having a security solution on a dedicated appliance facilitates the manageability. In addition, the appliance solution provides benefits such as enhanced security, one-stop support, and a "plug-and-play" solution.

This white paper assumes that the user is selecting the first option to install ACS on their own. Otherwise please go directly to section 3 on page 10.

### Installing ACS 4.1

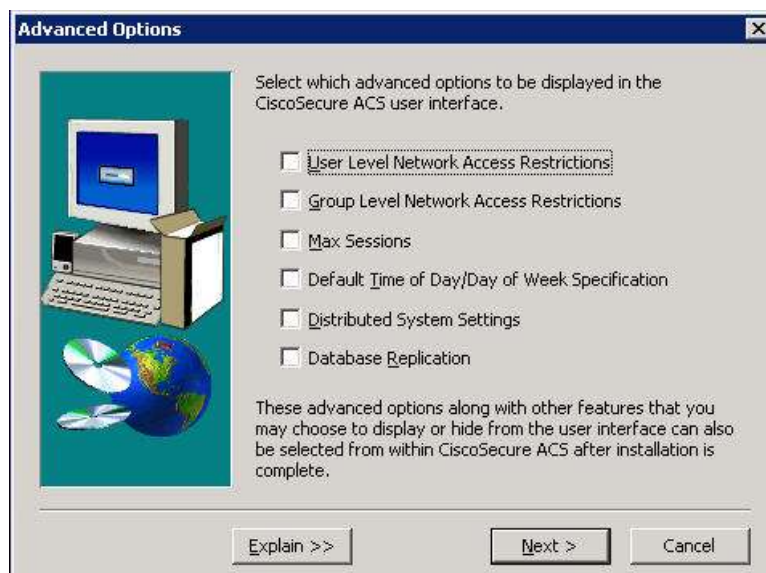
Table 1 lists the system requirements for installing Cisco Secure ACS.

**Table 1.** System Requirement for ACS 4.1

Component	Minimum Requirement
<b>Hardware</b>	<ul style="list-style-type: none"> <li>• IBM PC-compatible with Pentium 4 processor, 1.8 GHz or faster</li> <li>• Color monitor with minimum graphics resolution of 256 colors at 800 x 600 resolution</li> <li>• CD-ROM drive</li> <li>• 100BaseT or faster connection</li> </ul>
<b>Operating system</b>	<ul style="list-style-type: none"> <li>• Windows 2000 Server (English version only)</li> <li>• Windows 2000 Advanced Server (Service Pack 4) without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed (English version only)</li> <li>• Windows Server 2003, Enterprise Edition or Standard Edition (Service Pack 1)</li> </ul>
<b>File system</b>	New Technology File System (NTFS)
<b>Memory</b>	1 GB, minimum
<b>Virtual memory</b>	1 GB, minimum
<b>Hard drive space</b>	At least 1 GB of free hard drive space, minimum <b>Note:</b> The actual amount of hard drive space required depends on several factors, including log file growth, and replication or backup purposes.

The setup program for ACS 4.1 is quite straightforward, just like any other Windows installation programs. The user can finish the installation easily by following the GUI messages. Most of the advanced options can be kept as default if there is no need to customize the ACS server settings (Figure 2).

**Figure 2.** ACS 4.1 Installation



For detailed information, consult the **Installation Guide for Cisco Secure ACS** at [http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_secure\\_access\\_control\\_server\\_for\\_windows/4.1/installation/guide/windows/install.html#wp1041324](http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/installation/guide/windows/install.html#wp1041324).

You need to have administrative privileges for the Cisco Secure ACS server and CiscoWorks server to be able to execute the steps explained in this document.

Common Services 3.1 supports the following versions of Cisco Secure ACS for Windows Server:

- Cisco Secure ACS 3.2 for Windows Server
- Cisco Secure ACS 3.2.3 for Windows Server
- Cisco Secure ACS 3.3.2 for Windows Server
- Cisco Secure ACS 3.3.3 for Windows Server
- Cisco Secure ACS 3.3.4 for Windows Server
- Cisco Secure ACS 4.0.1 for Windows Server
- Cisco Secure ACS 4.1 for Windows Server
- Cisco Secure ACS 4.1.1 for Windows Server
- Cisco Secure Appliance 3.3.3
- Cisco Secure Appliance 3.3.4
- Cisco Secure Appliance 4.0.1
- Cisco Secure Appliance 4.1
- Cisco Secure Appliance 4.1.1

It is recommended that you install the patches, such as the Admin HTTPS PSIRT patch, for the earlier versions.

To install the patch:

- Go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acis-win>.
- Click the **Download Cisco Secure ACS Software (Windows)** link. You can find the link to the Admin HTTPS PSIRT patch in the table.

### Network and Port Requirements

CiscoWorks uses TACACS+ to integrate with ACS. Make sure that the gateway devices between AAA clients and Cisco Secure ACS allow communication over the ports needed to support the TACACS+ protocol for Cisco Secure ACS to provide AAA services to the AAA client.

It is recommended to open all ports on ACS prior to the integration, and then close unused ports after the integration. Table 2 lists the port numbers to be allowed by the gateway devices.

**Table 2.** Port Numbers for the Gateway Devices

Feature/Protocol	UDP or TCP?	Ports
TACACS+	TCP	49
Cisco Secure Database Replication	TCP	2000
RDBMS Synchronization with synchronization partners	TCP	2000
User-Changeable Password web application	TCP	2000
Logging	TCP	2001
Administrative HTTP port for new sessions	TCP	2002
Administrative HTTP port range	TCP	Configurable; default 1024 through 65535

ACS Server can be accessed across remote machines from the browser; it uses the port number 2002 for its communication.

**Note:** Cisco Secure ACS and CiscoWorks Common Services cannot coexist on the same server due to a port number conflict.

To find out more on how to install, maintain, and operate Cisco Secure ACS, refer to the online documentation at

[http://www.cisco.com/en/US/products/sw/secursw/ps2086/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2086/tsd_products_support_series_home.html).

### Verifying the ACS Installation

After ACS 4.1 is successfully installed, the first thing you need to do is to create an administrator user so you can access the ACS server remotely using a Web browser.

**Note:** If ACS is running on an appliance, the appliance administrator cannot be used as the ACS administrator for LMS integration. The ACS appliance administrator will be visible on the main Administration Control page.

To create the user administrator:

Step 1. Log in to the ACS server locally or through Remote Desktop if it is available.

Step 2. The ACS installation program created a desktop icon for ACS Admin. Double-click the desktop icon to open the browser interface, or manually start Internet Explorer/Firefox and point to <http://127.0.0.1:6729>. See Figure 3.



**Figure 3.** Cisco Secure ACS 4.1 Browser Interface



**Note:** If you cannot view the ACS Web interface, check whether your Internet Explorer/Firefox application is up to date and Java is installed on the local machine.

Step 3. From the menu on the left side, click the **Administration Control** button. Then add the username you can want to add, for example, **administrator**, as in the figure 4.

