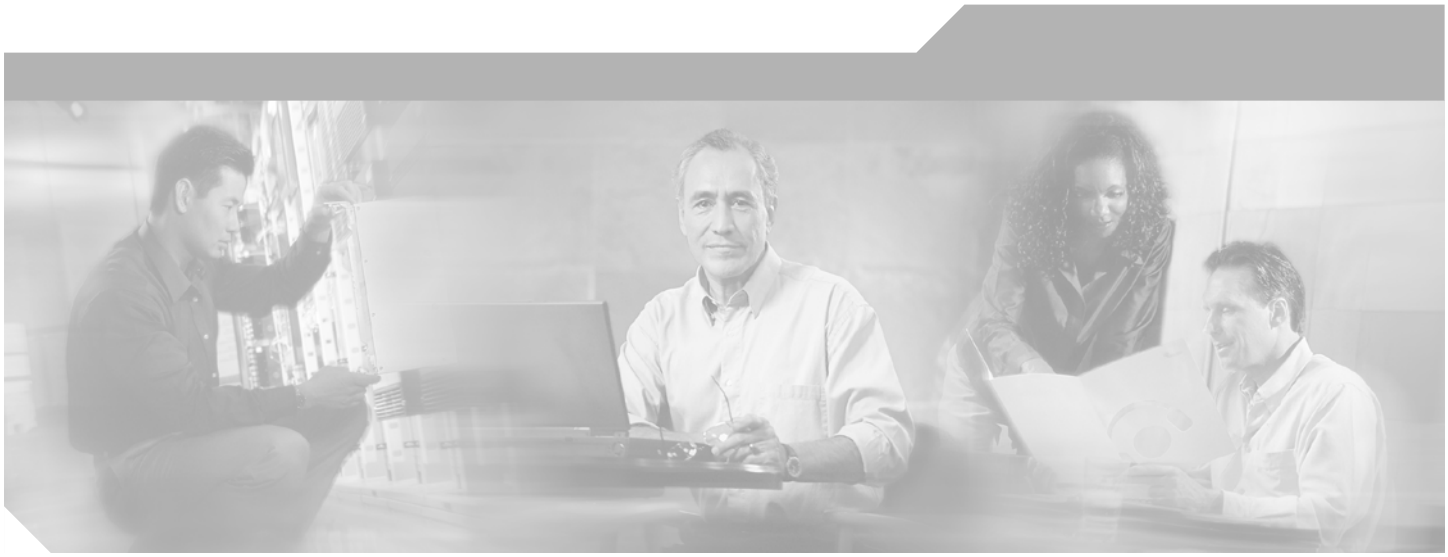


CiscoWorks Common Services 3.0 Whitepaper

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

CiscoWorks Common Services 3.0 Whitepaper

CONTENTS

CHAPTER 1

Using the CiscoWorks Home Page

Introduction

Common Services represents a common set of management services that are shared by Cisco Works applications. Cisco Works is a family of products based on Internet standards for managing networks and devices. All Cisco Works products use and depend on Common Services.

The latest version of Common Services is 3.0. This release of Common Services has been integrated with Cisco LAN Management Solution (LMS) 2.5 and scheduled to be integrated with VPN/Security Management Solution and Small Network Management Solution bundles of Network Management.

Common Services provides a set of new features required to drive the products towards a common look and feel. It also enables sharing of some critical information among the various products.

Common Services includes (but is not limited to) a home page, device credential repository, grouping services, single sign-on for a distributed set of Cisco works servers, and components to integrate with AAA services.

The objective of this document is to provide an overview of the following topics in Common Services 3.0.

- CiscoWorks Home Page

  CiscoWorks Home Page provides a launch point for CiscoWorks family of products and other resources. It is the web page displayed after logging into a CiscoWorks server.

- Device Credential Repository and Administration

  It is a repository to store device and their credentials and share the information across multiple applications in the same server or different Cisco Works servers.

- Single Sign On – Master/Slave model for authentication

  To login into multiple CiscoWorks servers with a single action and the entry of a single password. The user needs to login once in a CiscoWorks server group.

- Grouping Services – Group Devices based on criteria

  Group devices based on criteria. The criteria can be based on user defined fields created by the user for a device or based on variables provided by the Device and Credential Repository in Common Services.

- Integration with ACS

  ACS is a central server for authentication and authorization for a group of CiscoWorks servers. ACS can be used to manage user roles, create new user roles and to restrict device access in the CiscoWorks server for users.

Note Please note that the Local Security mode of CiscoWorks server can help in authenticating and authorizing the users in the absence of an ACS server in the network.

To get more information on other topics in Common Services such as licensing, backup and restore, Browser Security mode settings, authentication and authorization when CiscoWorks is in Local Security mode, etc., please refer to the *CiscoWorks Common Services User Guide* installed as part of your CiscoWorks server. For instructions on how to access the User Guide, see Appendix A, "Accessing the CiscoWorks User Guides."

CiscoWorks Home Page

The CiscoWorks Home Page provides a launching point for the CiscoWorks family of products and other resources. It is a launch point for applications in the same or remote server, other third party products, and home-grown tools residing on the same or a different server.

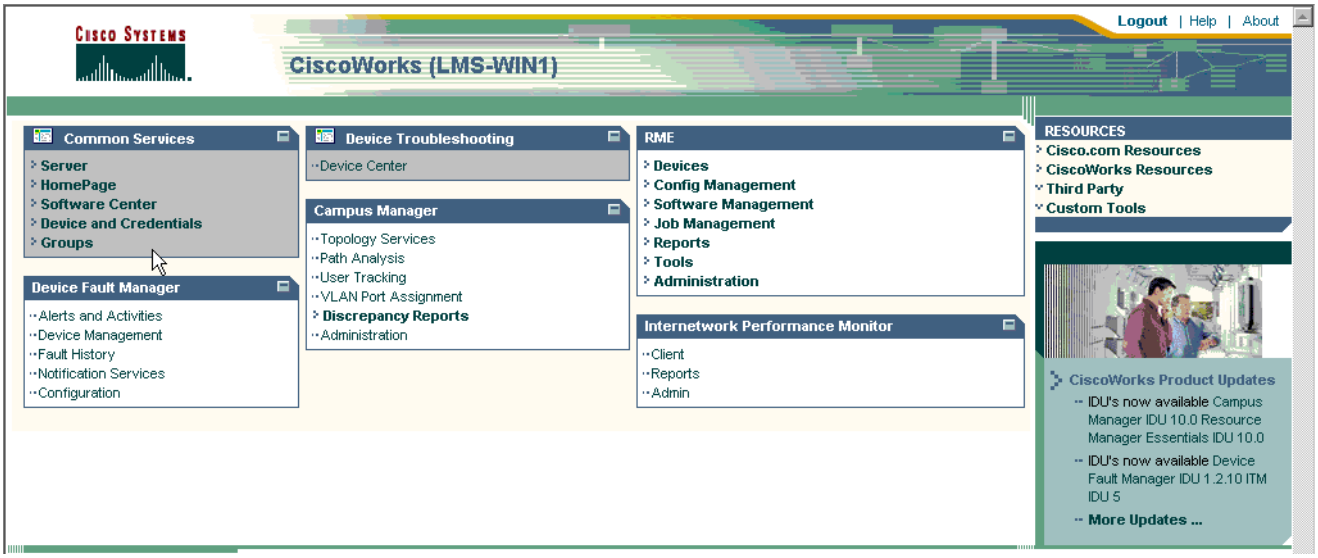
To invoke the CiscoWorks Home Page, enter the following URL:

http://server-name:portnumber

In both Windows and Solaris the port numbers are **1741** for normal access; the secure port number is **443**.

The CiscoWorks Home Page appears as shown in Figure 1-1.

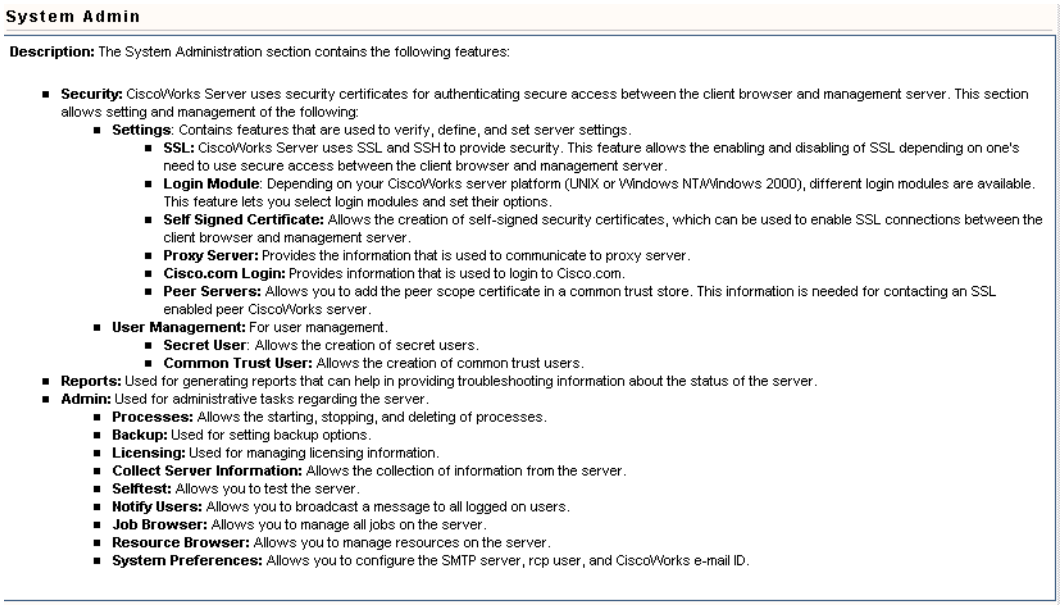
Figure 1-1 CiscoWorks Home Page



When you log in to the CiscoWorks Home Page using a valid username (created either in local user setup mode or in ACS), a home page with many panels is displayed.

By navigating through the Common Services panel, you can launch Server Configuration, Homepage Configuration, Device and Credentials Repository, Grouping Services, and Device Center. Figure 1-2 shows the screen that is displayed when you select **Server** from the Common Services panel.

Figure 1-2 System Administration Page



How Can You Use the CiscoWorks Home Page?

You can use the CiscoWorks Home Page to:

- Import application links from other CiscoWorks servers. The imported application link will provide a single home page from which all applications in all CiscoWorks servers can be launched.
- Set up links to other third party software used along with CiscoWorks servers (for example, HP OpenView, Tivoli, etc.).

Customizing the CiscoWorks Home Page

To customize the CiscoWorks Home Page:

1. From the Common Services panel, choose **Home Page**.
2. Click on either the **Application Registration** or the **Links Registration** link.

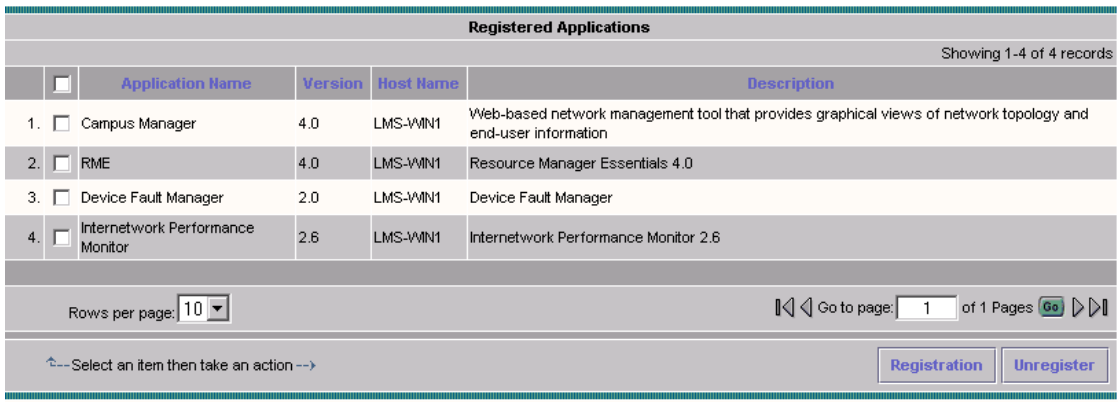
To Register an Application Installed on Another Server

A CiscoWorks application can be registered with or without using a predefined templates.

Step 1 To register an application, navigate to the **Application Registration** link.

The Applications Registration Status dialog box appears (see Figure 1-3).

Figure 1-3 System Administration Page



You can register a CiscoWorks application from another CiscoWorks server without using predefined templates.

Step 2 To register all or a select set of applications running in another CiscoWorks server, click **Registration**.

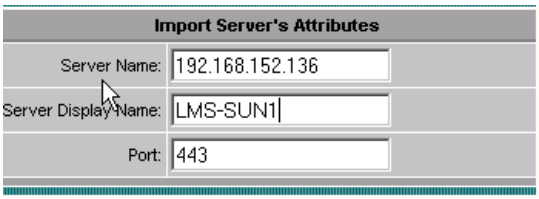
The Registration Locations dialog appears (see Figure 1-4).

Figure 1-4 Importing From Other Servers

Step 3 Select the **Import from Other Servers** option, then click **Next**.

The Import Server's Attributes dialog is displayed (see Figure 1-5).

Figure 1-5 Importing the Server's Attributes



Step 4 Specify the server's attributes:

a. Enter the server name or the server's IP address.

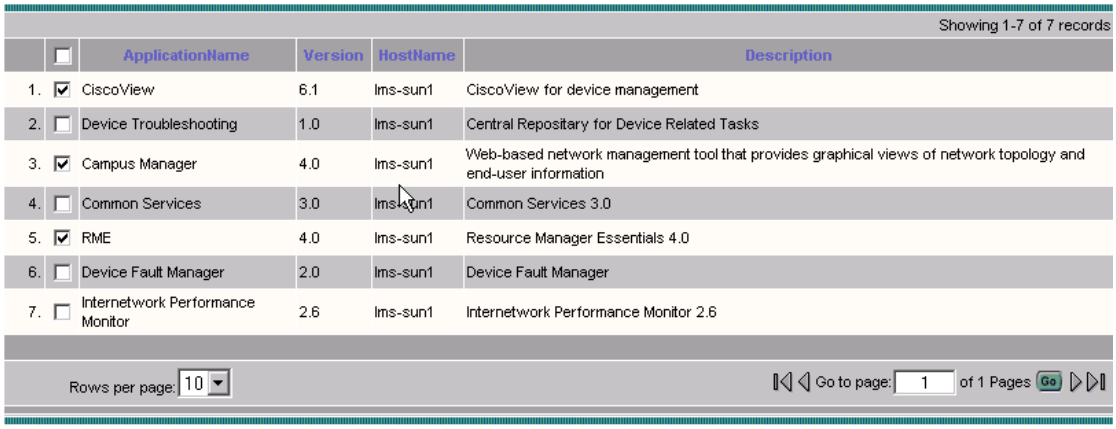
b. Enter the server's display name to be seen on the CiscoWorks Home Page.

c. Specify the server's port number, then click **Next**.

Tip Before proceeding to the next step, 1) you must import the certificates of the other servers into this CiscoWorks server, and 2) the System Identity User must be the same on both the servers.

The list of applications that are available for import appears (see Figure 1-6).

Figure 1-6 Applications Available for Import

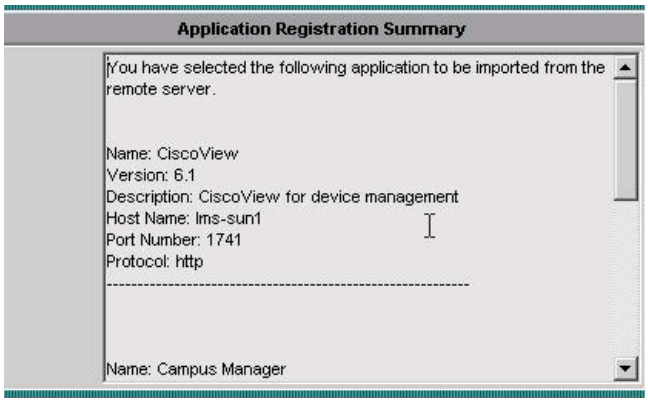


All the applications in the other CiscoWorks serves are available for import.

Step 5 Select a list of applications that you would like to launch from the CiscoWorks Home Page of this CiscoWorks server, then click **Next**.

The Application Import Registration Summary page is displayed (see Figure 1-7).

Figure 1-7 Application Import Registration Summary



The Application Import Registration Summary page lists all the applications that are selected for import into CiscoWorks Home Page.

Step 6 Click **Finish**.

The applications that are available from the other CiscoWorks server (lms-sun1) appear on the CiscoWorks Home Page (listed in the left column) as shown in Figure 1-8.

Figure 1-8 Applications Available on the lms-sun1 Server

To Register an Application Using a Predefined Template

Step 1 To register an application using a predefined template, click **Registration**.

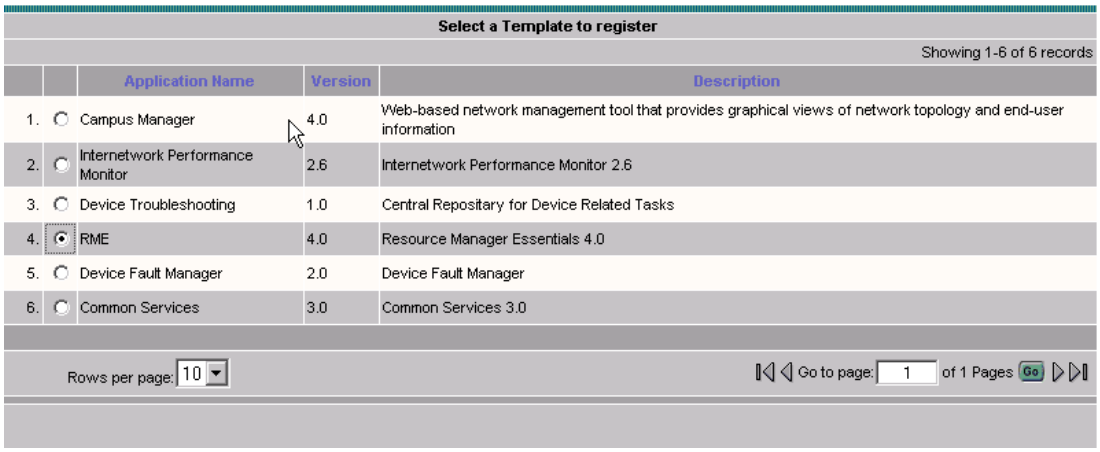
The Registration Location dialog is displayed (Figure 1-9).

Figure 1-9 Registering Applications From Templates

Step 2 Choose the **Register From Templates** option, then click **Next**

The dialog box shown in Figure 1-10 is displayed.

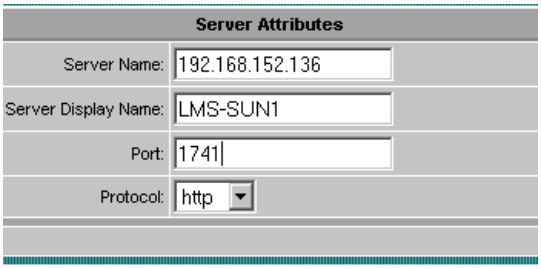
Figure 1-10 Selecting Predefined Applications to Import From Another Server



Step 3 Choose from the list of predefined applications that you want to import from another server, then click **Next**.

The Server Attributes dialog box appears (see Figure 1-11).

Figure 1-11 Specifying Server Attributes



Step 4 Specify the server's attributes:

a. Enter the name of the server or its IP address.

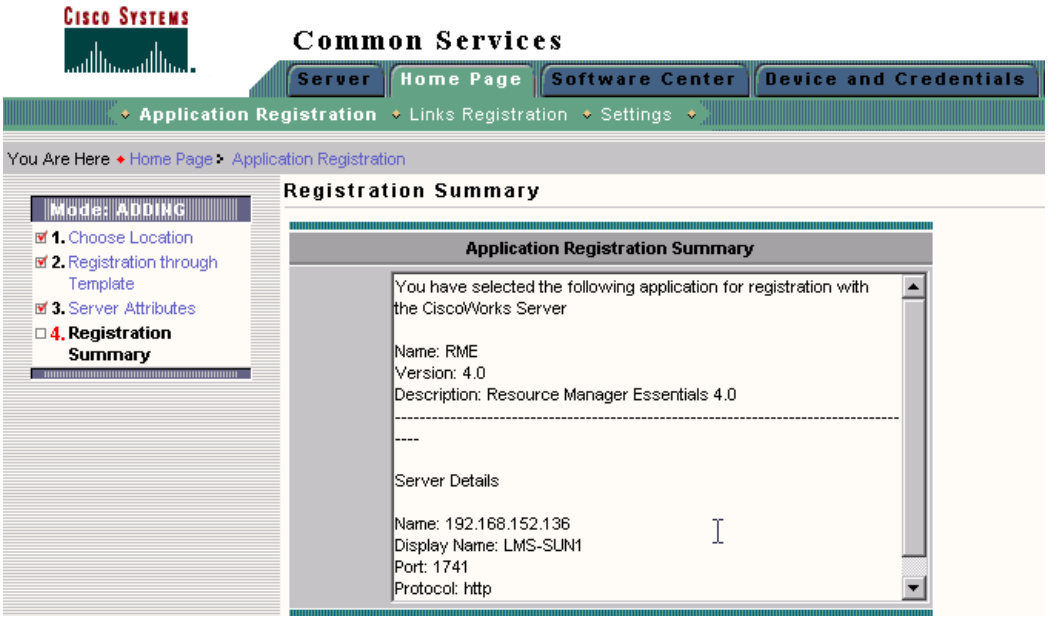
b. Enter the server's display name to be shown on the CiscoWorks Home Page.

c. Specify the port number that will launch the application.

d. Choose the protocol as **HTTP** or **HTTPS**, then click **Next**.

The Application Registration Summary is displayed (see Figure 1-12).

Figure 1-12 Application Registration Summary



Step 5 After checking the details of the application that is to be imported, click **Finish**.

The CiscoWorks Home Page is updated with a panel that shows the RME server links from the remote server.

Registering Bookmarks in the CiscoWorks Home Page

You can register additional links to Custom tools and home grown tools with CiscoWorks Home Page. These new links appear in the Custom Links panel in the right corner of CiscoWorks Home Page.

To register a new link, from the Common Services menu, choose **Home Page > Link Registration**.

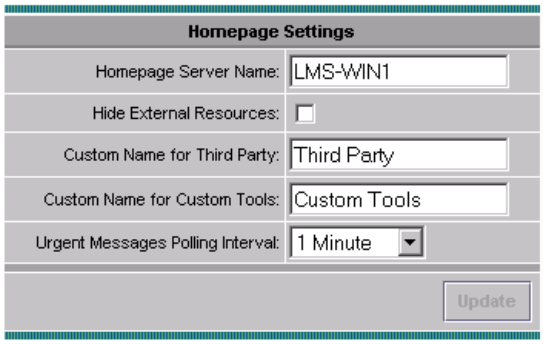
Configuring the CiscoWorks Home Page

To configure the CiscoWorks Home Page, follow these steps:

Step 1 From the Common Services menu, choose **Home Page**.

The Homepage Settings dialog box appears (see Figure 1-13).

Figure 1-13 Homepage Settings



Step 2 Specify the homepage settings:

a. **Homepage Server Name**: This is the name for the Cisco Works server. This name will appear when you log in to the Cisco Works server.

Note If you chooses the option, the server display name can be used as the top-level group name for groups appearing in the object selector. A Daemon Manager restart is required if the display name is to appear as part of the top-level group name.

Tip The display name specified for the CiscoWorks Home Page should be unique across any group of CiscoWorks servers that have a DCR Master and DCR Slaves.

b. **Hide External Resources**: If you enable this checkbox, you will hide the Resources and CiscoWorks Product Updates panel in the CiscoWorks Home Page.

c. **Custom Name for Third Party**: Display name for the list of third-party tools.

d. **Custom Name for Custom Tools**: Display name for the custom tools.

e. **Urgent Message Polling Interval**: Select the appropriate interval from the drop-down list to specify the period of time after which the CiscoWorks server will check for important messages that need to be shown to the users of this server. The list of important messages includes alerts to users on disk usage thresholds being reached.

Step 3 When finished, click **Update**.

CHAPTER 2

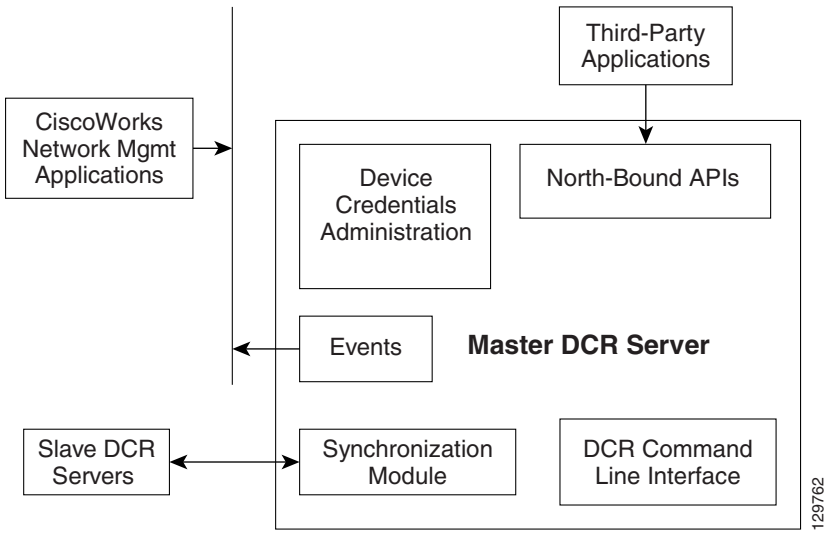
Device and Credentials Repository Administration

Introduction

The Device and Credentials Repository (DCR) is a common repository of devices, their attributes, and their credentials required to manage devices in a management domain. The Device and Credentials Repository lets you share device information among various network management applications. The Device and Credentials Administration (DCA) provides an interface to administer the Device and Credentials Repository.

Individual applications (Campus Manager, Resource Manager Essentials, Internetwork Performance Monitor, and Device Fault Manager) interact with this repository to get the device list, device attributes, and device credentials. Applications can read or retrieve the information, as well as update the information in DCR so that it can be shared with other applications.

Figure 2-1 DCR Overview



The Device and Credentials Repository:

- Permits dynamic creation of attribute types, default grouping, and filtering within the Device and Credentials Repository.

  An attribute of a device can be any user-defined name, such as “Device Location,” etc. You can then provide a value for this attribute for devices D1, D2, and D3, such as “Chicago Office.” You can then use this attribute value to group devices based on a criteria such as “Create a group of devices whose attribute ‘Device Location’ has the value ‘Chicago Office.’”
- Supports proxy device attributes, unreachable devices, and device preprovisioning.
- Allows you to populate the Device and Credentials Repository by importing from many sources, and to export device data for use with third-party products like HP OpenView and NetView.
- Uses a unique Internal Device Identifier to access device details, and detects duplicate devices based on specific attributes.
- Encrypts credential data stored in the Repository. Access to device data is permitted only by secured channel and client authentication.
- Supports IPv6 and SNMP v3.

What Types of Devices and Information are Stored?

Device Types

Information on three different types of devices is stored in the Device and Credentials Repository.

- *Cluster managed devices* that form a cluster are stored in a special format. DCR provides means to store the association between the cluster members and the cluster.

  For cluster managed member devices, the member number, display name and cluster name are mandatory.
- *Auto Update Server (AUS) managed devices*. The Auto Update server (AUS) supports a pull model of configuration that can be used for the initial configuration, configuration updates, operating system updates and periodic configuration verification. The Device and Credentials Repository provides the means to store the association between AUS and AUS-managed devices.

  For AUS managed devices, the Display Name and AUS Device ID (device_identity) are mandatory.
- *Standard devices*. All other devices that are not cluster managed devices or AUS managed devices are referred to as “standard devices” and are also stored in the Device and Credentials Repository.

In addition to storing credential information, DCR stores device-identity attributes and user-defined attributes for all the device types mentioned above.

- *Device identity attributes* are considered to be unique to each device and are used to identify a device; for example, a device’s device name and host name.
- *User-defined attributes* can be any notable information that you want to store about a device.

Device-Identity Attributes

The following device-identity attributes are stored in the Device and Credentials Repository.

Table 2-1 Device-Identity Attributes Stored in the DCR

Attribute	Description
Host Name	Device host name
Domain Name	Domain name of the device
Management IP Address	IP address used to access the device. Both IPv4 and IPv6 address types are supported.
Device Identity	Identifies preprovisioning devices. The value would be application specific.
Display Name	The device name, as you want it to be represented in reports or graphical displays. This name can be derived from the host name, management IP address, or device identity. This is a mandatory attribute.
sysObjectID	sysObjectID value. It may be UNKNOWN in the case the facility that is populating the repository does not know the value.
MDF-Type	Normative name for the device type as described in Cisco's Meta Data Framework (MDF) database. Each device type has a unique normative name defined in MDF.
DCA Device ID	Device and Credentials Administration Device ID. This is an internally-generated unique sequential number that identifies the device record in the DCR database. The DCR clients should remember the value to access device details from the repository.

User-Defined Attribute

The following user-defined attribute is stored in the Device and Credentials Repository.

Table 2-2 User-Defined Attribute Stored in the DCR

Attribute	Description
User Defined Fields	DCR supports 10 user-defined fields. These fields are used to store additional user-defined data for a device. DCA initially provides four user-defined fields. You can add up to 10 user-defined fields as needed.

Device Credentials Information

Device credentials are values that are used by applications to access and operate on devices. It is typically an SNMP community string or a user ID and password pair. A device credential is used to access a managed device such as a switch or router.

The following device credential information is stored in the Device and Credentials Repository:

Table 2-3 Device Credential Information Stored in the DCR

Credential	Description
Standard Credentials	
primary_username	The primary user name used to access the device.
primary_password	The password for the primary_username.
primary_enable_password	The device's primary enable password or enable secret password.
snmp_v2_ro_comm_string	The device's SNMP v2 read-only community string.
snmp_v2_rw_comm_string	The device's SNMP v2 read/write community string.
snmp_v3_user_id	The device's SNMP v3 user ID.
snmp_v3_password	The device's SNMP v3 password.
snmp_v3_engine_ID	The device's SNMP v3 engine ID.
snmp_v3_auth_algorithm	The SNMP v3 authorization algorithm used on the device (e.g., MD5 or SHA-1).
http_username	The device's HTTP-interface user ID.
http_password	The device's HTTP-interface password.
Additional Credentials for Cluster-Managed Devices	
dsbu_member_number	The number of the cluster managed member. This number represents the order in which the device was added to the cluster.
parent_dsbu_id	The DCR device ID of the parent cluster device.
Auto-Update Server-Specific Credentials	
aus_url	The URL for the AUS device.
aus_port	The port number of the AUS service running on the AUS device.
aus_username	The user login providing access to the AUS device.
aus_password	The password for the corresponding aus_username.
Auto-Update Server Managed Device-Specific Credentials	
aus_username	The user login providing access to the AUS-managed device.
aus_password	The password for the corresponding aus_username**.**
parent_aus_id	The DCR device ID of the managing AUS device.

Management Domain

A management domain is a group of network management products that effectively share the device list and device credentials through one single instance of a DCR Master server.

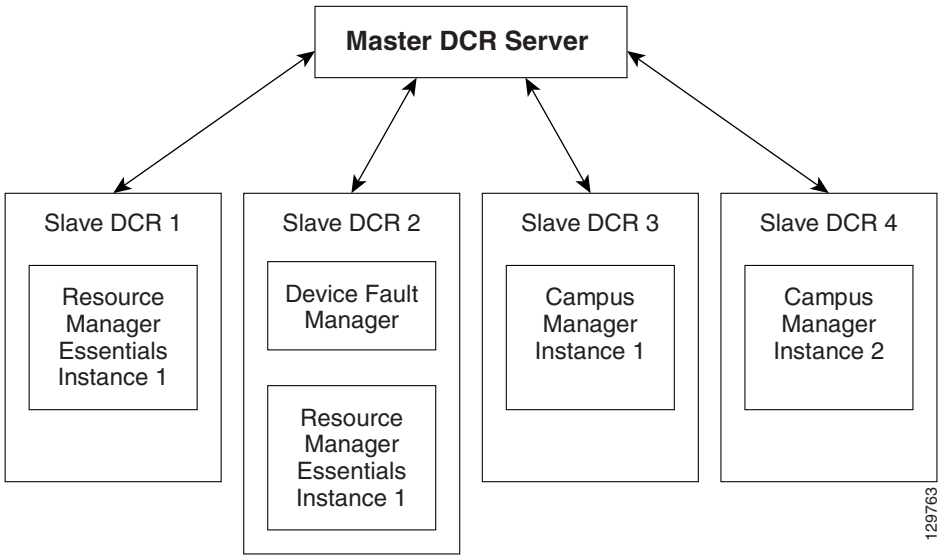
Why is a management domain necessary? CiscoWorks applications are bundled into the LAN Management Solution (LMS), Routed WAN Management Solution (RWAN) and VPN/Security Management Solution (VMS) bundles. Each CiscoWorks application that is part of a bundle cannot scale more than a predetermined set of devices.

For example, the optimal recommended list of devices that a single instance of Resource Manager Essentials and Campus Manager can manage is 5,000 devices per application instance. For Device Fault Manager, the optimal number is 1,500 devices per device in an LMS installation (based on performance numbers on a standard configuration machine).