Figure 4. Administration Control Window



Follow the screen to give the password and click the **Grant All** button to give all administrative privileges to the administrator (Figure 5).

Figure 5. The Administrator Privileges Window



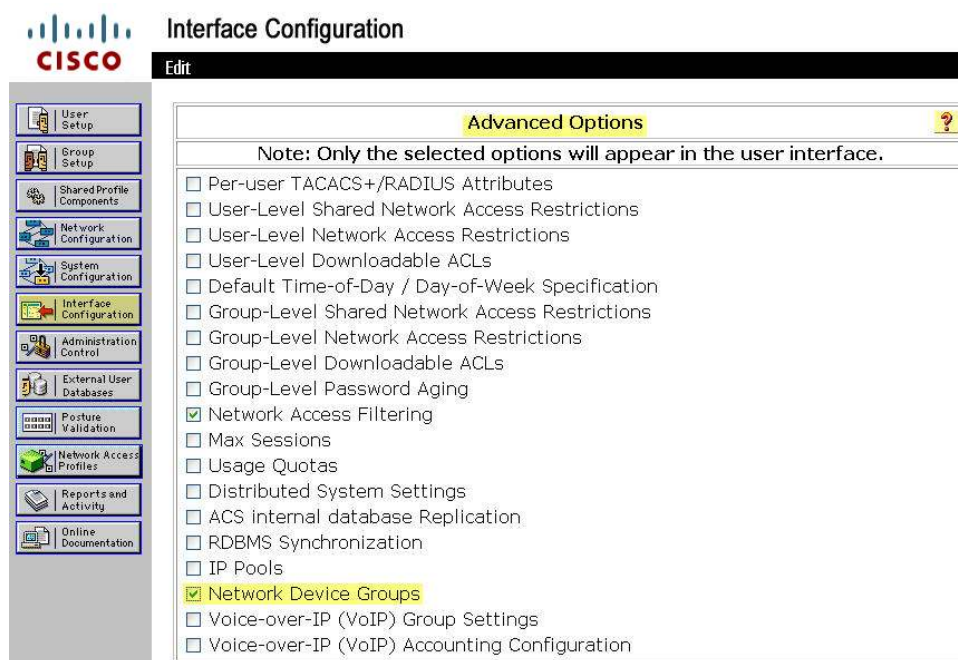
After the administrator user is created, you can log in to the ACS server remotely through the browser at <http://servername:2002>. Port 2002 is the default port for ACS server Web access.

## Workflow for LMS/ACS Integration

### Add CiscoWorks Server as an AAA Client in ACS

By default, ACS allows the user to add AAA clients individually. The best practice is to use a network device group (NDG) so you can group the AAA clients and manage them as groups. To use an NDG, you need to turn on the NDG option under Interface Configuration/Advanced Options (Figure 6).

Figure 6. Advanced Options



Then go to Network Configuration to add the CiscoWorks server as an NDG (Figure 7).

Figure 7. Network Configuration



Click **Add Entry** to add a new NDG LMS server (Figure 8).

Figure 8. New Network Device Group Window

**New Network Device Group**

Network Device Group Name: LMS Server

Shared Secret: trust

**RADIUS Key Wrap**

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format:  ASCII  Hexadecimal

Submit Cancel

Then add the LMS server itself as an AAA client to the NDG you just created. The LMS server must be added to ACS as a TACACS+ (Cisco IOS) client even though the server does not run Cisco IOS® Software (Figure 9).

**Figure 9.** Adding an AAA Client

**Add AAA Client**

AAA Client Hostname	lms server1
AAA Client IP Address	192.168.141.207
Shared Secret	trust
Network Device Group	LMS Server
<b>RADIUS Key Wrap</b>	
Key Encryption Key	
Message Authenticator Code Key	
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal
Authenticate Using	TACACS+ (Cisco IOS)
<input checked="" type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure) <input checked="" type="checkbox"/> Log Update/Watchdog Packets from this AAA Client <input checked="" type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client <input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client <input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	

In the Shared Secret box, type the shared secret key that your CiscoWorks server and Cisco Secure ACS use to encrypt the data (up to 32 characters).

**Note:** For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive.

From the **Authenticate Using** list, select the network security protocol used by the AAA client. Here we selected TACACS+.

Uncheck the single connection TACACS+ option. This must not be used for LMS integration.

If you want to log watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box.

If you want to log RADIUS tunneling accounting packets, select the **Log RADIUS Tunneling Packets from this AAA Client** check box.

If you want to track session state by username rather than port number, select the **Replace RADIUS Port info with Username from this AAA** check box.

**Note:** If you select this option, Cisco Secure ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through an AAA client with this feature selected.

**Note:** Restart the ACS service by going to System Options.

#### Add Network Devices as AAA Clients in ACS

Before you register LMS applications with ACS, it is recommended to add all the devices into ACS so both LMS and ACS have the complete list of devices in their database.

There are two ways to do this; one is to export the device list from LMS to ACS using the `dcrcli` command utility; the other way is add the devices manually.

- Export LMS devices to ACS using `dcrcli`.

See Appendix C for how to use `dcrcli`.

- Manually add devices.

For example, in Figure 10, three NDG groups are created, Core, NorCal, and SoCal. These NDGs will be used in the example in the section “Secure View: Limit the Device Access per User Group Level.”

**Figure 10.** Network Device Groups

Network Device Groups		
Network Device Group	AAA Clients	AAA Servers
<a href="#">Core</a>	1	0
<a href="#">LMS Server</a>	1	0
<a href="#">NorCal</a>	1	0
<a href="#">SoCal</a>	1	0
<a href="#">(Not Assigned)</a>	0	1

Add devices into the NDGs. For example, Figure 11 shows the IP address range or individual IP addresses specified for the NDGs.

**Figure 11.** Specifying the Address or Address Ranges for the NDGs

NorCal AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">NorCalDevices</a>	192.168.141.211-230	TACACS+ (Cisco IOS)

SoCal AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">SoCalDevices</a>	192.168.141.231-240	TACACS+ (Cisco IOS)

Core AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">distributionswitches</a>	192.168.141.200 192.168.141.210	TACACS+ (Cisco IOS)

### Switch CiscoWorks Server to AAA Mode

Now it is time to change the AAA mode from non-ACS to ACS. Go to **Common Service > Security > AAA Mode Setup** (see Figure 12).

Figure 12. Common Services AAA Mode Setup

Here is an explanation of the options available on this screen.

### Server Details

Cisco Works Common Services Software supports up to three backup servers. When the primary Cisco Secure ACS server fails, the AAA requests are redirected to the secondary or backup servers. You can have multiple backup servers for a higher level of redundancy.

It is not mandatory to have all three Cisco Secure ACS servers. You can still have a single primary server.

When you have multiple Cisco Secure ACS servers for backup, make sure that the configurations on all servers are synchronized.

**Note:** If you enter the hostname instead of the ACS server IP in Solaris, make sure the hostname is resolvable through either Domain Name System (DNS) or the local hosts file.