Thus, if a customer wants to maintain and manage about 50,000 devices in a network, several LMS bundles need to be installed. These machines should share a common set of device list and credentials information that is managed centrally.

DCR provides modes by which a central DCR server maintains a device list; other slave DCR servers share the device identity and user-defined attributes, along with credentials information (see Figure 2-2).

Figure 2-2 Management Domain Overview



DCR Modes

The DCR server will run in either *Master mode*, *Slave mode*, or *Standalone mode*. Mode changes can be done via the user interface or the DCR command-line interface.

Master DCR Server

The salient features of the Master DCR server are as follows:

- It is the master repository of device list and credential data.

- There is only one master repository per management domain and it always contains up-to-date device list and credential data.
- Though the DCR server starts as a Standalone server, it can be configured (through the user interface) to run in Master mode.
- Any change to the repository data will first occur in the DCR Master server.
- It provides the GUI used to administer the data in the repository.

Slave DCR Server

The salient features of the Slave DCR server are as follows:

- The Slave DCR server is an exact replica of the Master DCR server data.
- Though the DCR server starts in Standalone mode, it can be configured (through the user interface) to run in Slave mode. Specifying the Master DCR server is also part of the configuration process.
- There can be more than one Slave DCR server in a management domain.
- When repository data is updated (using northbound APIs), the Slave DCR server first updates the Master DCR server and then updates its own repository data.
- The Slave DCR server has a mechanism to keep synchronized with the Master DCR server.

Standalone DCR Server

The salient features of Standalone DCR server are as follows:

- The standalone DCR server is an independent repository of device list and credential data.
- It neither participates in management domain nor does it communicate with the Master DCR server. It does not have any Slave DCR servers registered with it.
- It does contain up-to-date device list and credential data. The repository data is not shared in the management domain.
- By default, the DCR server starts in Standalone mode.

Changing DCR Mode

To change DCR mode settings:

Step 1 In the CiscoWorks Homepage, choose **Common Services > Device and Credentials > Admin**.

The Admin page appears with the current DCA settings.

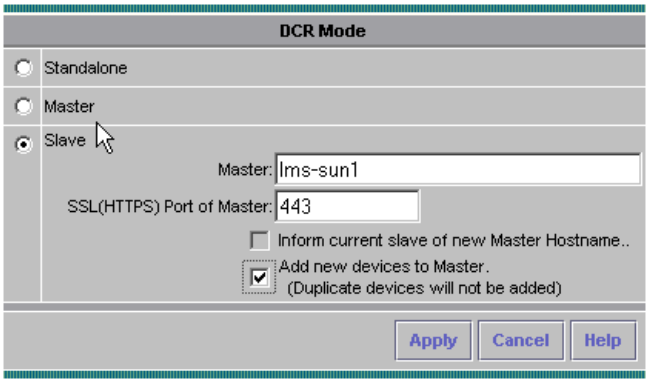
Step 2 Click the **Mode Settings** link.

The Mode Settings window appears.

Step 3 To change the current mode, click **Change Mode**.

The DCR Mode dialog box appears (see Figure 2-3). You can select the required mode from this dialog box.

Figure 2-3 Selecting the Required DCR Mode



Change to Standalone Mode

The default DCR mode is *Standalone*. To set the DCR mode to *Standalone*:

1. Select the **Standalone** radio button.
2. Click **Apply**.

Change to Master Mode

To set the DCR mode to *Master*:

1. Select the **Master** radio button.
2. Click **Apply**.

Change to Slave Mode

Before you change the mode to *Slave*, ensure that Master-Slave configuration prerequisites are in place.

To change the DCR mode to *Slave*, follow these steps:

Step 1 Select the **Slave** radio button.

Step 2 Enter the hostname of the Master in the *Master* field.

Note This hostname should exactly match the *Hostname* field in the Master server's Self Signed Certificate.

Step 3 Specify the SSL port of the master. The default is **443**.

- If the mode is changed from Master to Slave, select the **Inform Current slave(s) of New Master Hostname** check box.

  If you select this check box, all the slaves of the Master (whose mode you currently changed to Slave) will be informed of the new master hostname. That is, they will become the slaves of the new Master.

- If the **Add New Devices to Master** check box is selected, the devices in the Slave server will be added to the new Master. However, any duplicates will be discarded.

Step 4 Click **Apply**.

Set Up the DCR Master and Slave Configuration

Every CiscoWorks server has a default certificate created during the installation process. There is no need to create a separate certificate during the setup of the DCR Master and Slaves.

Master-Slave Configuration Prerequisites

Before you set up the Master and Slave, you must complete certain tasks to ensure that secure communication takes place between the Master and Slave.

Step 1 In the Master server, add a Peer server user and password.

Step 2 In the Slave server, add a System Identity user and password. This should be same as the Peer server user set up in the master.

Step 3 Copy the Self-Signed Certificate of the Slave to the Master.

Step 4 Copy the Self-Signed Certificate of the Master server to the Slave server.

Step 5 Configure the Slave server as a slave and the Master server as a master.

Set Up the DCR Master and Slave Servers

To set up DCR Master and Slave servers, follow these steps:

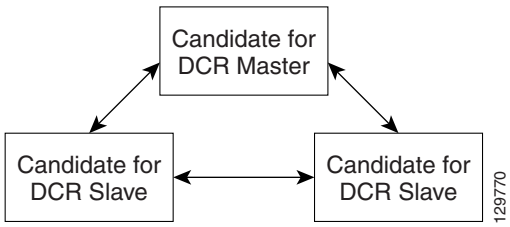
Step 1 Set up the same System Identity user and password in all the servers.

Step 2 Set up the System Identity Credentials by navigating from the Common Services Panel > **Server** > **Security** > **Multi-Server Trust Management** > **System Identity Setup**.

The next task is to exchange the peer certificates between all the servers.

For example, if you need to set up one DCR master and two DCR slaves, then exchange the peer certificate of the master with the two slaves and also exchange the peer certificates between the slaves, as shown in Figure 2-4.

Figure 2-4 Exchanging Peer Certificates



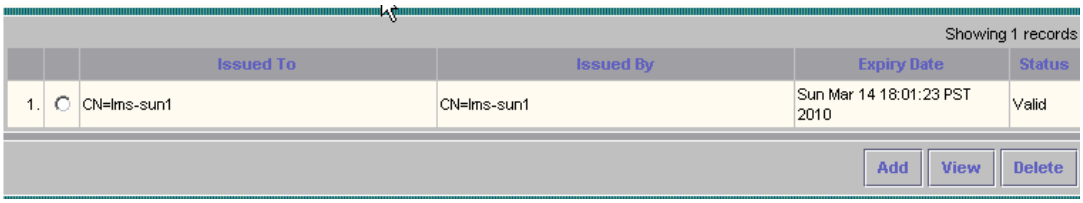
Step 3 To exchange peer certificates, from the Common Services panel, choose **Server > Security > Multi-Server Trust Management > Peer Server Certificate Setup**.

Step 4 Click **Add**.

Step 5 Enter the peer server name, then click **OK**.

The certificate will be imported as shown Figure 2-5.

Figure 2-5 Peer Certificate Imported



Step 6 Finally, place the DCR in a server in master mode and the rest of the servers in slave mode by navigating from the Common Services Panel and choose **Device and Credentials > Admin > Mode Settings** (for details on this procedure, see the "DCR Modes" section on page 2-5).

Note To point to the Master, create the DCR master before creating the DCR slaves.

If the Peer Certificate Import Fails

Due to differences in the date and time setup on different CiscoWorks servers, the peer certificate import process may fail. If this occurs, the following steps are recommended.

Step 1 Regenerate the certificate on the machine from which the import failed.

Step 2 Synchronize the time on the remote machine with the time on the local machine (that is, the time on the remote machine should match the time on the local machine).

Step 3 Restart the Daemon Manager on the machine from which the import failed.

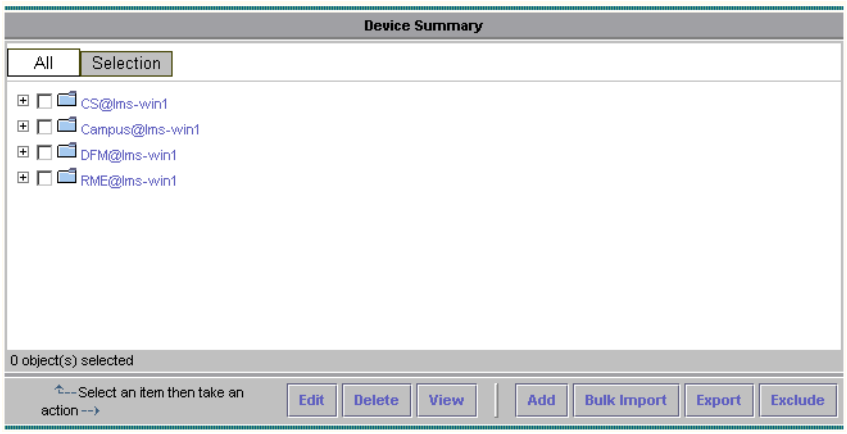
Step 4 Try to import the certificate from that machine again.

Device and Credentials Administration

Device and Credentials Administration (DCA) is the user interface for Device and Credential Repository.

You can access the DCA by navigating from the Common Services panel > **Device and Credentials** > **Device Management** (see Figure 2-6).

Figure 2-6 Device and Credentials Administration Device Summary



The following sections describe some of the major DCR functionality you can access using the DCA.

Add Device Types to the Device and Credentials Administration

This section describes how to add the following device types to the Device and Credentials Administration (DCA):

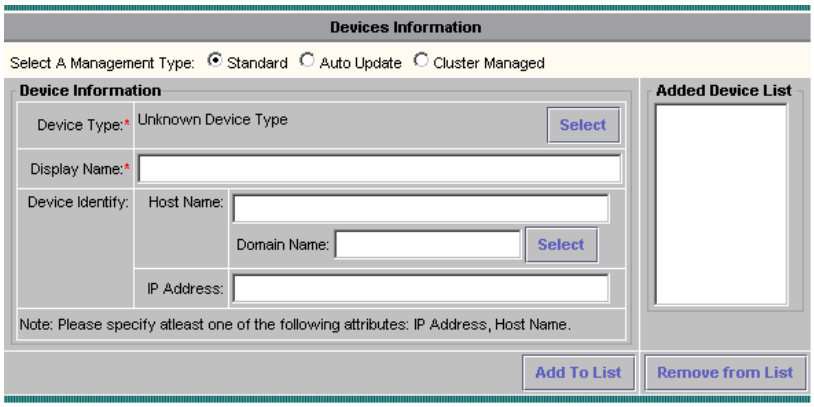
- Standard device
- Auto Update server
- Cluster-managed device

Add a Standard Device to the DCA

Step 1 To add a standard device to the DCA, click **Add**.

The Devices Information dialog appears (see Figure 2-7)

Figure 2-7 Add a Standard Device

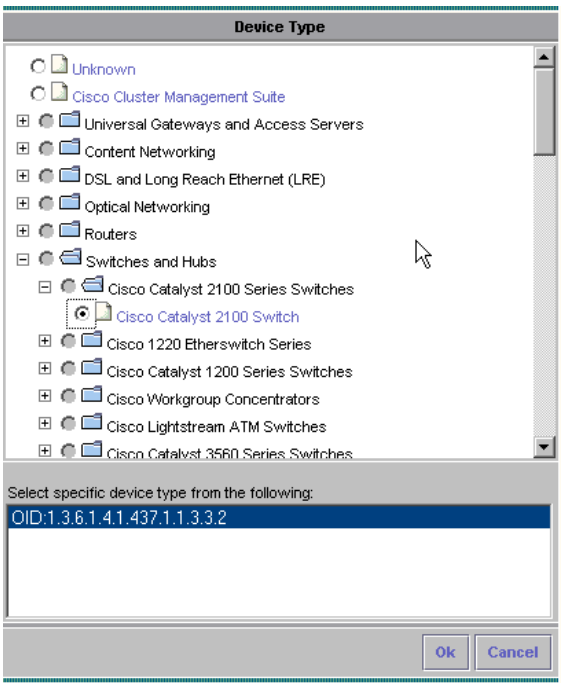


By default, **Standard** is already selected for the management type.

Step 2 From the *Device Type* field, click **Select**.

The Device Type window is displayed (see Figure 2-8).

Figure 2-8 Selecting a Standard Device Type



Step 3 Select the appropriate device type (for example, **Switches and Hubs**).

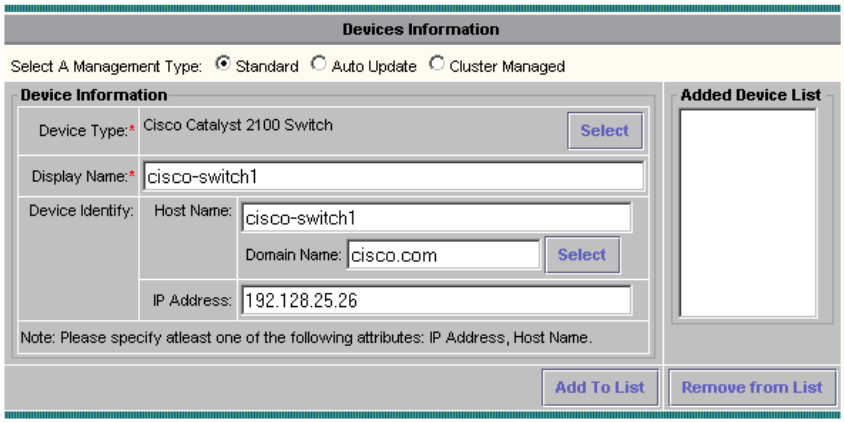
The Device Type selected expands to display the available devices of that type.

Step 4 Select the specific device of interest.

Tip To add a cluster manager device, select **Cisco Cluster Management Suite**.

The Devices Information dialog is displayed with the appropriate fields for that device, as shown in Figure 2-9.

Figure 2-9 Specifying Information for a Cisco Switch



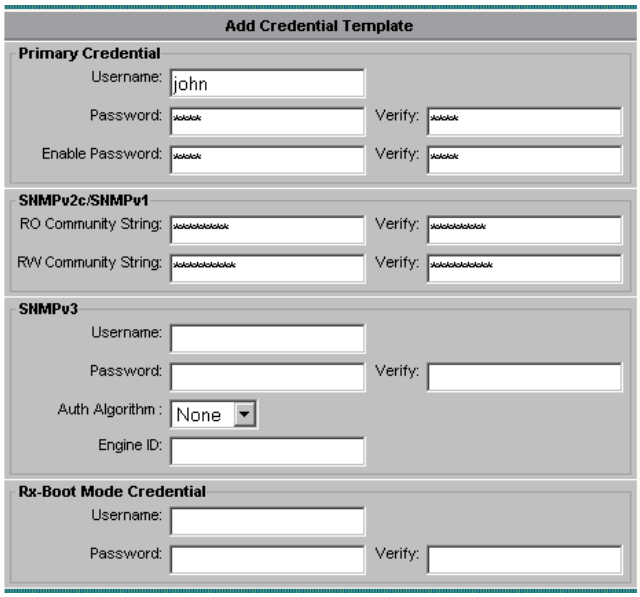
Step 5 Enter the device-specific information for the selected device.

Step 6 Click **Add to List**.

The device is added to the Added Device List in the window. To remove the device from the Device List, select the device and click **Remove from List**.

Step 7 Click **Next**. The Add Credential Template dialog appears (see Figure 2-10).

Figure 2-10 Entering the Device's Credential Information



DCA provides the option to define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

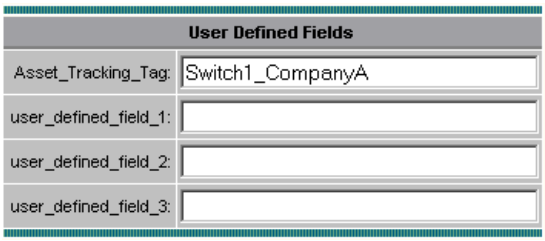
You can change the attribute fields that appear here at **Device and Credentials > Admin > User Defined Fields** (see "Add, Rename, or Delete User-Defined Fields to DCR" section on page 2-16).

Step 8 Enter the following credentials in the Add Credential Template, then click **Next**.

- *Primary Credentials*: Username, Password, and Enable Password
- *SNMP v2C Credentials*: Read-Only Community String, and Read-Write Community String
- *SNMPv3 Credentials*: Username, Password, authentication Algorithm, and Engine ID
- *Rx Boot Mode Credentials*: Username and Password

The Standard UDF dialog box appears (see Figure 2-11).

Figure 2-11 Specifying the User-Defined Fields



Step 9 Enter any value for user-defined fields 0 to 3 or any other user-defined fields that you may have created.

These field values are applied to all devices added in this procedure. In the example shown here, the device has value **Switch1_CompanyA** set for User Defined Field *Asset_Tracking_Tag*.

When finished defining the user-defined fields, click **Finish**.