ACS TACACS+ Port: Port number 49 is utilized by Cisco Secure ACS for the TACACS+ communication.

### Login

ACS Admin Name: Enter the administrator user name that you would use to log in to Cisco Secure ACS. This is the same user you created under Administration Control in ACS.

ACS Admin Password: Enter the administrator password that you would use to log in to Cisco Secure ACS.

ACS Shared Key: Enter the shared secret key that you entered in Cisco Secure ACS while adding the CiscoWorks Common Services server as an AAA client.

## Application Registration

You can choose to register all installed applications with Cisco Secure ACS by selecting the check box under Application Registration. But you need to know about the following before registering the applications with Cisco Secure ACS:

- Authorization in CiscoWorks is done based on tasks available for every application. The task definition and task to role mapping are available in three XML files. They are:
  - <App name>TaskDefinition.xml
  - <App name>RoleDefinition.xml
  - <App name>Tasks.xml
- By default five predefined roles are available. However, Cisco Secure ACS provides the feature of customized roles, wherein you can create a new role or edit the privileges of the predefined roles. See the section “Role-Based Access Control: Edit Predefined User Roles and Create New Custom User Roles” about this topic.
- In case of an application being reregistered from Common Services, the custom roles (if any) created for that application would be lost. The application registration from the AAA Mode Setup will reregister all the installed applications to Cisco Secure ACS, which will cause the custom roles (if any) to be lost. But this mass application registration can be avoided by using the command-line interface (CLI) script **AcsRegCli.pl** as explained later.

## ACS Communication on HTTPS

Cisco Secure ACS supports secured communication through the Secure Sockets Layer (SSL) mode. HTTP/HTTPS mode is used for device cache initialization, application registration, and administration purposes.

It is recommended to use HTTP to set up LMS integration with ACS. This comes with less overhead, and allows sniffer traces to be collected

In case you have to use HTTPS, select the check box option under ACS Communication on HTTPS when Cisco Secure ACS is configured to work in HTTPS mode.

**Note:** When you select HTTPS mode, make sure that the backup servers are also in HTTPS mode.

**Note:** The SSL mode is not applicable to the TACACS+ or RADIUS security protocols, which are used for authentication and authorization between AAA clients and the server.

Refer to Appendix A of this document for information on selecting HTTPS mode and installing security certificates on Cisco Secure ACS.

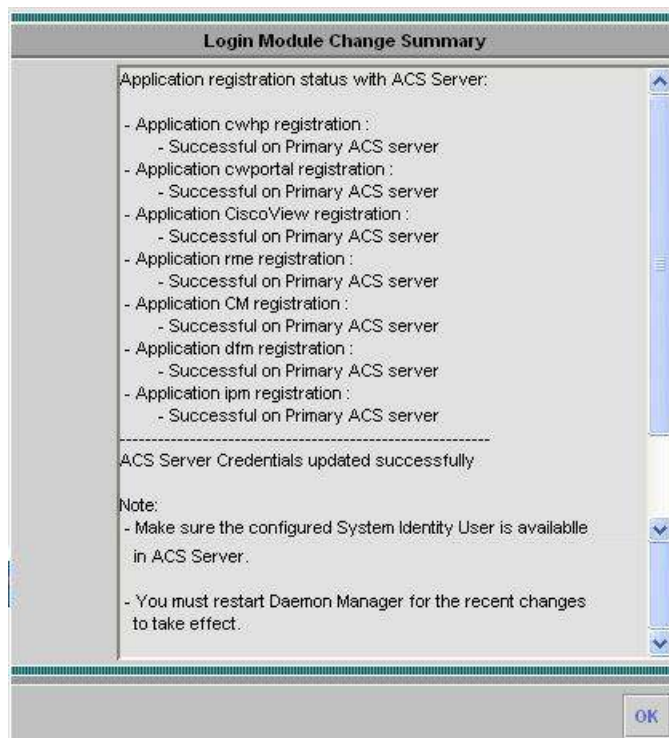
After clicking the **Apply** button, one message shows up (Figure 13).

**Figure 13.** Verification Status

Click the **Apply** button again to register the applications.

**Note:** If you have registered before, clicking the **Apply** button will lose all the custom roles created in ACS.

Figure 14 shows that the LMS applications have been registered successfully to ACS.

**Figure 14.** Login Module Change Summary

### Add the System Identity user

The System Identity user makes possible the trusted communication between LMS and ACS servers. It must be properly set up on both the LMS and ACS servers.

First, in LMS Common Services, add the System Identity user under **Local User Setup** and assign it all the default roles (Figure 15).

Figure 15. Local User Setup

Then specify the System ID under **Common Service > Server > Security > System Identity Setup** (Figure 16).

Figure 16. System Identity Setup

In ACS, create a group named SuperAdmin and create a user systemiduser to belong to this group.

First, create the SuperAdmin group (Figure 17)

**Figure 17.** Creating the SuperAdmin Group

#### Ciscoverworks

- None  
 Assign a Ciscoverworks for any network device  
 Assign a Ciscoverworks on a per Network Device Group Basis

Device Group

Remove Association

Device Group

LMS Server

Approver

Add Association

- cwportal  
 Custom attributes

#### CiscoWorks Portal

- None  
 Assign a CiscoWorks Portal for any network device  
 Assign a CiscoWorks Portal on a per Network Device Group Basis

Then create and assign a user systemiduser to this SuperAdmin group.

#### Restart the Daemon Manager from the Command Line

##### On Windows:

1. Enter `net stop crmdmgt.d.`
2. Enter `net start crmdmgt.d.`

##### On Solaris:

1. Enter `/etc/init.d/dmgt.d stop.`
2. Enter `/etc/init.d/dmgt.d start.`

#### Verify the Integration

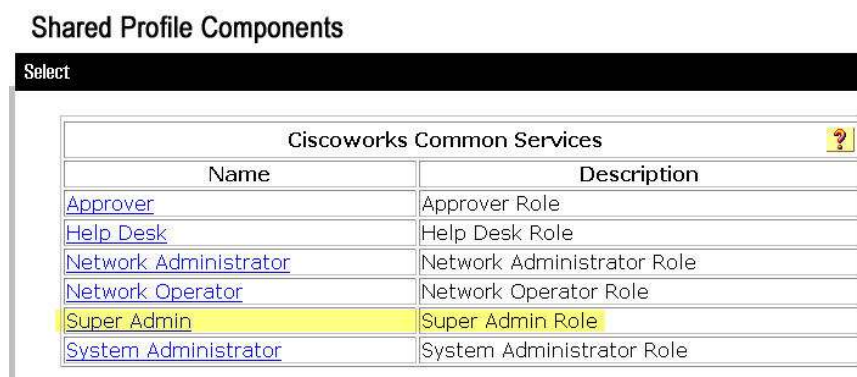
To verify the integration, log in to ACS as administrator, click **Shared Profile Components** and check to make sure that all the LMS applications show up (Figure 18).

Figure 18. Shared Profile Components



Also notice under each application, such as **Common Services**, a new Super Admin user role is created (Figure 19).

Figure 19. CiscoWorks Common Services Shares Profile Components



**Note:** Since you have not created any user on ACS, the CiscoWorks server is not open for access yet. Please perform the steps in the scenarios described below to create ACS users to get access to CiscoWorks.

### Use Cases for LMS/ACS Integration

Here are two typical use cases for integrating LMS with ACS for the AAA functions.

#### Secure View: Limit the Device Access per User Group Level

Here is a typical use case:

Acme Corp is a corporation headquartered in Central California. The company has two branch offices, one in Northern California, another one in Southern California. There are three groups of network administrators:

- The SuperAdmin group is in charge of the whole network. Members of this group must have access to all the devices and be able to perform all management tasks on the network.
- The SoCal group is responsible only for the Southern California office network. Members of

this group are allowed to perform management tasks only on the devices in their office.

- The NorCal group is responsible only for the Northern California office network. Members of this group are allowed to perform management tasks only on the devices in their office.

To meet this goal, you can separate the network devices into three NDGs:

- The core NDG: Network devices for the headquarters in Central California
- The SoCal NDG: Network devices in the Southern California office
- The NorCal NDG: Network devices in the Northern California office

The SuperAdmin administrator group will have access and control on all the NDGs. SoCal administrators will have access and control only for the SoCal NDG. NorCal administrators will have access and control only for the NorCal NDG. This way you can create secure views of the network that limit the management scope based on the group of the administrators.

Step 1. Create NDG groups for the devices (Figure 20).

**Figure 20.** Creating NDG Groups for the Devices

Network Device Groups		
Network Device Group	AAA Clients	AAA Servers
<a href="#">Core</a>	1	0
<a href="#">LMS Server</a>	1	0
<a href="#">NorCal</a>	1	0
<a href="#">SoCal</a>	1	0
<a href="#">(Not Assigned)</a>	0	1

Add devices into the NDGs. For example, Figure 21 shows the IP address ranges for the NorCal, SoCal, and Core NDGs.

**Figure 21.** Address Ranges for the NDGs

NorCal AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">NorCalDevices</a>	192.168.141.211-230	TACACS+ (Cisco IOS)

SoCal AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">SoCalDevices</a>	192.168.141.231-240	TACACS+ (Cisco IOS)

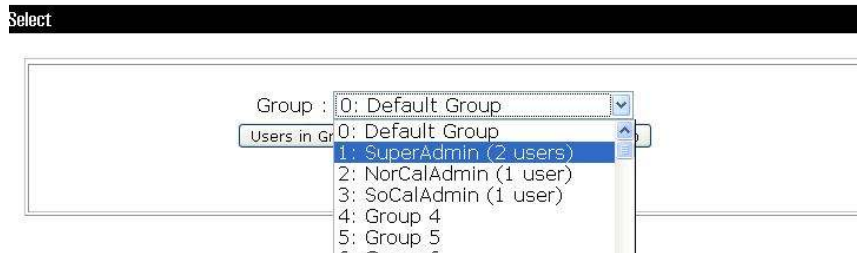
Core AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">distributionswitches</a>	192.168.141.200 192.168.141.210	TACACS+ (Cisco IOS)

Step 2. Create user groups for the administrators.

First, click the **Group Setup** menu, then rename the default Group 1 as the SuperAdmin group, Group 2 as NorCalAdmin, and Group 3 as SoCalAdmin (Figure 22).

**Figure 22.** Renaming the Groups

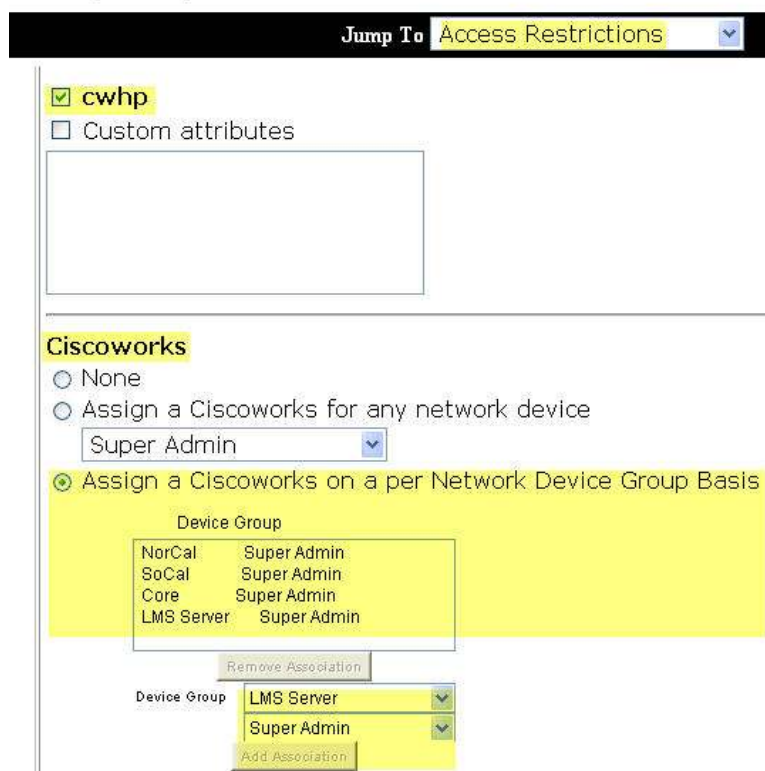
## Group Setup



Select the group and choose **edit setting**. For example, for the SuperAdmin group, scroll down until you see the LMS applications. Then grant access to all the NDG groups as the superadmin role by adding associations from the dropdown lists. Make sure it has superadmin permission to both the device groups NDG and the LMS server NDG (Figure 23).

**Figure 23.** Group Setup

## Group Setup



Repeat for all the application for the SuperAdmin group.

For the NorCal group, perform the same operation on all LMS applications but limit its access to only the NorCal NDG. Make sure it also has superadmin permission to the LMS server NDG (Figure 24).

**Figure 24.** The NorCal NDG

cwhp  
 Custom attributes

---

**Ciscoverks**

None  
 Assign a Ciscoverks for any network device  
  
 Assign a Ciscoverks on a per Network Device Group Basis

Device Group	
NorCal	Super Admin
LMS Server	Super Admin

Device Group

Notice the NorCal administrator group can only access the NorCal NDG and the LMS server NDG.

Similarly for the SoCal administrator, access is granted to only the SoCal NDG and LMS Server (Figure 25). Make sure it also has superadmin permission to the LMS server NDG.