Add a Cluster Managed Device and Associate with the Cluster Manager

Each cluster member has its own host name, sysObjectID, and MDF type, and uses the same Telnet credentials as the Cluster.

Note The Cluster must be added before a cluster-managed device. For example, if a device X belongs to cluster Y, first add the Cluster Y, and then add the Cluster Managed device X.

Step 1 In order to add a cluster managed device, first add a Cluster Manager.

a. Add a cluster manager as you would add a normal device as described in the "Add a Standard Device to the DCA" section on page 2-11.

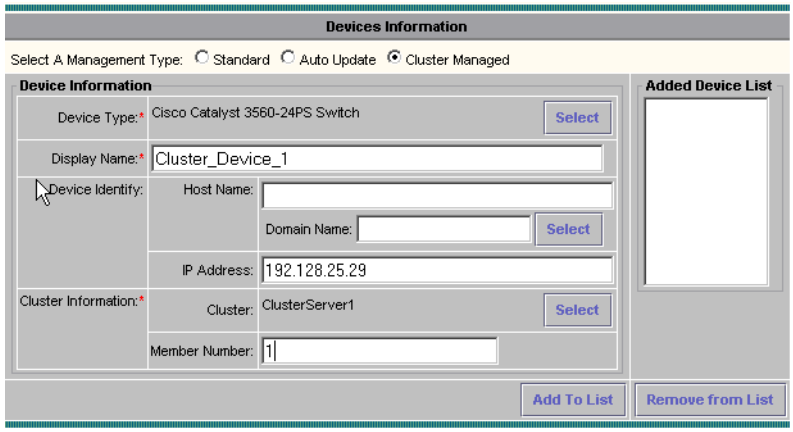
b. When the Device Type window appears, choose **Cisco Cluster Management Suite**.

The Cluster Manager is part of the Cisco Cluster Manager Suite. The Cluster Manager displays the front panel and LEDs of all cluster switches. Within Cluster Manager, you can point-and-click to configure ports and switches. You can select several ports from the same cluster and configure them all to run with the same settings. All of the device-management features are available through the Cluster Manager menu bar.

Step 2 To add a cluster managed device and associate it to the Cluster Manager, select the **Cluster Managed** management type.

The Devices Information dialog displays the following cluster-specific fields (see Figure 2-12):

Figure 2-12 Cluster Managed Device Information



Step 3 Enter the information related to this cluster device:

a. **Device Type**: Click **Select** and specify the device type.

b. **Display Name**: Enter the device's name as you wish it to be displayed.

c. **Device Identity**: Specify the device's host name, domain name, and IP address.

d. **Cluster**: Click **Select** and specify the appropriate cluster name.

e. **Member Number**: Specify the member number of this device.

The *Member Number* field is mandatory. The Member Number is the number of the Cluster member. This number represents the order in which the device is added into the cluster.

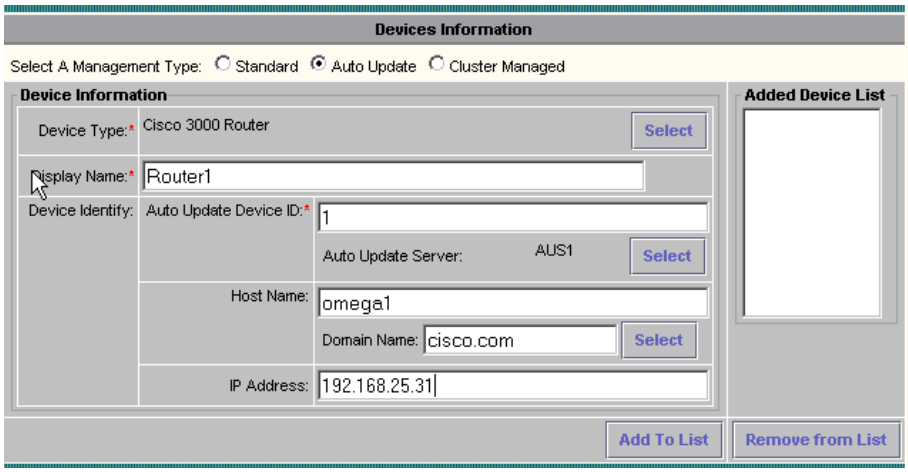
Step 4 When finished, click **Next**.

Add an Auto Update Sever Managed Device to DCA

Step 1 To add an Auto Update Server managed device and associate it with the AUS, select the **Auto Update** management type from the dialog shown in Figure 2-7.

The Device Information dialog displays the following AUS-specific fields (see Figure 2-13):

Figure 2-13 Auto Update Server Device Information



Step 2 Enter the information related to the Auto Update device:

a. **Device Type**: Click **Select** and specify the device type.

b. **Display Name**: Enter the device's name as you wish it to be displayed.

c. **Device Identity**:

- Auto Update Device ID
- Auto Update Server: Click **Select** and specify the Auto Update Server name.
- Host name
- Domain name: Click **Select** and specify the server's domain name.
- IP address

Step 3 When finished, click **Next**.

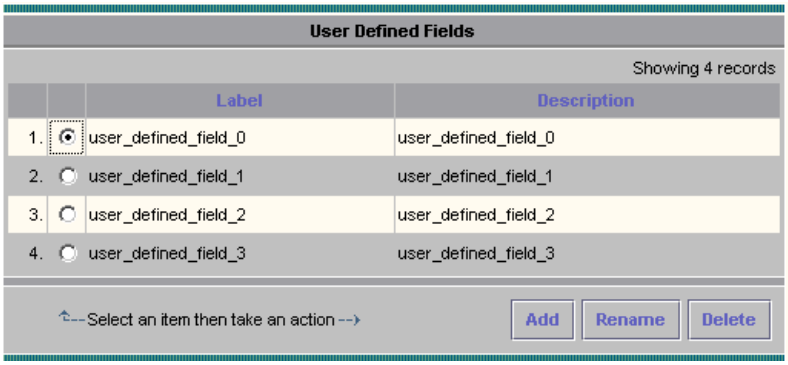
Add, Rename, or Delete User-Defined Fields to DCR

You can use user-defined fields to associate name value pairs with the devices maintained in DCR. These name value pairs can be then used to group devices based on criteria defined by the user.

To customize User Defined Fields, follow these steps:

Step 1 From the Common Services Panel, choose **Device and Credentials** > **Admin** > **User Defined Fields**.

Figure 2-14 Customizing User-Defined Fields



Step 2 Select the field you want to modify from the list of user-defined fields.

Step 3 To rename the selected user-defined field, click **Rename**.

For example, you could rename *user_defined_field_0* to *Asset_Tracking_Tag*. This field will then have a value for every device. Device 1 will have a value for the user-defined field *Asset_Tracking_Tag* as *Switch1_Lab1*, and so on.

Step 4 To add a user-defined field, click **Add**.

Step 5 To delete a user-defined field, select the field from the list, then click **Delete**.

Add an Auto Update Server

The Auto Update server (AUS) supports a pull model of configuration that can be used for the initial configuration, configuration updates, operating system updates and periodic configuration verification.

The Auto Update server is ideal for remote PIX firewall network (including SOHO), remote sales agent, and educational networks. The Auto Update server also supports the management of remote firewalls that are dynamically addressed with DHCP or networks with intermittent connectivity.

The Auto Update server increases the scalability of remote security networks, reduces the costs involved in maintaining a remote security network, and enables the management of dynamically addressed remote firewalls. The Auto Update server is a component of the CiscoWorks VPN/Security Management Solution (VMS).

You can use this feature to add, edit, and delete devices managed using Auto Update Server. The CiscoWorks Auto Update Server is a web-based interface for upgrading device configuration files and software images on firewalls that use the auto update feature.

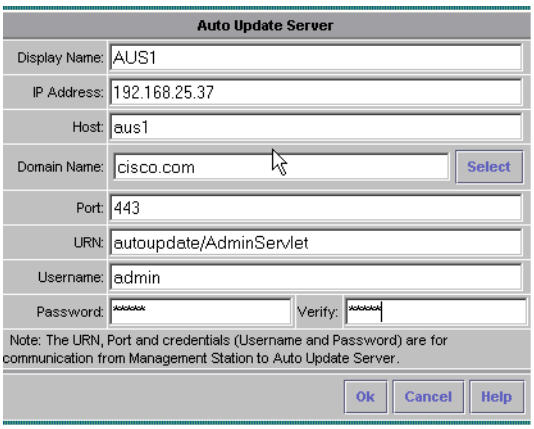
The Auto Update Server managed device has its own attributes and credentials just like normal devices in DCR. In addition, it will have the following attributes:

- Device Identity: The string value that uniquely identifies the device in parent Auto Update Server.
- The DCR Device ID of the parent Auto Update Server record.

To add an Auto Update server to be managed by DCR:

Step 1 From the Common Services Panel, choose **Device and Credentials > Auto Update Server Management** (see Figure 2-15).

Figure 2-15 Defining an Auto Update Server



These credentials fields enable the NM station to access the Auto Update server.

Step 2 Enter the appropriate information in each of the fields in the Auto Update Server dialog box, then click **OK**.

Import Devices and Their Credentials

You can import device lists, device properties or attributes and device credentials to the DCR and populate DCR using this feature. Devices and credentials can be imported into DCR using the DCA from the following sources:

- File: CSV or XML format
- Local Network Management Station (NMS) (HP OpenView 6.x and NetView 7.x): Installed on the same CiscoWorks server.
- Remote NMS (HP OpenView 6.x and NetView 7.x): Installed on a different server.

For details on the procedure for importing devices and credentials, refer to the *User Guide for Common Services 3.0* at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_chapter09186a008022f961.html#wp1118446

To import devices and credentials, follow these steps:

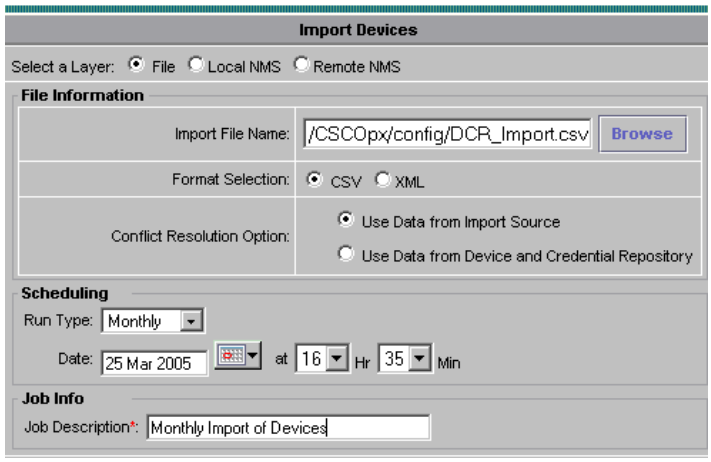
Step 1 Navigate to the CiscoWorks Home Page.

Step 2 From the Common Services panel, choose **Device and Credentials > Device Management**.

Step 3 Click **Bulk Import** (in the lower right frame).

The following screen appears (seeFigure 2-16):

Figure 2-16 Specifying the Device Import Information



The Import Devices dialog box has radio buttons to choose to import the devices from a file:

- Local NMS
- Remote NMS

The import operation can be run by a job that can be scheduled daily, weekly, or monthly. The **Conflict Resolution** option can resolve conflicts in credentials for devices that are already part of the CiscoWorks server.

Export Devices and Their Credentials

You can use this feature to export a list of device and their credentials into a file. The device list can be obtained from the device selector, or from a CSV file.

For details on this procedure, refer to the *User Guide for Common Services 3.0* at the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_chapter09186a008022f961.html#wp1057600

To specify the credentials you need to export, you can edit the *Export Format* file located at:

NMSROOT\objects\dcrimpexp\conf\Export_Format_CSV.xml or Export_Format_XML.xml

To see the list of attributes that can be exported:

1. At the command prompt, enter `NMSROOT/bin/dcrcli -u username`.
2. Enter the password corresponding to the user name.

3. Enter `lsattr`.

   The list of attributes and their description is displayed. You can include the attributes you need to export in the *Export Format* file.

Note The list of attributes that need to be exported is not shown as part of the user interface. You can specify the attributes to be imported by editing either the *Export_Format_XML.xml* file or the *Export_Format_CSV.xml* file (these files are located in the *$NMSROOT/objects/dcrimpexp/conf* directory).

To export devices and credentials, follow these steps:

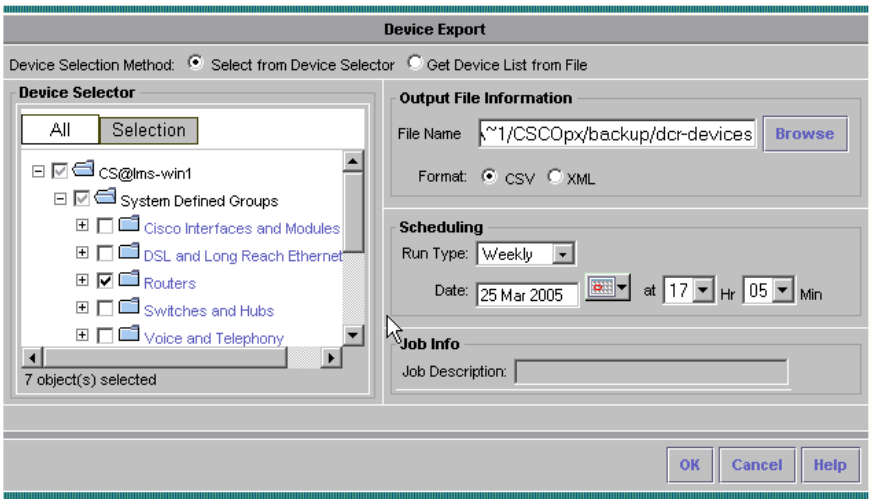
Step 1 Navigate to the CiscoWorks Home Page.

Step 2 From the Common Services panel, choose **Device and Credentials > Device Management**.

Step 3 Click **Export**.

The following screen appears (see Figure 2-17):

Figure 2-17 Specifying the Device Export Information



You can use either of the following device selection methods:

- Select from Device Selector

  Select this option if you want to export devices from DCR to the file you specify in the *Output File Information* field. You can select the required devices from the Device Selector pane of the Device Export dialog box.

- Get Device List from File

  Select this option if you want to export devices from a CSV file that is already present in the server, to the file you specify in the *Output File Information* field.

  You can use this option when the CSV file contains only partial device credentials, and you want to get the full list of credentials. The input CSV file checks for data in DCR, and exports the data to the output file.

Tip To export up to a maximum of 1,000 devices, we recommend that you use the **Get Device List from File** option.

Device and Credentials Repository Command-Line Interface

Using the command-line interface, you can add, delete, modify devices and change DCR modes. You can also view the list of DCR attributes that can be stored in DCR, and view the current DCR mode.

The command line interface can be invoked in two modes.

- Enter a Unix shell-like environment where you can invoke the various DCR command-line interface subcommands.
- Execute the CLI from the command line and provide the input parameters via an input file.

Invoke DCR CLI Subcommands in a Shell Environment

The main command to launch the DCR command-line interface is at *NMSROOT/bin/dcrcli*.

To invoke DCR command-line interface subcommands in a shell environment, follow these steps:

Step 1 Enter **`NMSROOT/bin/dcrcli`** `-u` *`username`*

Step 2 Enter the password corresponding to the username.

Step 3 Select one of the various top-level commands.

Table 2-4 DCR Command-Line Interface

Command	Syntax and Description

add	`add {ip=`*`ipaddress`*`|hn=`*`hostname`*`|di=`*`deviceID`*`} dn=`*`displayName`* `-a attribName=`*`attribValue`*`,...`
	Adds the specified device to the DCR server's device list. You must specify an IP address, host name, or device ID. You can specify as many comma-separated attribute name-value pairs as needed. For example:
	`add hn=MyHostName dn=MyDevice -a sysObjectID=23.45.65.29`

del	`del id=`*`value`* Deletes the specified device. You must specify the id=*dcr_device_id* (an internal value maintained by DCR). For example: `del id=256666989`
detail	`detail id=`*`deviceID`* Lists the values of all attributes for a DCR device. You must specify the device's DCR device ID. For example: `detail id=89992921023`
exit	Exits the DCR command line interpreter shell.