**Figure 25.** The SoCal NDG

cwhp

Custom attributes

---

**Ciscoverks**

None

Assign a Ciscoverks for any network device

Approver ▼

Assign a Ciscoverks on a per Network Device Group Basis

Device Group

SoCal	Super Admin
LMS Server	Super Admin

Remove Association

Device Group SoCal ▼

Super Admin ▼

Add Association

**Step 3.** Create users and assign them to different user groups.

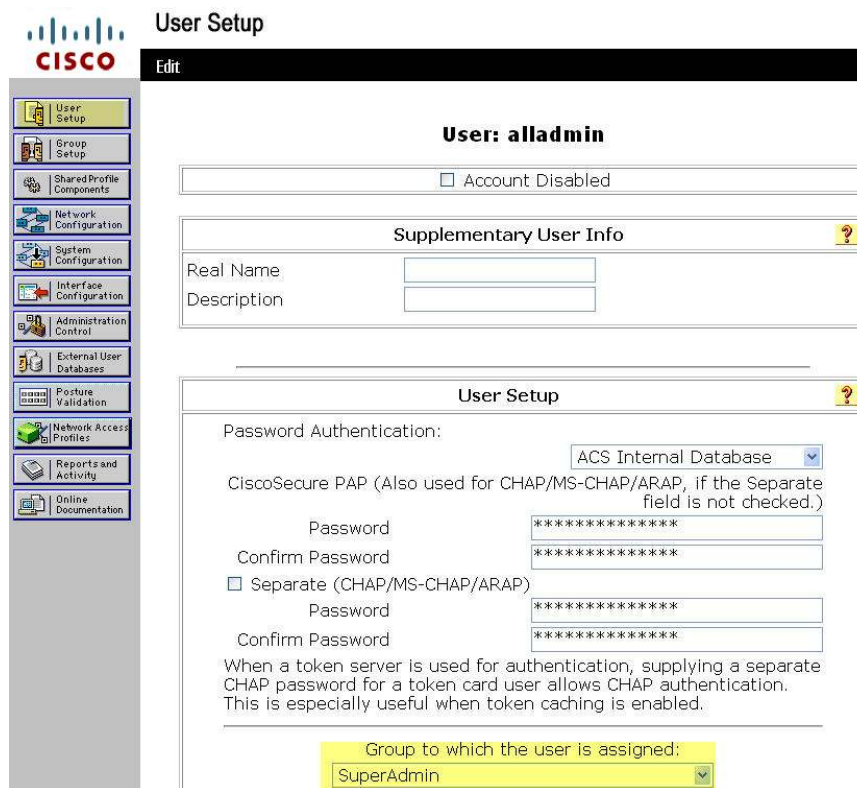
Now you are ready to create the administrator as ACS users and assign them to different user groups.

Create three users:

- alladmin belongs to the SuperAdmin group.
- lajolla belongs to the SoCalAdmin group.
- nobhill belongs to the NorCalAdmin group.

As an example, the Figure 26 shows that the alladmin user is assigned to the SuperAdmin group.

Figure 26. The User alladmin



Step 4. Verify the setup.

To verify the setup, log in to LMS using the different user names just created. Go to **Common Services/Device Management**, and make sure the users can only see their assigned devices. For example, user alladmin can see all devices, also under the System view (Figure 27).

Figure 27. DCR and AAA Information

DCR and AAA Information	
Authentication Mode	TACACS+
Authorization Mode	ACS
SSO Mode	Standalone
Authorized Devices	32
Devices Not Configured in ACS	0
DCR Mode	Standalone

If the user is granted access to only part of the network, the rest of the devices will show up in Devices Not Configured in ACS. For example, user lajolla can only see 10 devices; the other 22 devices are marked as Devices Not Configured in ACS (Figure 28).

**Figure 28.** Access for User lajolla

DCR and AAA Information	
Authentication Mode	TACACS+
Authorization Mode	ACS
SSO Mode	Standalone
Authorized Devices	10
Devices Not Configured in ACS	22
DCR Mode	Standalone

The last step to verify the integration works is to perform some management jobs such as device discovery in Campus Manager, sync archive in Resource Manager Essentials (RME), and so on. If the task can be started and finished as expected, the integration is considered a success.

**Note:** If the task cannot be started due to permission error, then something is wrong with the integration. Some possible reasons are:

- The user group is not assigned with proper permissions to carry out the job.
- The System Identity user is not set up properly. Remember it must belong to the SuperAdmin group.

#### Role-Based Access Control: Edit Predefined User Roles and Create New Custom User Roles

CiscoWorks LMS has five predefined local user roles. These roles cannot be edited or customized. The only way to create customized roles is to integrate with ACS.

Here are the default five predefined local user roles:

- **Help Desk (default role for all users):** Can access network status information only. Can access persisted data on the system but cannot perform any action on a device or schedule a job that will reach the network.
- **Approver:** Can approve all tasks.
- **Network Operator:** Can do all Help Desk tasks. Can do tasks related to network data collection but cannot do any task that requires write access on the network.
- **Network Administrator:** Can do all Network Operators tasks. Can do tasks that result in a network configuration change.
- **System Administrator:** Can perform all CiscoWorks system administration tasks.

These roles determine which CiscoWorks applications, tools, and product features you are allowed to access. Roles are not set up hierarchically, with each role including all the privileges of the role "below" it. Instead, these roles provide access privileges based on user needs.

You can view the permission in details by generating a Permission Report under **Common Services/Server/Reports** (Figure 29).

**Figure 29.** Permission Report

**Permission Report**  
WARNING: This report is not valid for ACS Mode of Security.

Go to: <<Select an Item>>

**CiscoWorks Common Services**

**Homepage Configuration > Application Registration**

Task/Name	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Register	X				
Search Registry	X	X	X	X	X
Unregister	X				

**Homepage Configuration > Link Registration**

Task/Name	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Register	X	X			
Unregister	X	X			

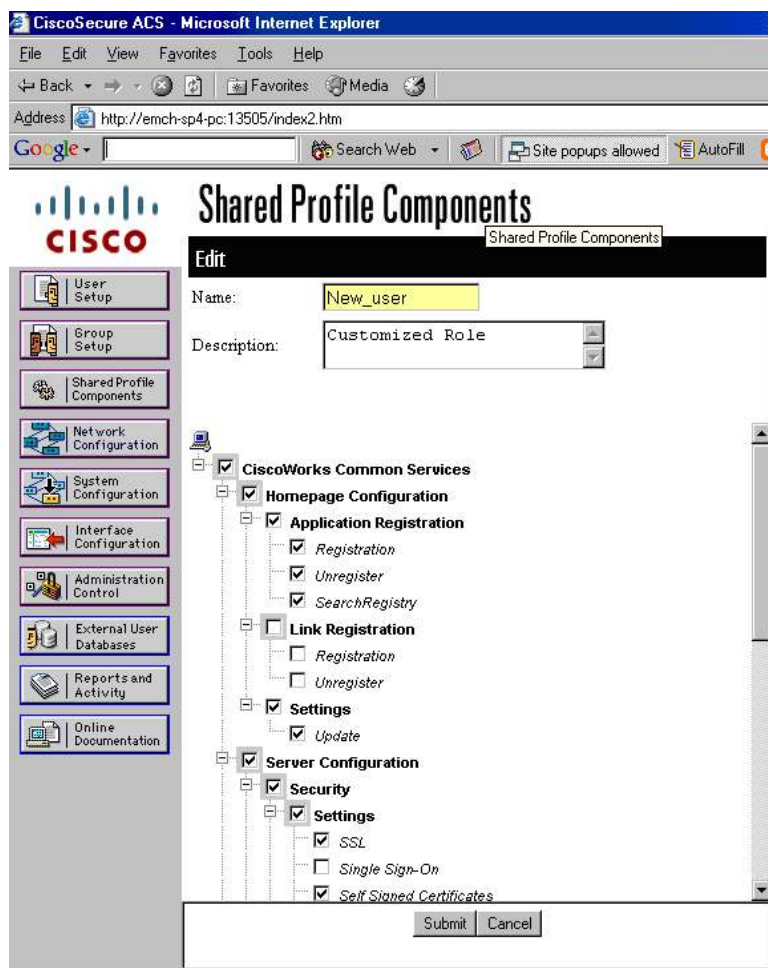
**Note:** This Permission Report is for the local user role only. It will not reflect the change after integration with ACS.

After integrating with ACS, you can create new custom roles to provide role-based access control (RBAC). Please do not edit the predefined roles.

### Adding a New Role

To add a new CiscoWorks role on Cisco Secure ACS:

1. Select **Shared Profile Components > CiscoWorks Common Services** and click the **Add** button to add a new role. The new role definition page will appear as show in the Figure 30.
2. Select or deselect any of the Common Services tasks that suit your business workflow and needs of the new role.
3. Click **Submit**.

**Figure 30.** Shared Profile Components: Adding a New CiscoWorks Common Services Role

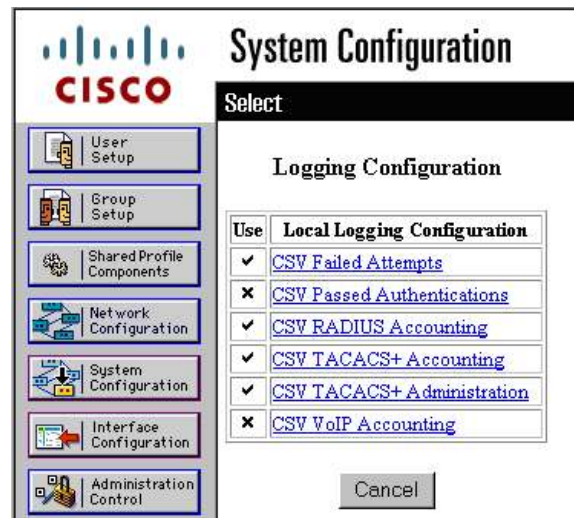
After the new customized role is created, you can create new users in ACS and assign them to these roles for proper access permission.

### Logs and Reports

Cisco Secure ACS logs a variety of user and system activities. Depending on the log, and how you have configured Cisco Secure ACS, logs can be recorded in different formats with different attributes.

The logging can be enabled from the Logging configuration under the System Configuration (Figure 31). Refer to the Cisco Secure ACS User Guide section on system configuration for more information.

Figure 31. System Configuration: Logging

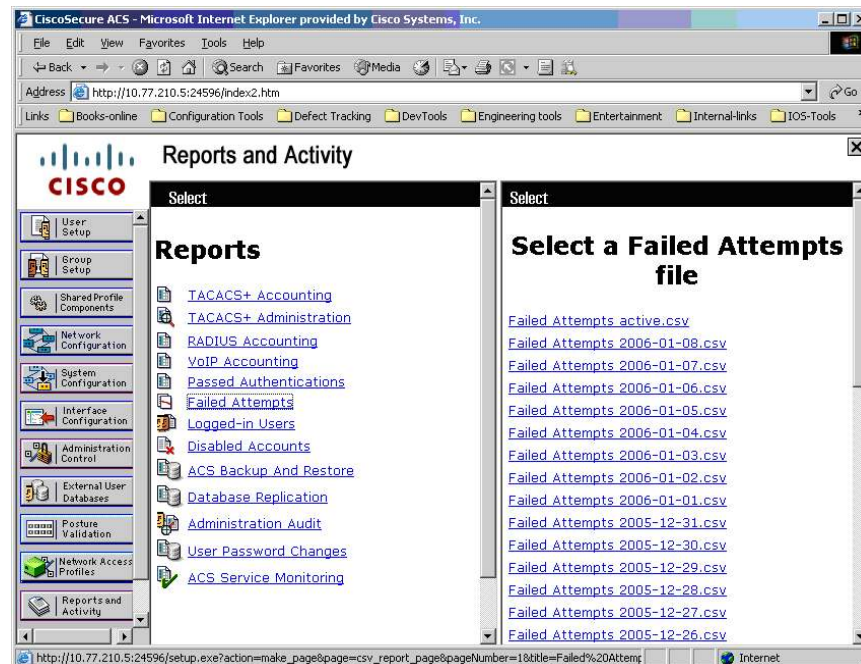


You can enable the following three logs, which can be useful when you are debugging CiscoWorks-related user activities and events:

- **Passed Authentications:** Contains the details of passed authentication
- **Failed Attempts:** Contains the information for failed authentication and authorizations
- **TACACS+ Administration:** Audit records

The reports and logs can be viewed from the Cisco Secure ACS Reports and Activity page (Figure 32).

Figure 32. Reports and Activity



## Appendix A: Generating Certificates in ACS for SSL Mode

The ACS Certificate Setup pages help enable you to install digital certificates to support HTTPS for secure access to the Cisco Secure ACS HTML interface.

HTTP/HTTPS is used for the following operations between the CiscoWorks server and Cisco Secure ACS:

- Import/export device groups
- Import/export devices
- Audit requests
- Initialize device cache (which in turn calls Import devices)
- Register/unregister applications

Perform this procedure to install a server certificate for your Cisco Secure ACS. You can perform certificate enrollment to support HTTPS for HTML Interface to Cisco Secure ACS. There are three basic options by which you can install the server certificate; you may:

- Obtain a certificate from a CA
- Use an existing certificate from local machine storage
- Generate a self-signed certificate

### Installing the Certificate from Local Machine Storage

Before you install the certificate, you must have a server certificate for your Cisco Secure ACS. With Cisco Secure ACS, certificate files must be in Base64-encoded X.509. If you do not already have a server certificate in storage, refer to the procedure under the section [Generating a Certificate Signing Request](#) in the Cisco Secure ACS User Guide, or any other means, to obtain a certificate for installation.

If you are installing a server certificate that replaces an existing server certificate, the installation could affect the configuration of the CTL and CRL settings your Cisco Secure ACS. After you have installed a replacement certificate, you should determine whether you need to reconfigure any CTL or CRL settings.

To install an existing certificate for use on Cisco Secure ACS, follow these steps:

Step 1. In the navigation bar, click **System Configuration**.

Step 2. Click **ACS Certificate Setup**.

Step 3. Click **Install ACS Certificate**.

Cisco Secure ACS displays the Install ACS Certificate page.