Table 2-4 DCR Command-Line Interface (continued)

Command	Syntax and Description

exp	`exp fn=filename ft={csv|xml}`
	Exports the current DCR device list to a file in CSV or XML format. You must specify a filename with complete path, and whether the file type is in CSV or XML format. For example:
	`exp fn=d:/mypath/myExportFile.xml ft=xml`

impAcs	`impAcs ot=OS Type hn=hostname un=username pwd=password prt=port number` Imports device information directly from a remote ACS system. None of the parameters are optional. You must specify the ACS system's OT (OS type), host name, password, and PRT (port) with the command. For example: `impAcs ot=WIN2K hn=MyHostName un=ADMIN pwd=ADMIN999 prt=2001`
impFile	`impFile fn=filename ft={csv|xml}` Imports device information from a file. You must specify a filename with a complete path, and whether the file type is in CSV or XML format. For example: `impFile fn=d:/mypath/myImportFile.xml ft=xml`
impNMS	`impNms {nt=HPOV6.x|Netview7.x} il=value` Imports device information directly from a local NMS. You must specify the NMS type and the il=*value* (**il** is the install location). For example: `impNms nt=HPOV6.x il=/opt/OV`

impRNms	`impRNms={ntHPOV6.x | NetView7.x} hn=value un=value il=`**`value`** `ot=value`
	Imports devices from a remote NMS.
	You must specify the NMS type and the hn=*value* (host name), un=*value* (user name), il=*value* (installation location on the remote server), ot=*value* (OS type). For example:
	`impRNms nt=HPOV6.x hn=1.2.3.4 un=root il=/opt/OV ot=SOL`

lsattr	`lsattr` Lists all the names of all defined device attributes in the DCR server. Note that these are attribute names (including user-defined fields), not the values stored for those attributes. The command takes no parameters.
lsids	`lsids {all|dn=displayName|ip=IPAddress}` Lists the DCR device IDs for devices stored on the DCR server. It will list all devices if you specify no additional parameters, or only the device ID for the device with the specified display name or IP address. If several devices share the same IP address, the command will list the device IDs for all of them. For example: `lsids ip=168.192.1.20`

mod	`mod id=value`
	`{ip=ipaddress|hn=hostname|di=device_identity value} dn=displayName -a attribName=attribValue,...`
	Modifies the specified device. In addition to the id=*dcr_device_id* (an internal value maintained by DCR) and display name, you must specify at least an IP address, host name or device_identity value. For example:
	`mod id=256666989 ip=168.140.1.1 dn=MyDevice -a sysObjectID=99.242.780`

setmaster	`setmaster` Sets the DCR server to Master mode. The command takes no parameters.

Table 2-4 DCR Command-Line Interface (continued)

Command	Syntax and Description
setslave	`setslave master=DCRGroupID port=portNumber` Sets the DCR server to Slave mode. You must specify the DCR Group ID for the new Master with which this slave will communicate. You must also specify the Master's port number if it is anything except **443** (443 is the default Master port). For example: `setslave master=DCRMaster221 port=1099`
setstand	`setstand` Sets the DCR server to Standalone mode. The command takes no parameters.

Invoke DCR CLI from the Command Line

You can invoke the DCR command-line interface from the command line. The format of the command is as follows:

```
dcrcli -u username cmd=commands fn=filename ft=(csv or xml)
```

In the command above, the parameter **commands** can be of any value provided in Step 3 in the previous section. The **fn** and **ft** options are used for import and export options in the command list.

Here is an example of the command to import devices into DCR using the command line:

```
dcrcli -u admin cmd=impFile fn=d:/full_access/test ft=csv
```

- **impFile**: Selects the import file option.
- **fn**: Specifies the filename from which the devices need to be imported.
- **ft**: Specifies if the input file is in CSV format.

Refer to the *User Guide for Common Services 3.0* to get more details on the DCR command-line interface (see Appendix A, "Accessing the CiscoWorks User Guides").

CHAPTER 3

Enabling Single Sign-On

Introduction

Single Sign On (SSO) helps the user to use a single session to navigate to multiple Cisco Works servers without having to authenticate to each of them. Communication between multiple Cisco Works servers is enabled by a trust model addressed by certificates and shared secrets.

Using SSO can be summarized as follows:

- When you first log in to the slave servers, you're redirected to the master server for logging in. Check the URL while you log in. The login page should be that of the master server.

  After the login is successful, you're redirected to the slave server home page.
- When you successfully log into the master server, you can access any slave server home page without having to log in again.
- The Master server is used for authentication purposes only.

Setting Up Single Sign On

To set up Single Sign On, complete the following initial tasks:

1. Set up one of the CiscoWorks servers as the authentication server or Master SSO server.
2. Using self-signed certificates, build trust between the CiscoWorks servers.

   You can create a trusted certificate by adding it in the trust key store of the server. CiscoWorks TrustStore or KeyStore is maintained by the certificate management framework in Common Services.
3. Have each slave SSO CiscoWorks server set up a shared secret with the Master SSO authentication server. The System Identity user password acts as a secret key for SSO.

The SSO authentication server is called the *Master*, and the SSO regular server is called the *Slave*.

CiscoWorks Modes of Authentication

CiscoWorks has two modes of authentication:

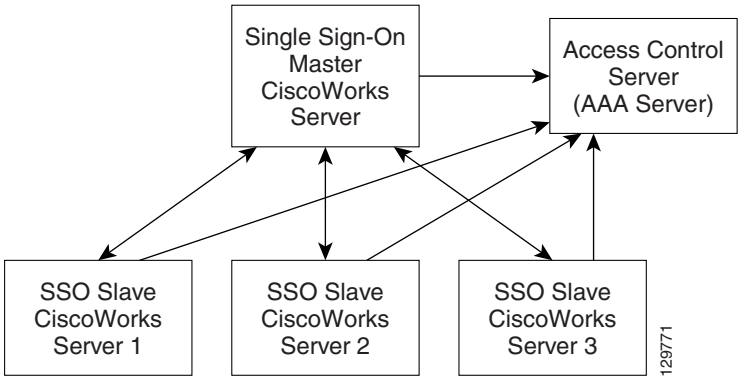
- One is local to the Cisco Works server based on the users created in the system.
- The other is based on users created on the ACS server, in other words, based on AAA.

Setup Recommendations

Cisco makes the following recommendations:

- Set up Single Sign On *only* when the SSO Master and SSO Slave servers are using a AAA server for authentication and authorization.
- Set up Single Sign On *only* when the SSO Master and SSO Slave servers are pointing to the same AAA server for authentication and authorization (see Figure 3-1).

Figure 3-1 Single Sign On Server Setup



If the Server Is Configured as Master or Slave

Perform the following tasks if the server is configured as Master or Slave:

1. Configure the System Identity user password in both the Master and Slave servers. Enter the same System Identity user name and password in both Master and Slave. (See the "Set Up the System Identity User" section on page 3-2.)
2. Configure the Master's Self-Signed Certificate in the Slave server. (See the "Configure the Master's Self Signed Certificate in the Slave" section on page 3-3.)

The Master and Slave servers form an SSO domain (similar to the management domain).

Note The Single Sign On Domain and the Management Domain are completely different elements. A Single Sign On Master does not need be a DCR Master and vice versa.

Set Up the System Identity User

SSO uses the System Identity User password as the secret key to provide confidentiality and authenticity between Master and Slave.

It is sufficient to have the same System Identity User passwords in the Master and Slave, without having the same username.

Note We recommend that you have the same user name and password across Master and Slave.

To set up the System Identity User:

Step 1 Choose **Common Services > Server > Security > System Identity Setup**.

Step 2 Enter the username and password.

Step 3 Click **Apply**.

Configure the Master's Self Signed Certificate in the Slave

To configure the Master's Self Signed Certificate in the Slave:

Choose **Common Services > Server > Security > Peer Server Certificate Setup > Add**.

The CN present in the certificate should match with the Master server name. Otherwise it is not considered a valid certificate.

Navigate Between Cisco Works Servers

To navigate seamlessly between CiscoWorks servers, use the *Link Registration* feature and create links to slave SSO servers in the Master server and vice versa. Now you can simply click on the links to navigate between the slave and master servers seamlessly.

CHAPTER 4

Grouping Services

Introduction

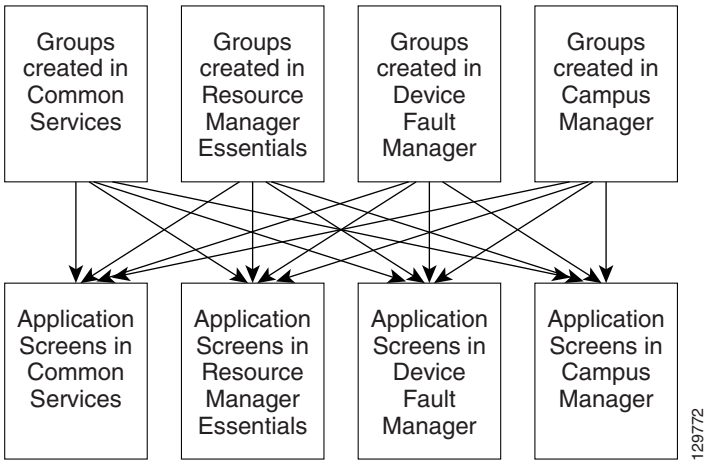
The *Groups* feature in Common Services helps you to group devices managed by CiscoWorks applications. It helps to create, manage, and share groups of devices. The groups created are shared across applications. The groups created in applications can also be viewed from Common Services.

The Groups feature is comprised of the following components:

- **Group Server**: Manages groups of devices. It helps you to create, edit, delete, and refresh groups. The Group server evaluates group rules and retrieve devices of a particular group.
- **Group Admin**: Allows you to interact with the Group server to create and manipulate groups using Group Admin.

In the case of the LAN Management Solution (LMS) bundle, Figure 4-1 depicts the usage of groups that are created in various applications.

Figure 4-1 Implementing Groups in LAN Management Solution (LMS)



Creating Groups in the LMS Applications

To create groups in the applications in LMS, navigate through the following paths from the CiscoWorks Home Page:

- *Common Services*: Navigate to the **Common Services panel > Groups > Group Admin**.

- *Resource Manager Essentials*: Navigate to the **RME panel > Devices > Group Administration**.
- *Device Fault Manager*: Navigate to the **Device Fault Manager panel > Configuration > Other Configuration > Group Administration**.
- *Campus Manager*: Navigate to the **Campus Manager panel > Administration > Groups**.

Group Concepts

A group is a named set of devices. The group is characterized by a set of properties such as an associated rule, name, description, type, and access permission.

- The rule determines the membership of a group, which may change whenever the rule is evaluated.
- Groups are managed in a hierarchical fashion that supports subgrouping.

  Each child group is a subgroup of a parent group and its group membership will be a subset of its immediate parent group. Changes in some of the properties of a parent group impact all child groups under it. These properties include Name, Rule, Evaluation Type, and Access Permissions. When you remove a group, all child groups under it are also removed. However, when a user is removed from the list of users, the groups created by the user are not removed.
- Groups can be dynamic or static.
  - A dynamic group is a group for which the membership list is always up-to-date—a dynamic group's membership list is effectively computed every time you view its members. Whenever you view a dynamic group, it always displays the latest group membership list.
  - A static group's membership is refreshed only when you explicitly request it. Between reevaluations, the Group server stores the membership list and group definition of the static group. Whenever you view a static group, you get the membership list that was created the last time the group rule was evaluated.
- Groups can be private or public in scope.
- Container groups are groups with no rule, whose membership is the union of the membership of its children.

Common Groups and Shared Groups

Common groups are the Common Services (CS) groups that are seen in the Groups user interfaces of CiscoWorks applications. A Groups user interface is any user interface in CiscoWorks in which groups are shown in a device selector window. Shared groups are the application groups other than the application's local group that can be seen from the Common Services and the applications' Groups user interfaces.

You have read-only access on shared groups. You can perform the following tasks:

- Check group details
- Refresh the group

To perform any operation on Common Services groups, you have to invoke the Groups user interface from Common Services. From the Common Services Group Admin user interface, you cannot perform create, edit, and delete operations on Application Groups.

Provider Groups

For example, if you have a machine on which Common Services, RME, and Campus Manager are installed.

Common Services Provider Groups

If you invoke the Groups user interface from Common Services, you can see three provider groups. They are:

- CS@hostname
- RME@hostname
- Campus@hostname

The group CS@hostname is the local group.

The groups RME@hostname and Campus@hostname are shared groups.

RME Provider Groups

If you invoke the Groups user interface from RME, you will find three provider groups:

- CS@hostname
- RME@hostname
- Campus@hostname

Here, RME@hostname is the local group.

CS@hostname is the common group, and Campus@hostname is a shared group.

Campus Manager Provider Groups

Similarly, in the Groups user interface in Campus Manager, Campus@hostname is the local group. RME@hostname is a shared group, and CS@hostname is the common group.

System-Defined Groups and User-Defined Groups

Two predefined top level parent groups are available when Common Services is installed:

- System-defined groups: Automatically created based on device type information in Device and Credentials Repository (DCR).

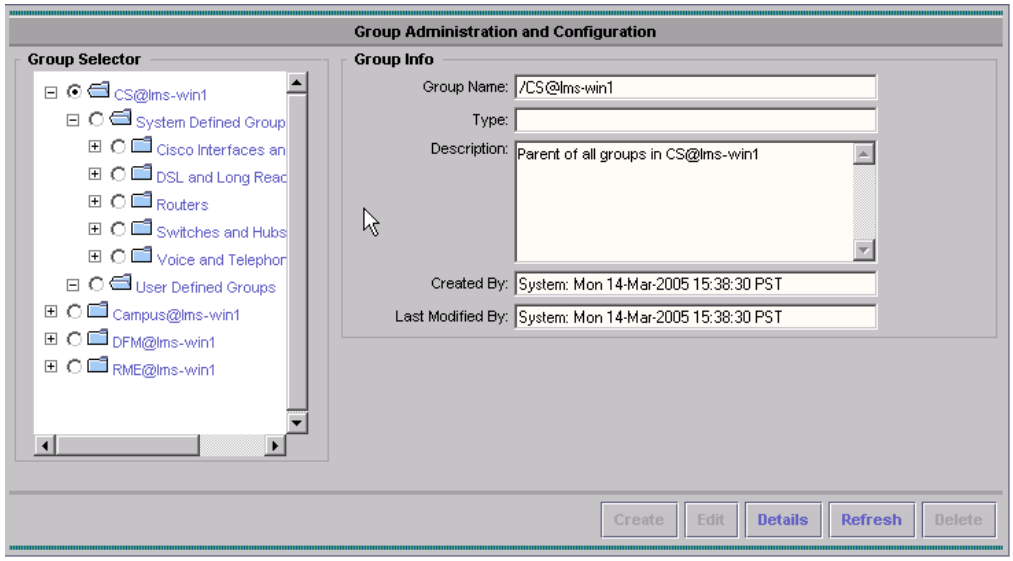
  When a device is added to DCR, the device is either added to an existing group with the corresponding device type, or if such a group does not exist, a new group based on the device type is automatically created. If all devices belonging to a device type are deleted in DCR, the corresponding group will also be deleted. System-defined groups cannot be created.

- User-defined groups: Groups can be created here based on device attributes in DCR. This is possible only if the user has admin privileges.

These predefined groups come under the Provider group (or the root group), which by default has the format: *CS@hostname*. This Provider group is the parent of all groups found in the machine/server.

To illustrate this with an example as shown in Figure 4-2, the provider group name is *CS@lms-win1* where *lms-win1* is the display name of the machine/server.

Figure 4-2 Example of Provider Group



The provider group name is the top-level group name in each group hierarchy.

You can change the provider group name by changing the CiscoWorks Home Page Server Name, which can be configured at **Common Services > HomePage > Settings**.

For the name change to take effect, the Daemon Manager has to be restarted after changing the provider group name. After this, the provider group name will be of the format CS@CWHP Server Name. These groups can be viewed in the Device Credentials Admin (DCA) user interface and Device Center user interface. Actions can be performed on the members of the group.

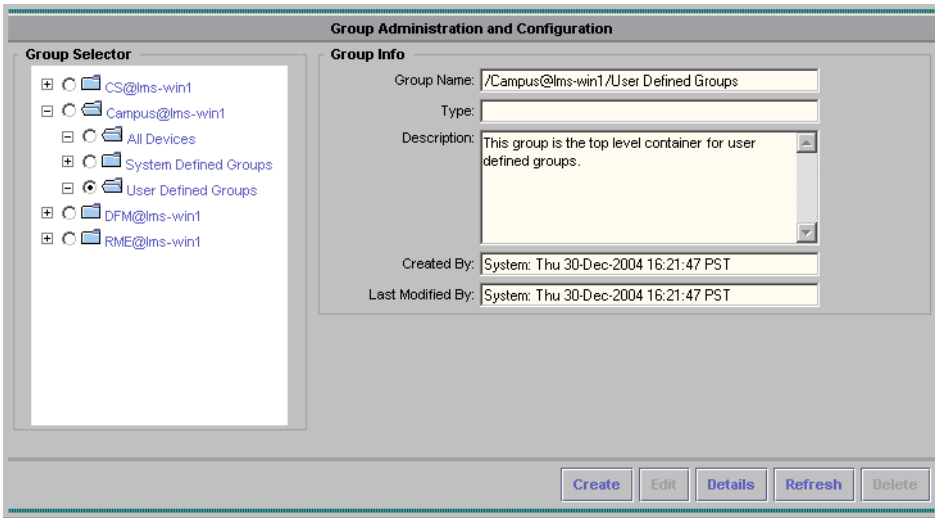
Example of Creating a Group

This section describes the procedure for creating groups in Campus Manager.