Step 4. You must specify whether Cisco Secure ACS reads the certificate from a specified file or uses a certificate already in storage on the local machine. Do one of the following:

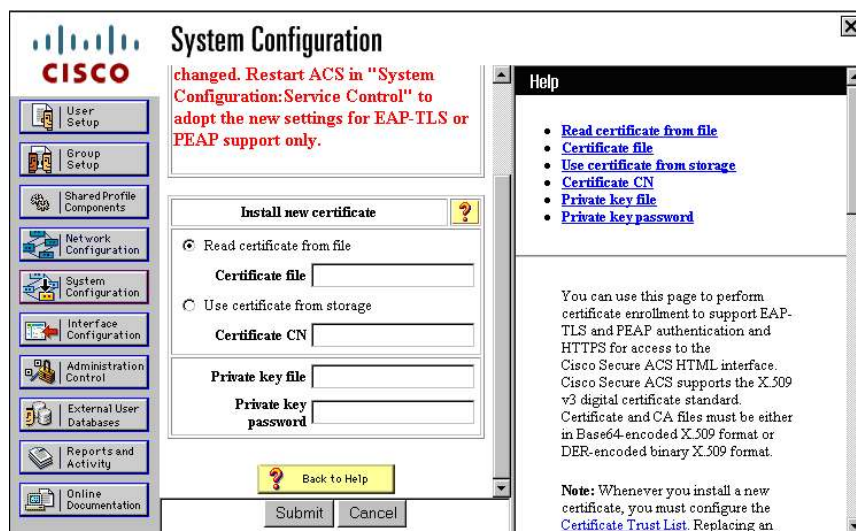
- To specify that Cisco Secure ACS reads the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- To specify that Cisco Secure ACS uses a particular existing certificate from local machine certificate storage, select the **Use certificate from storage option**, and then type the certificate CN (common name/subject name) in the Certificate CN box.

Step 5. If you generated the request using Cisco Secure ACS, in the **Private key file** box, type the full directory path and name of the file that contains the private key.

Step 6. In the **Private key password** box, type the private key password.

Step 7. Click **Submit**.

**Figure 33.** Cisco Secure ACS System Configuration: Installing New Certificate



### Generating a Self-Signed Certificate

Installing self-signed certificates is a way for administrators to meet this requirement managing the certificate without having to interact with a certification authority to obtain and install the certificate for the Cisco Secure ACS.

The self-signed certificate feature in Cisco Secure ACS allows the administrator to generate the self-signed digital certificate and use it for Protected Extensible Authentication Protocol (PEAP) authentication protocol or for HTTPS support in Web administration service.

To generate a self-signed certificate, follow these steps:

Step 1. In the navigation bar, click **System Configuration**.

Step 2. Click **ACS Certificate Setup**.

Step 3. Click **Generate Self-Signed Certificate**.

Cisco Secure ACS displays the Generate Self-Signed Certificate edit page.

Step 4. In the **Certificate subject** box, type the certificate subject in the form **cn=XXXX**. You can enter additional information here. For information, refer to the section [Self-Signed Certificate Configuration Options](#) in the **Cisco Secure ACS User Guide**.

Step 5. In the **Certificate file** box, type the full path and file name for the certificate file.

Step 6. In the **Private key file** box, type the full path and file name for the private key file.

Step 7. In the **Private key password** box, type the private key password.

Step 8. In the **Retype private key password** box, retype the private key password.

Step 9. In the **Key length** box, select the key length.

- Step 10. In the **Digest to sign with** box, select the hash digest to be used to encrypt the key.
- Step 11. To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.
- Step 12. Click **Submit**.

The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational, if you also selected the Install generated certificate option, only after you restart Cisco Secure ACS services. See Figure 34.

**Figure 34.** Generating a Self-Signed Certificate

The screenshot shows the Cisco System Configuration interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' and 'Edit'. Below this is a form titled 'Generate Self-Signed Certificate'. Inside the form is a sub-section 'Generate new self-signed certificate' with a help icon. The form contains the following fields and options:

- Certificate subject:** cn=emch-sp2-pc
- Certificate file:** c:\acs\_server\_cert.cer
- Private key file:** c:\acs\_server\_cert.pvk
- Private key password:** (empty text box)
- Retype private key password:** (empty text box)
- Key length:** 2048 bits (dropdown menu)
- Digest to sign with:** SHA1 (dropdown menu)
- Install generated certificate:**

Below the form is a yellow 'Back to Help' button with a question mark icon. At the bottom of the form are 'Submit' and 'Cancel' buttons.

For more information on Cisco Secure ACS authentication and certificates refer to the Cisco Secure ACS User Guide at

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/acs33/user/sau.htm#wp326973](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/user/sau.htm#wp326973).

## Appendix B: FAQ on Troubleshooting CiscoWorks LMS Integration with Cisco Secure ACS

**Q. Are there any backend script or command-line interface options to change the login module from ACS to CiscoWorks local?**

- A.** To revert the LMS server from ACS mode back to local user mode, shut down the CiscoWorks daemons and run the following script:

```
NMSROOT/bin/perl ResetLoginModule.pl (for Solaris)
```

```
NMSROOT\bin\perl ResetLoginModule.pl (for Windows)
```

Then restart the daemon.

**Q. Application registration failed with ACS appliance server. What could be wrong?**

- A.** Check the following to troubleshoot:

1. Check whether there is any protocol mismatch between LMS server and ACS server.
2. Check whether the given ACS admin username and ACS admin password is valid or not.
3. Check any IP based restriction is given in ACS server. You can get these under "Administration control -> Access Policy"
4. Check the port range given in ACS server. You can get these details from "Administration control -> Session policy". It will be better to have at least 5 to 10 ports.
5. Check whether the default ACS appliance administrator is used for LMS integration with ACS. We should not use the default ACS appliance administrator for integration purpose. Create another admin user and use the same for ACS integration.

**Q. Some of my devices disappeared from LMS device selector after integration with ACS. Why?**

- A.** First log in to ACS to verify that you are authorized to view and manage these devices. Then check the Not Configured in ACS list in Common Services. Before the LMS/ACS integration, the devices must be present in both LMS and ACS. If some devices are configured in LMS but not in ACS, they will appear in the Not Configured in ACS list and are not managed by LMS.

**Q. Any caveat about deleting devices after LMS integration with ACS?**

- A.** After LMS has been integrated with ACS, it's recommended to delete devices first from the Device Credentials Repository (DCR) on the LMS side, and then delete them from ACS. If you delete the devices first from ACS, these devices will show up in LMS as Not Configured in ACS. There is no direct way to delete these devices once they are on the Not Configured in ACS list. However, one workaround is:

Step 1. Create a dummy NDG group in ACS to include these devices.

Step 2. Delete the devices in DCR and then in ACS.

**Q. Question: Can I register applications individually from the CLI?**

- A.** You can reregister the CiscoWorks applications with Cisco Secure ACS from the AAA Mode Setup in CiscoWorks Common Services, which will cause the custom roles (if any) to be lost. But this mass application registration can be avoided by using the CLI script **AcsRegCli.pl**. CiscoWorks Common Services 3.0 provides a CLI script that can be used to register individual applications.

The location of the script is \$NMSROOT\bin\AcsRegCli.pl. Following are the optional parameters available when running the script from the CLI:

```
NMSROOT/bin/perl AcsRegCli.pl --register <App-name>
```

The following are the available application names:

- **cwhp**: Common Services
- **rme**: Resource Manager Essentials
- **CM**: Campus Manager
- **dfm**: Device Fault Manager
- **CiscoView**: CiscoView
- **ipm**: Internetwork Performance Monitor
- **hum**: Health and Utilization Monitor (HUM is a new add-on product introduced in LMS 3.0.)

**AcsRegCli.pl --register all**

This option is similar to application registration from the GUI, where all the installed applications are registered with the Cisco Secure ACS server.

**Q. I have configured my LMS server to integrate with Cisco Secure ACS for AAA. When I log in to in CiscoWorks ACS server, the authentication succeeds but all the buttons are disabled/grayed-out. How do I troubleshoot this issue?****A.**

Step 1. Check whether you have restarted the daemons using:

```
net stop crmdmgt, net start crmdmgt for Windows and
/etc/init.d/dmgt stop, /etc/init.d/dmgt start for Solaris
```

Step 2. If the preceding solution doesn't solve the problem, then check the Cisco Secure ACS user configuration to see whether a role has been assigned to the user.

**Q. I have provided the ACS credentials in my Cisco Secure AAA mode page and restarted the daemons. When I try to log in as a user in ACS, I get an authentication failed message. How do I troubleshoot this issue?****A.**

Step 1. Check whether the ACS server is up and running.

Step 2. Check the Failed Attempts log in the ACS server. If it says "Bad request from NAS", it means the Common Services server has not been added as an AAA client to ACS. Please refer to the section "Adding AAA Client to ACS Server" in this document.

Step 3. If the message is "Password mismatch", then check whether the ACS administrator password and shared secret key entered in the Common Services AAA mode page are correct.

**Q. I have integrated my CiscoWorks Common Services server with the Cisco Secure ACS server and have assigned appropriate roles to the user. But I am not able to see the devices added in DCR at all and the list is always empty. What do I need to do?**

**A.** To view the devices added to DCR, you need to add the devices as AAA clients to the ACS server.

**Q. When I perform an application registration, I am getting an error message “Application <App-name> registration: Failure on Primary ACS Server”. What could be the problem?**

**A.**

Step 1. Check whether the ACS server is up and running.

Step 2. Check whether the ACS admin Password specified in the Cisco Secure AAA mode page is correct.

Step 3. Check/uncheck the **Connect to ACS in HTTPS mode** checkbox in the Cisco Secure AAA mode page depending on the HTTP/HTTPS mode of ACS.

**Q. How do I unregister an application? I do not see any option available from the GUI.**

**A.** There is no way of unregistering an application from the front end, but registering/unregistering applications can be done from the back end using the script **ACSRegCli** located at `$NMSROOT\bin\`.

Following are the available command arguments and options:

- `NMSROOT/bin/perl ACSRegCli.pl -register All`
- `NMSROOT/bin/perl ACSRegCli.pl -unregister All`
- `NMSROOT/bin/perl ACSRegCli.pl -register <App-Name>`
- `NMSROOT/bin/perl ACSRegCli.pl -unregister <App-Name>`

**Q. How do I enable the CAM (Core Admin Module) debugging log?**

**A.** From the CLI, execute the following command:

```
$NMSRoot/MDC/bin/ccraccess - updateLog Core cam DEBUG.
```

The logs can be found at `$NMSRoot/MDC/log`.

**Q. I have installed several applications over CiscoWorks Common Services. I have configured the user in ACS, and I am seeing the respective role of the user is being applied in CiscoWorks Common services, but the buttons are grayed out for all the applications pages.**

**A.** Similar to assigning a role to a user for CiscoWorks Common Services, you must assign roles to all the other registered applications also.

**Q. Where do I specify the fallback user for ACS mode?**

**A.** The fallback option for the ACS mode can be given in the non-ACS TACACS+ mode setup page.

To add the fallback users in ACS, execute the following steps:

1. Select non-ACS mode.
2. Select **TACACS+** and click **Change**.
3. Specify the fallback users in the **Login fallback options** text field.
4. Click **OK**.

5. Select ACS mode.
6. Enter the required values.
7. Click **Apply**.

**Q. I have specified a user under the fallback option for ACS, but I am not seeing the fallback option from Cisco Secure ACS to CiscoWorks local working for the authorization request. What could be wrong?**

**A.** The fallback option in ACS is only for authentication where the requests are redirected to the Common Services server; there is no fallback option for the authorization requests.

**Q. What info is needed to send to the Cisco Technical Assistance Center (TAC) if there is any issue with ACS integration?**

**A.** Before contacting Cisco TAC, consider:

- If the ACS server is multi-homed, are all the IP addresses added to the ACS server?
- If the user is using a version prior to LMS 3.0, all the checks that are made as part of **ACSTestTool.pl** can be manually verified.
- Check the ACS configuration, such as the ports opened, IP filtering.
- Is there any firewall, proxy, Network Address Translation (NAT), or any other company security policy enforced between the ACS server and the CiscoWorks server?
- In the ACS and CiscoWorks environments, are there any antivirus or security agents installed?

The customer should also provide screenshots of the ACS Administration Control screen and Administration Control Access Policy screen. The customer should also provide the regdaemon.xml file at least (MDCSupport at best).

Based on this information, the TAC may then require that the customer enable CAM (Core Admin Module) debugging and/or get a sniffer trace.

### Appendix C: Export to ACS Server Using the CLI

You have the option to export the devices from the Device Credentials Repository (DCR) to the specified ACS server using the command-line interface in Secure Shell Protocol mode.

1. Enter `NMSROOT/bin/dcrcli -u username`.
2. Enter the password corresponding to the username.
3. Enter `expAcs hn=value un=value pwd=value prt=value proto=value seckey=value ndg=value fn=value`,  
where

**hn** is the ACS server name or IP address.

**un** is the ACS administrator username.

**pwd** is the ACS administrator password.

**prt** is the ACS administrative port number.

**proto** is the current ACS administrative access protocol. Supported values are http and https.

**seckey** is the ACS shared secret key.

**ndg** is the network device group in ACS.

**fn** is the file name.

If you do not specify the file name:

- In non-ACS mode, all the devices from DCR will be exported to the specified server.
- In ACS mode, only the devices that not configured in ACS will be exported from DCR to the specified server.

To export using Batch mode:

1. Go to `NMSROOT/bin`.
2. Enter `dcrcli -u Username cmd=expAcs hn=value un=value pwd=value prt=value proto=value seckey=value ndg=value fn=value`.

After the export operation is completed successfully, the CLI prompt displays the following summary:

- Number of devices exported to ACS
- Number of duplicate devices
- Number of error devices

You should log out from CiscoWorks and log in again. Only then do the changes come into effect.

**Note:** For a complete list of attributes and their description, use the `lsattr` command in `dcrcli`.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)