Step 1 In the CiscoWorks Homepage, choose **Common Services > Groups > Group Admin**.

The Campus Manager Group Administration dialog box appears (see Figure 4-3).

Figure 4-3 Campus Manager Group Administration

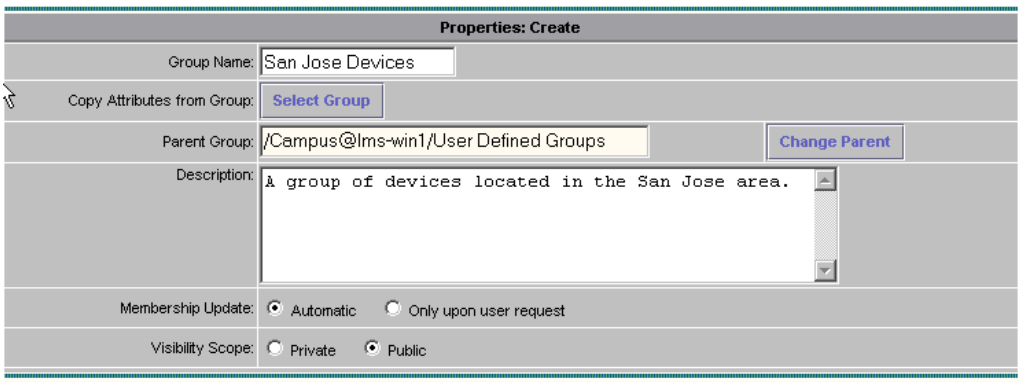


You can create a group called *MyGroup1* under the */Campus@lms-win1/User Defined Groups* group.

Step 2 Click **Create**.

The Group Properties dialog box is displayed (see Figure 4-4).

Figure 4-4 Group Properties



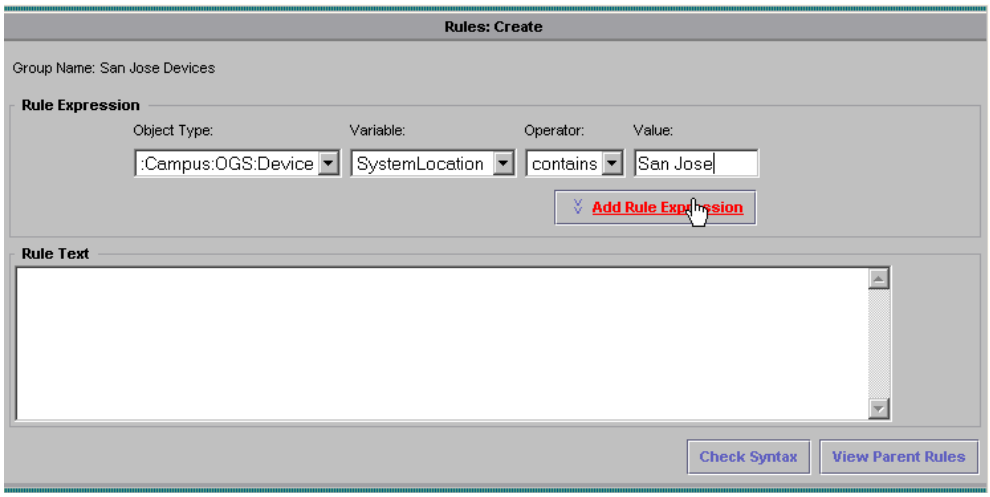
While specifying group properties, you can enter the properties such as name and description, and modify the parent group, if required, and update membership, and specify the visibility scope.

The group name must be unique within the parent group. However, it need not be so across groups. The same group name cannot be used in the same group hierarchy.

For example, if you have a group */CS@servername/User Defined Groups/MyView*, you cannot create another group with the same name "MyView" under /CS@servername/User Defined Groups.

Step 3 Click **Next**.

Figure 4-5 Create Rules



In the Create Rules dialog box, you can define the rules for the group. The rules you define in this phase determine the contents of the group. The rules you specify here determine the devices to be included in the group.

If you have created the group copying the attributes of another group, the rules specified for that group appears in the *Rule Text* field. You can retain these and add more rules, or delete these rules and create a new set of rules.

In the Create Rules dialog box, you can either enter the rules directly in the *Rule Text* field, or select the components of the rule from the *Rule Expression* fields, and form a rule.

The rule expression has the following components:

Class.attribute operator value

The Create Rules dialog box allows you to check the syntax in the Rules Text field. You can use this facility to validate the rules you have created.

If you leave the rule blank, it creates a Container group.

To display the rules defined for its ancestor groups, click **View Parent Rules**.

You can select the parameters from Rule Expression fields to create a new set of rules.

If you do not want to use the rules currently displayed in the *Rule Text* field, you will have to create a new set of rules.

Step 4 To create a new set of rules:

a. Delete the rules displayed in the *Rule Text* field, and click any other field.

b. Select appropriate parameters for *Object Type*, *Variable*, and *Operator*.

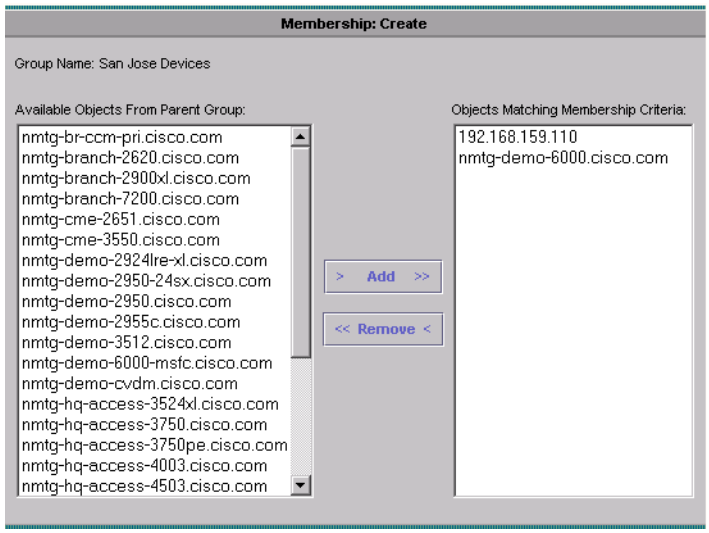
c. Enter the value for the variable you have selected.

d. Click **Add Rule Expression**.

The Group Administration wizard creates the rule based on the parameters you specified and adds the rule to the *Rules Text* field.

e. Click **Next**.

Figure 4-6 Create Group Memberships



To decide the devices available to the group you have created, the wizard uses the details of the parent members and rules you have already specified.

These devices appear in Available Objects From Parent Group column based on the properties and rules you have already specified.

Step 5 To add devices to the group you have created:

a. Select one or more devices in Available Objects From Parent Group column.

b. Click **Add**.

The selected devices are removed from Available Objects From Parent Group and added to the Object Matching Membership Criteria column.

Step 6 Click **Next**.

Figure 4-7 Summary of New Group

Summary: Create	
Group Name:	San Jose Devices
Parent Group:	/Campus@lms-win1/User Defined Groups
Description:	A group of devices located in the San Jose area.
Membership Update:	Automatic
Rules:	:Campus:OGS:Device.SystemLocation contains "San Jose"
Visibility Scope:	Public

Figure 4-7 is a summary page that shows all of the properties of the group:

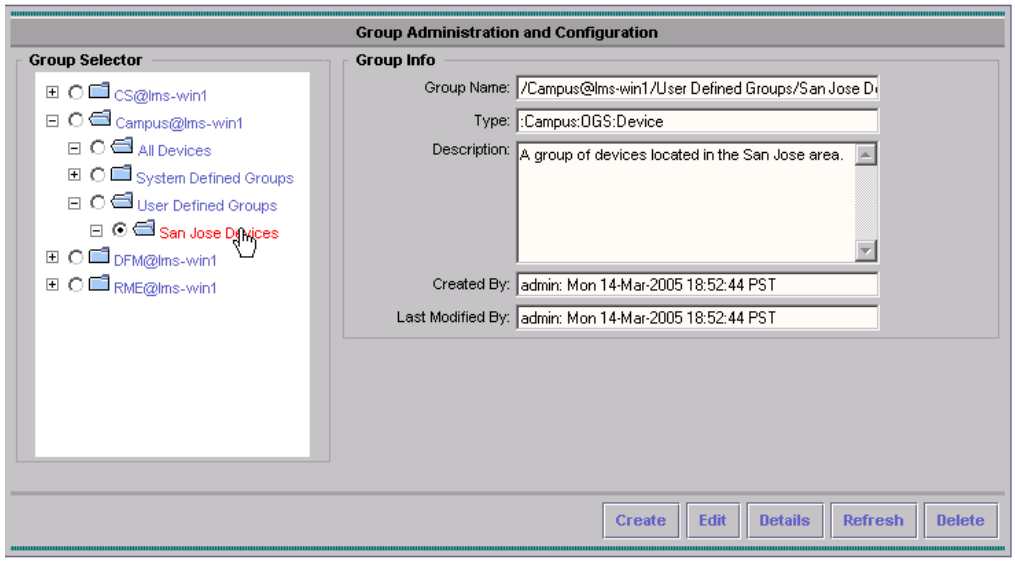
- Group Name.
- Parent Group. The group underneath which the current group is to be created. Thus the current group membership will be a subset of the parent group.
- Description

- Membership Update type. This indicates whether the group will be evaluated when a user accesses it or once when the group is created and then periodically refreshed by the user).
- Rule. Criteria that determines the group membership.
- Visibility Scope. Indicates whether only the creator of the group can access it or all CiscoWorks server users can access it.

Step 7 Click **Finish**.

The group will be created as shown Figure 4-8.

Figure 4-8 New Group Created



Creating a group through group administration in Common Services will also follow the same steps as shown in this example. The only difference will be that the variable used in creating the rule will be different.

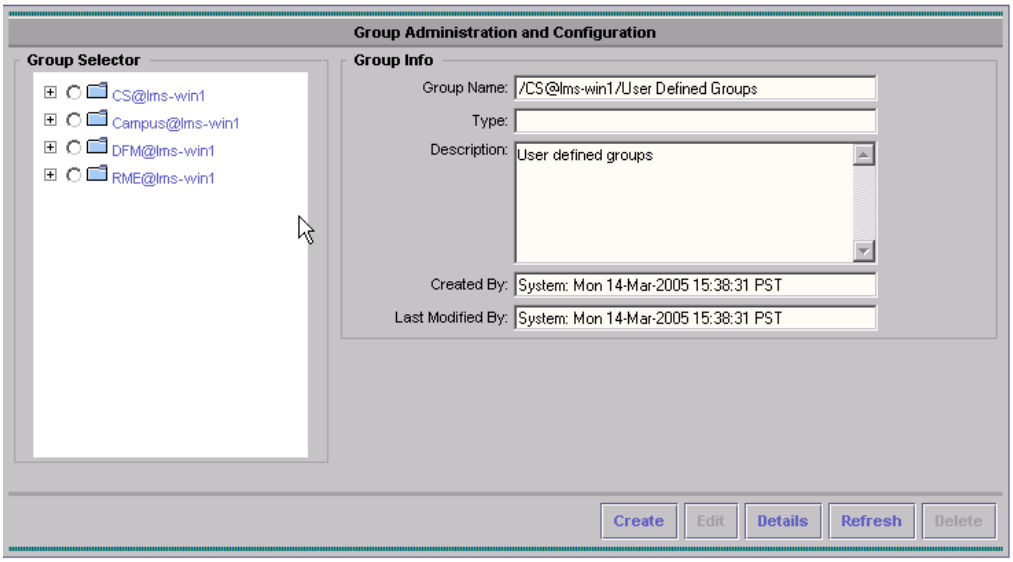
Groups in a Single-Server Scenario

The devices you see in the Group Administration user interface in applications depends on whether the devices are being managed by that particular application or not.

For example, if we have Common Services, Campus Manager, and RME installed on a server, you can see the following groups in the Groups user interfaces of Common Services, Campus Manager, and RME (see Figure 4-9).

- CS@hostname
- RME@hostname
- Campus@hostname

Figure 4-9 Single Server Group Administration



Let's say you add 100 devices to the subgroup Routers in Common Services. All the 100 routers you have added are listed whenever you perform any operation on the group Routers, from the Groups user interface in Common Services.

However, if you perform any operation on the subgroup Routers, from the Groups user interface in RME, you may not see all the 100 devices you have added to the group from Common Services. Instead, you will see only those devices that RME manages are displayed.

Assume you create a subgroup in Campus Manager, based on subnets, and add 30 devices. When you perform any operation on this subgroup from the Groups user interface in RME, the number of devices you will see may be less than 30. This depends on whether RME is managing those devices.

Top-Level Groups in Common Services

The following are the descriptions of the top level groups seen in the Group Selector pane in Figure 4-9.

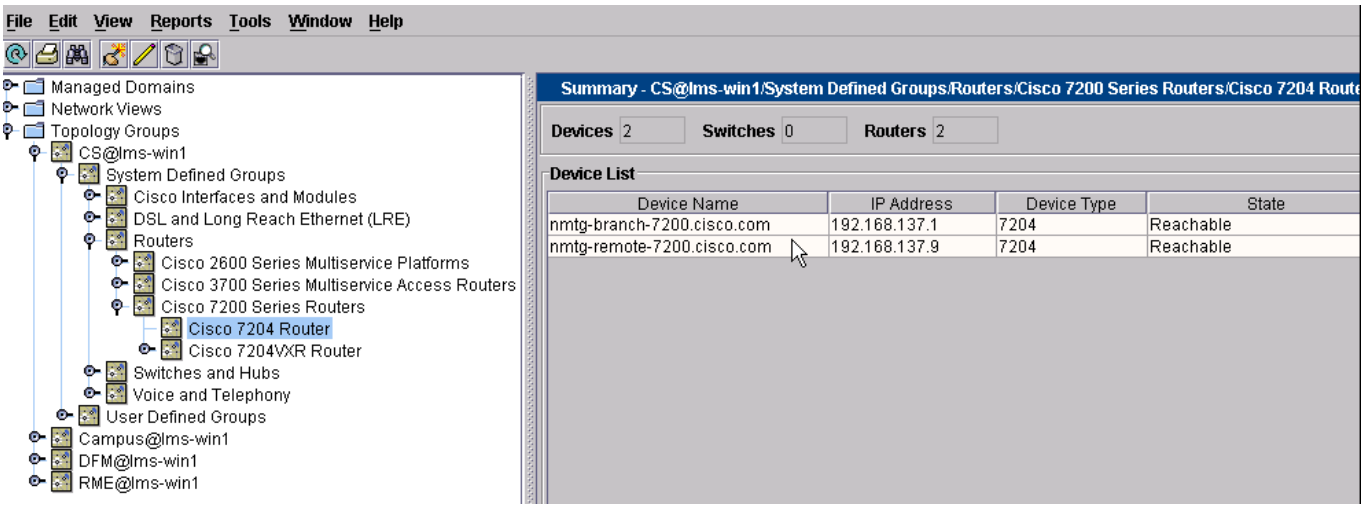
- CS@lms-win1: Contains both system defined and user defined groups created in Common Services in the lms-win1 server machine. The groups created in Common Services are based on criteria using DCR attributes.
- Campus@lms-win1: Contains system defined, user defined, and all devices groups created in Campus Manager in the lms-win1 server machine. The groups created in Campus Manager are based on criteria using attributes exposed by Campus Manager.
- DFM@lms-win1: Contains a user defined group created in Device Fault Manager in the lms-win1 server machine. The groups created in Device Fault Manager are based on criteria using attributes exposed by Device Fault Manager.
- RME@lms-win1: Contains all devices, normal devices, predeployed, previous selection, saved device list, and user defined groups created in Resource Manager Essentials in the lms-win1 server machine. The groups created in Resource Manager Essentials are based on criteria using attributes exposed by Resource Manager Essentials.

You can edit the user-defined groups of the top-level groups only by navigating to the corresponding application group administration screen. For example, you can edit User Defined Groups defined under *CS@lms-win1* only by going to the group administration screen in Common Services.

DCR is the central location where device information (including credentials information, user defined attributes, and identity attributes) is stored. In LAN Management Solution (LMS), devices need to be imported into the individual applications like RME, Campus Manager and Device Fault Manager. If a device D1 is imported into Campus Manager but not imported into RME, then D1 will be shown as a member of a group (for example) G1 in Campus Manager Application screens and may not show up in RME application screens.

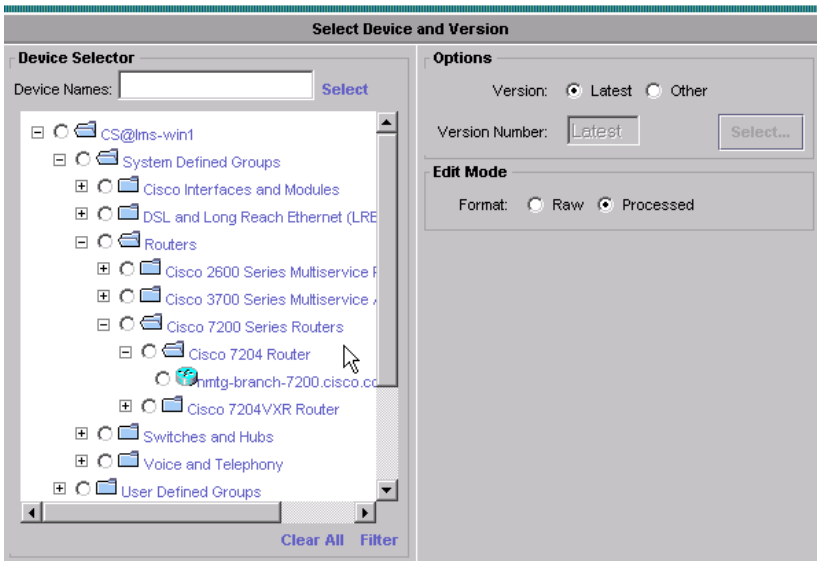
To illustrate this, the Topology Services window of Campus Manager shows the device nmtg-remote-7200.cisco.com as a member of group */CS@lms-win1/System Defined Groups/Routers/Cisco 7200 Series Routers/Cisco 7204 Router* (see Figure 4-10).

Figure 4-10 Topology Services Window in Campus Manager



But, the same device won't be shown as a member of the group */CS@lms-win1/System Defined Groups/Routers/Cisco 7200 Series Routers/Cisco 7204 Router* in an RME Config Editor Application screen (see Figure 4-11).

Figure 4-11 Single Server: Resource Manager Essentials Config Editor



Groups in a Multi-Server Scenario

Groups you create in Common Services group administration in the Master get synchronized with the Slave server. This does not happen in the case of applications. (Whenever a group is created, it is done through *Group Administration*.)

If you create a subgroup under CS@master hostname in one server, it will appear under CS@slave hostname in the peer server.

But in the Master server, if you create a subgroup under application@master hostname, it will always appear under application@\master hostname\, in the Slave. That is, the subgroup created in the Master appears under the application's shared group in the Slave.

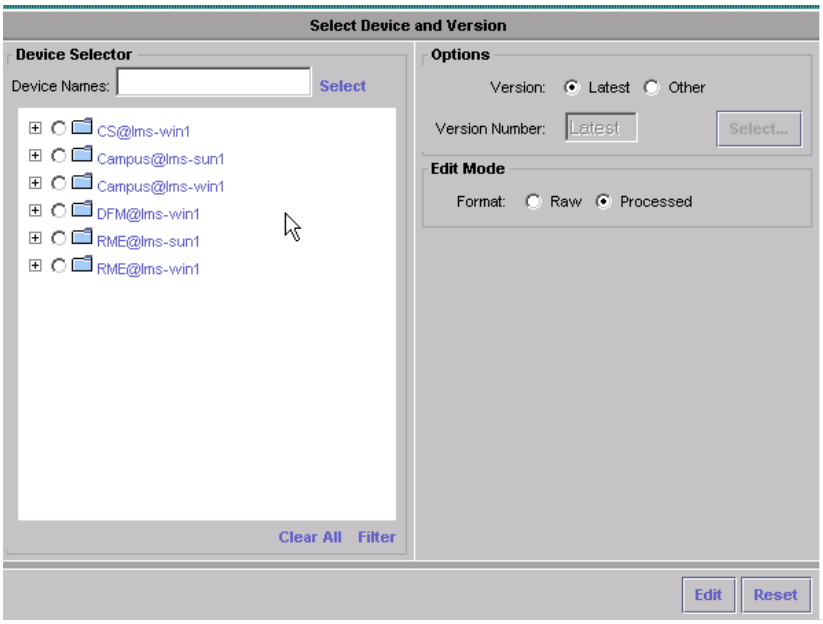
Note You cannot create groups in Common Services if it is in Slave mode. But for applications, you can create groups even if the server on which they are installed is in Slave mode.

LAN Management Solutions applications installed in a DCR Master server can use groups created in the LMS applications of a DCR Slave server. To illustrate this, consider the following example in which:

- The DCR Master server (the *lms-win1* machine) has all applications (Campus Manager, Device Fault Manager and Resource Manager Essentials) installed in it.
- The DCR Slave server (the *lms-sun1* machine) has all applications except Device Fault Manager installed in it.

When you open the Config Editor Application screen in Resource Manager Essentials, it will show top-level groups from all applications in both the servers.

Figure 4-12 Multi-Server: Resource Manager Essentials Config Editor



Top-Level Groups Displayed

Descriptions of the top-level groups seen in the Group Selector pane are as follows:

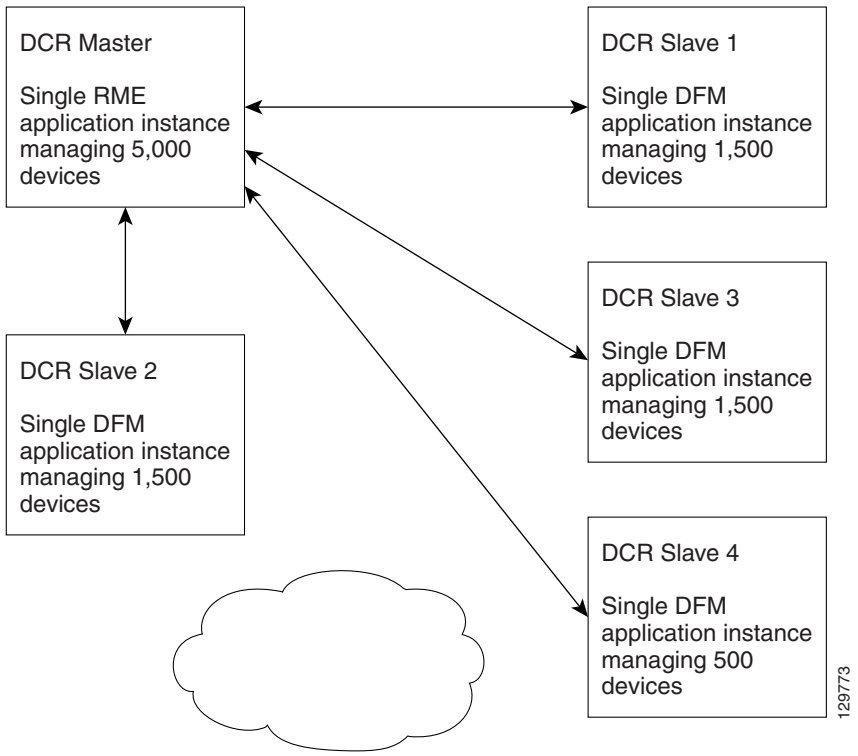
- *CS@lms-win1*: Contains both System Defined and User Defined groups created in Common Services Group Administration in the lms-win1 server machine. These Common Services groups can be created only in the DCR Master (lms-win1) and not in the DCR Slave (lms-sun1). In other words, the Common Services Group Administration user interface can be accessed only in the DCR Master and not in the DCR Slave.
- *Campus@lms-win1*: Contains System Defined, User Defined, and All Devices groups created in Campus Manager Group Administration in the lms-win1 server machine. The groups created in Campus Manager are based on criteria using attributes exposed by Campus Manager.
- *Campus@lms-sun1*: Contains System Defined, User Defined and All Devices groups created in Campus Manager Group Administration in the lms-sun1 server machine. The groups created in Campus Manager are based on criteria using attributes exposed by Campus Manager.
- *DFM@lms-win1*: Contains the User Defined group created in Device Fault Manager in the lms-win1 server machine. The groups created in Device Fault Manager are based on Criteria using attributes exposed by Device Fault Manager.
- *RME@lms-win1*: Contains All Devices, Normal Devices, Pre-Deployed, Previous Selection, Saved Device List, and User Defined groups created in Resource Manager Essentials in the lms-win1 server machine. The groups created in RME are based on criteria using attributes exposed by RME.
- *RME@lms-sun1*: Contains All Devices, Normal Devices, Pre-Deployed, Previous Selection, Saved Device List, and User Defined groups created in Resource Manager Essentials in the lms-sun1 server machine. The groups created in RME are based on criteria using attributes exposed by RME.

Note You cannot create groups in Common Services if it is in Slave mode. But, for LMS applications, you can create groups even if the server on which the applications are installed is in Slave mode.

About Sharing Groups Across Servers

Let's assume that a network has 5,000 devices that need to be managed. In LAN Management Solution (LMS), we recommend that a single Resource Manager Essentials application instance on a server manage up to 5,000 devices and a single Device Fault Manager application instance on a server manage up to 1,500 devices. So, the LMS servers would be deployed as shown in Figure 4-13:

Figure 4-13 Sharing Groups Across Servers



Let's assume that the devices managed by the Device Fault Manager instance in DCR Slave 1 are grouped based on specific criteria. The name of this group is *DFMGroup1* and it's created under */DFM@Slave1/User Defined Group*s.

Now you may want to perform a Configuration Update operation through Resource Manager Essentials on the devices of this group. In order to do this, the group */DFM@Slave1/User Defined Groups/DFMGroup1* must appear in the RME application screens. This is done by sharing groups across applications in different DCR servers (DCR Master and Slave).

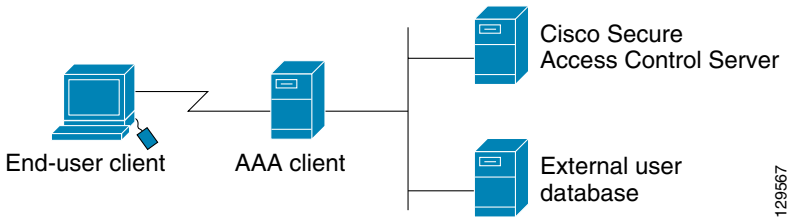
CHAPTER 5

Integrating with the ACS Server

Introduction

CiscoSecure Access Control Server (ACS) provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access server, PIXFirewall, or router (see Figure 5-1).

Figure 5-1 AAA Client Model



Why Do We Need an ACS Server?

CiscoWorks is integrated with 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. This is further explained in the **"Secure Views" section on page 5-6.**
- Provide editable user roles.

  The user roles are mapped to tasks that the user is authorized to perform on the devices. The mapping of roles to tasks can be changed in the ACS server.

To Display the Network Device Groups Table

For the Network Device Groups table to be displayed in the ACS server, the Network Device Groups option must be enabled. To enable the Network Device Groups table, take these steps:

Step 1 From the navigation menu, choose **Network Configuration**

Step 2 Click **Advanced Options**.

Step 3 Select the **Network Device Groups** check box.

Step 4 Click **Submit+Restart**.

The Network Device Groups table is now available.

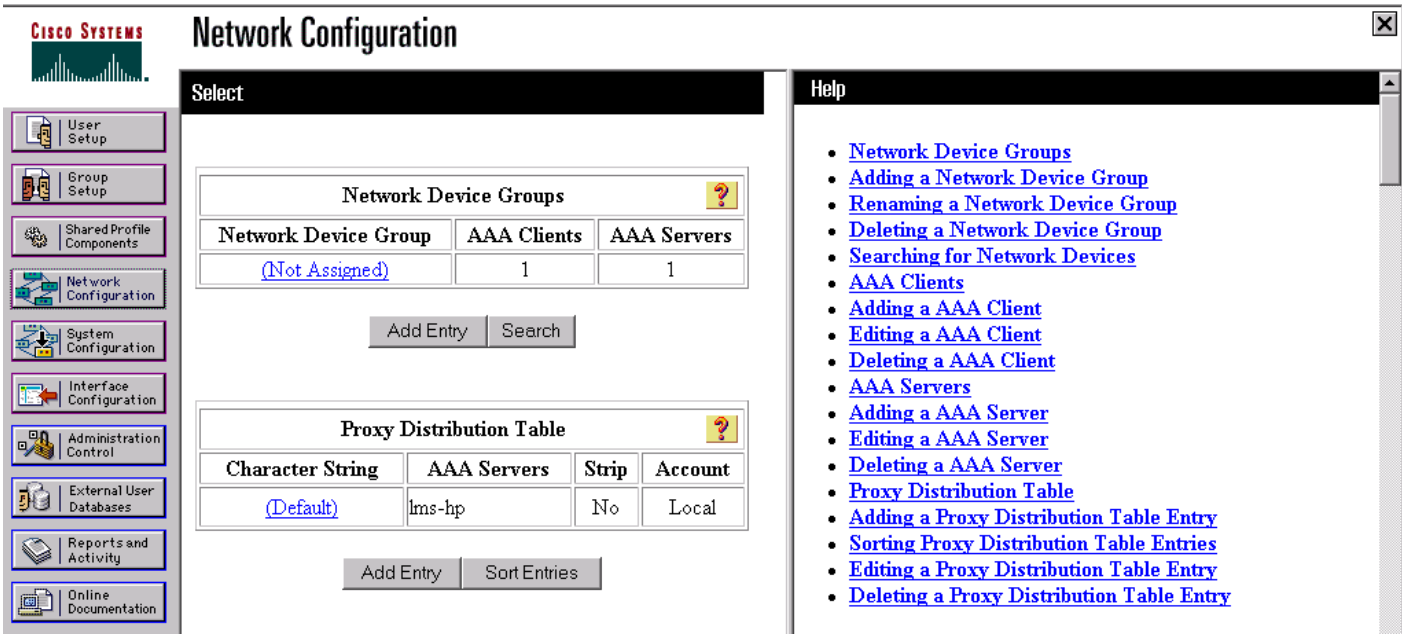
Integrating with the ACS Server

To integrate with the ACS server, follow these steps:

Step 1 From the Cisco Secure ACS log-in window, log in to the ACS server.

Step 2 From the navigation menu, choose **Network Configuration** (see Figure 5-2).

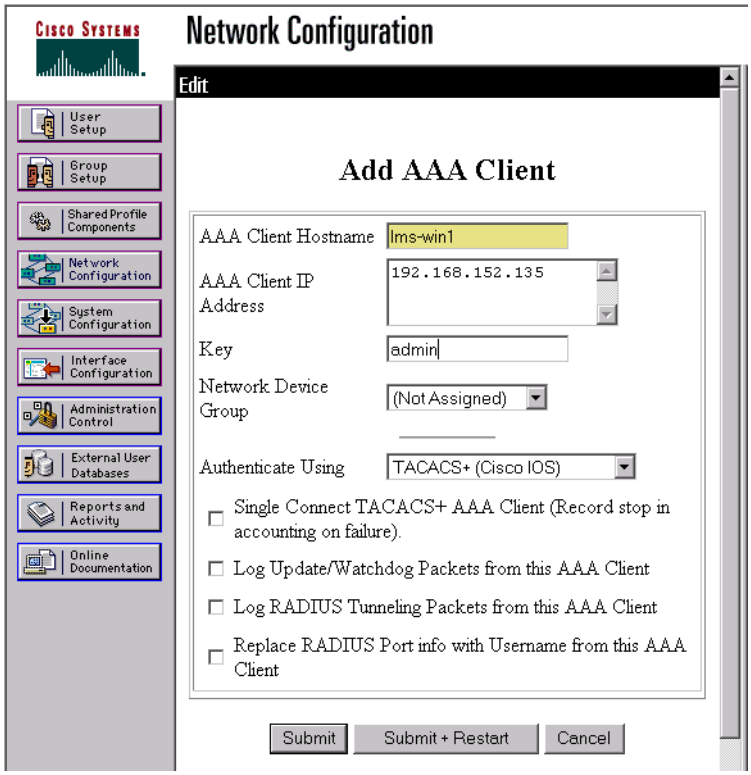
Figure 5-2 ACS Server Network Configuration Dialog Box



Step 3 In the Network Device Group table, click **(Not Assigned)**, then click **Add Entry**.

The Add AAA Client dialog box appears (see Figure 5-3).

Figure 5-3 Defining the AAA Client



Step 4 In the Add AAA Client dialog:

a. Enter the *host name* of the LMS server.

b. Enter the *IP address* of the LMS server.

c. Be sure to give a value to the *Key* field so that this client can contact the ACS server.

Step 5 Click **Submit+Restart**.

Setting Up the LMS Server

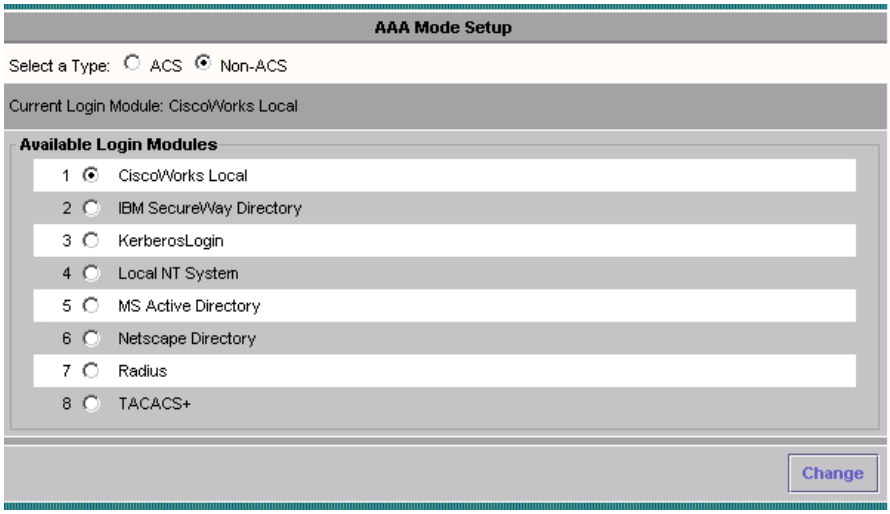
Step 1 Log in to the LMS server.

Step 2 To set the login mode of the LMS server, go to the Common Service panel, then choose **Server** > **Security**.

Step 3 Select **AAA Mode Setup** from the TOC menu options.

The AAA Mode Setup dialog box appears (see Figure 5-4).

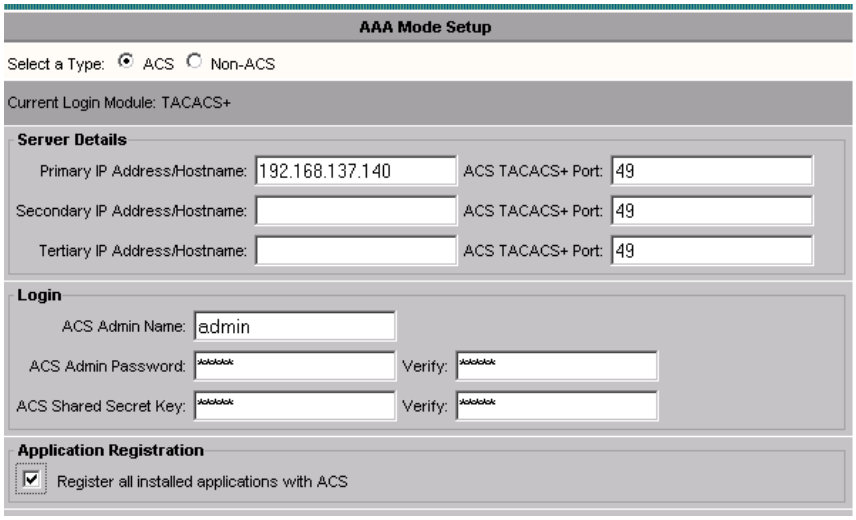
Figure 5-4 AAA Mode Setup Dialog



Step 4 Select the **ACS** option in the AAA Mode Setup window.

The dialog box shown in Figure 5-5 is displayed.

Figure 5-5 AAA Mode Setup Dialog



Step 5 Enter all the ACS server details (including the Key value provided in Step 4c in the "Integrating with the ACS Server" section on page 5-2).

- In the corresponding ACS TACACS+ port numbers fields, the default port is **49**. Secondary and Tertiary IP address and hostname details are optional.
- The values **true** and **false** will not be accepted in the *Primary*, *Secondary*, and *Tertiary IP Address/Hostname* fields.

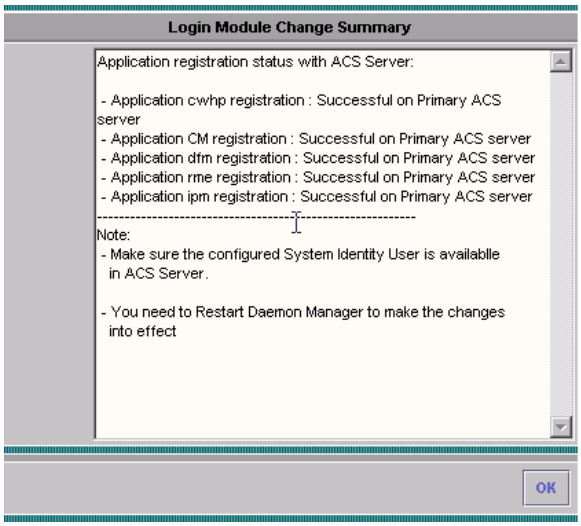
Step 6 Enable the **Register all installed applications with ACS** option to register all the installed applications with the ACS server.

Note If an application is already registered with ACS, the current registration will overwrite the previous one.

Step 7 Click **Apply**.

The following summary screen is displayed (see Figure 5-6).

Figure 5-6 Login Module Change Summary



When you click **Apply**, the following actions take place:

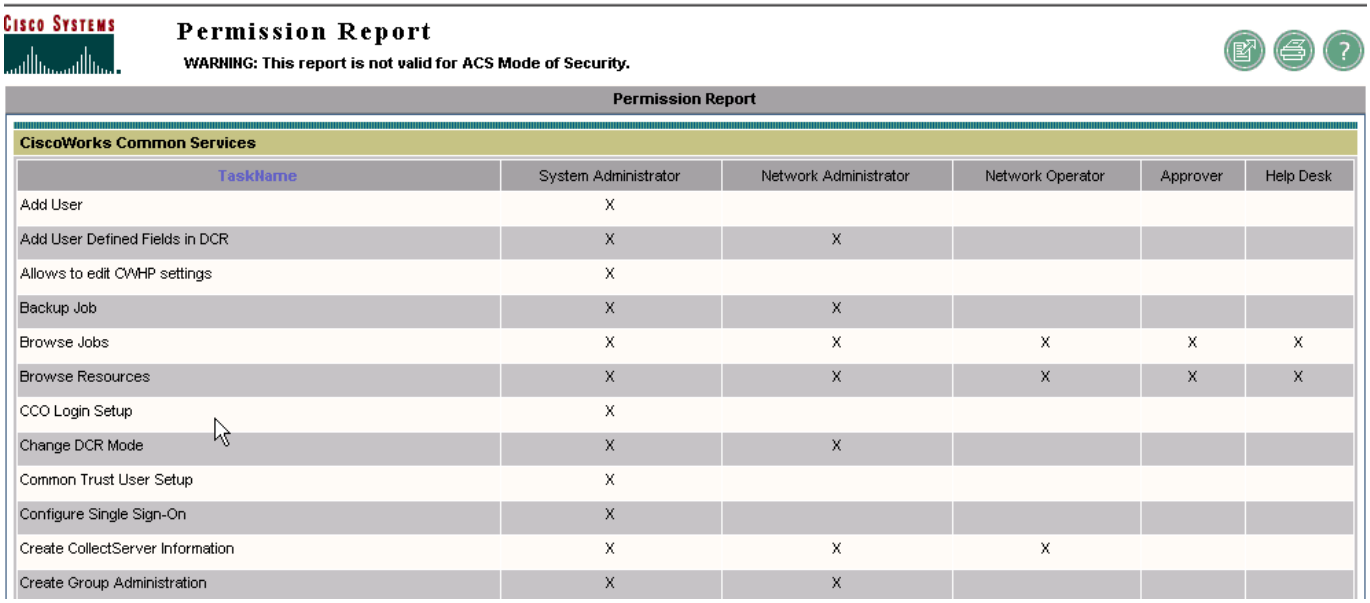
- A list of tasks in the products is registered to the ACS server.
- A list of default user roles—System Administrator, Network Administrator, Network Operator, Approved, and Help Desk—is registered to the ACS server.
- A mapping of the tasks that the above user roles can execute is registered with the ACS user.

In the case of the LMS bundle, many tasks can be executed in the following products: Campus Manager, Resource Manager Essentials, Internetwork Performance Monitor, Device Fault Manager, and Common Services.

The mapping between user roles and these tasks are registered with the user. Note that this is a default mapping of user roles and tasks.

You can access this default mapping in the LMS server by navigating to **Common Services** panel > **Server** > **Reports** > **Permission Report**. Then you can generate the report (see Figure 5-7).

Figure 5-7 Permission Report



Permission Report

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

Permission Report

CiscoWorks Common Services

TaskName	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Add User	X				
Add User Defined Fields in DCR	X	X			
Allows to edit CWHP settings	X				
Backup Job	X	X			
Browse Jobs	X	X	X	X	X
Browse Resources	X	X	X	X	X
CCO Login Setup	X				
Change DCR Mode	X	X			
Common Trust User Setup	X				
Configure Single Sign-On	X				
Create CollectServer Information	X	X	X		
Create Group Administration	X	X			

The default mapping between tasks and the roles can be changed in the ACS server, but note that the changed mapping won't be reflected in the permission report.

Step 8 Restart the Daemon Manager.

On Windows:

a. Enter `net stop crmdmgtd`

b. Enter `net start crmdmgtd`

On Solaris:

a. Enter `/etc/init.d/dmgtd stop`

b. Enter `/etc/init.d/dmgtd start`

Secure Views

Secure Views allows access to perform a task on a device or a set of devices to be restricted. Secure Views is applicable only when CiscoWorks server is in ACS Login mode.

Secure Views enable filtering of group membership based on the user and the application task context in which a request is made. Filtering is performed only when operating in ACS Login mode. While operating in non-ACS mode, no filtering is performed and evaluating a group results in all devices that group being returned.

To explain secure views, let go through the following example:

1. Two users Joe and Frank are configured in ACS.
2. Two Network Device Groups NDG1 and NDG2 are configured in ACS.
3. NDG1 contains devices D1.

4. NDG2 contains devices D2.
5. Network Administrator role is mapped to task *Edit Device Configuration*.
6. Joe has a Network Administrator role on NDG1 network device group. This means he is authorized to perform the Edit Device Configuration task on device D1 in NDG1.
7. Frank has a Network Administrator role on NDG2 network device group. This means he is authorized to perform the Edit Device Configuration task on device D2 in NDG2.
8. Group G1 is created in the LMS server and shows up in the Config Editor screen in Resource Manager Essentials. Let us assume that Group G1 has devices D1 and D2 in it.
9. When Joe logs into the LMS server and accesses the Config Editor window, he will see only device D1 in group G1. This is because his view of devices in G1 is restricted to only devices on which he can execute the Update Device Configuration task. The same is applicable to Frank as well, where he can see only device D2 in group G1 in the Config Editor screen.

Let's assume that the tasks described in "Integrating with the ACS Server" section on page 5-2 have been completed. In addition, the steps described in this section must be followed to exercise secured views.

Create the Users in ACS

To create two users named Joe and Frank in ACS, follow these steps:

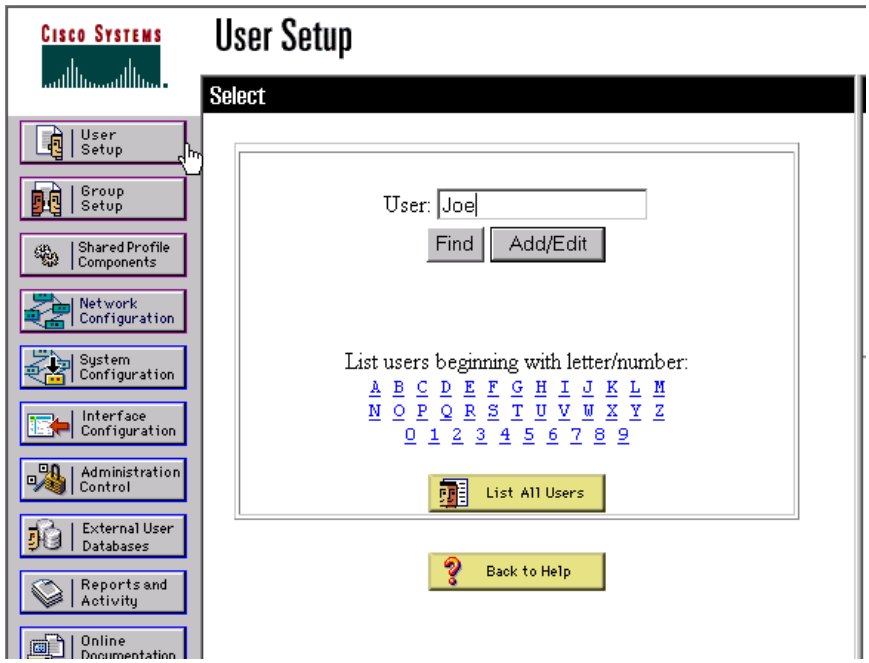
Step 1 Log in to the ACS server.

Step 2 Click **User Setup**.

The dialog box shown in Figure 5-8 appears.

a. Enter a username (in this example, "Joe"), then click **Add/Edit** (see Figure 5-8).

Figure 5-8 ACS User Setup



b. Assign a password to the user *Joe*.

c. Assign him to group named *Group1*, then click **Submit**.

d. Similarly, create a user called Frank and assign him to *Group2*.

Step 3 Set up the Network Device Groups to contain the following devices:

- D1 (192.168.137.65)
- D2 (192.168.137.69)

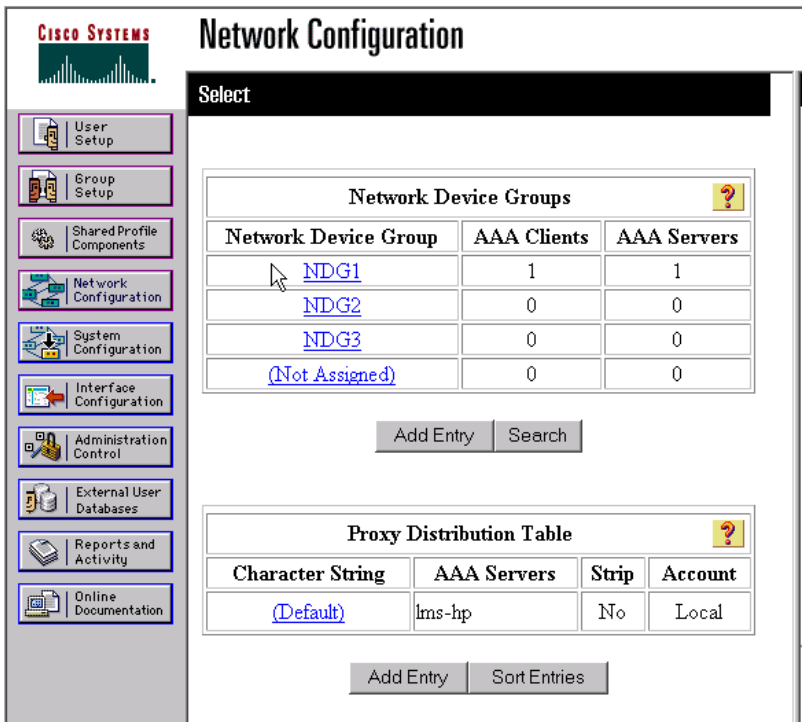
a. Click **Network Configuration**.

The Network Device Groups dialog is displayed.

b. Click **Add Entry**.

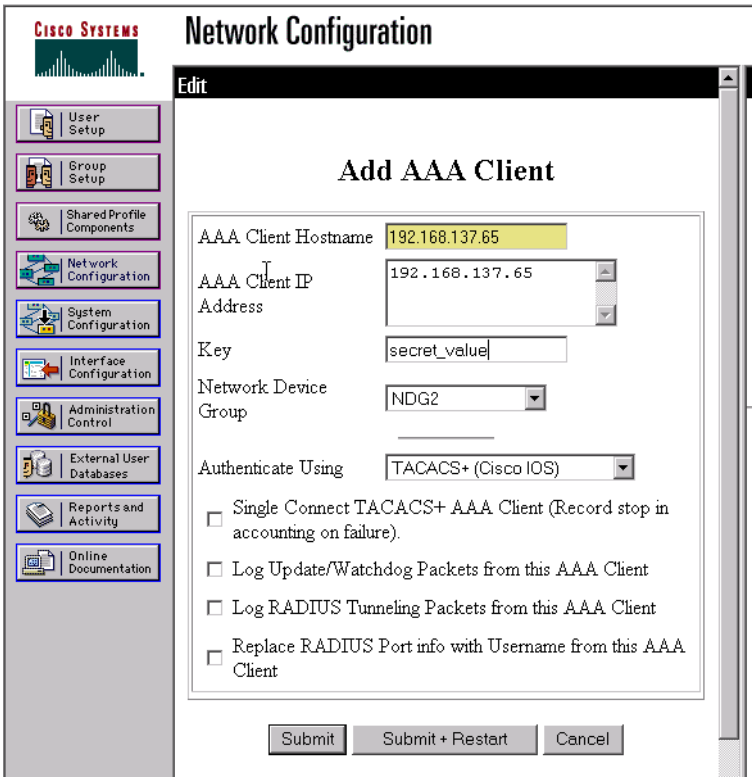
c. Create two Network Device Groups—*NDG2* and *NDG3*—as shown in Figure 5-9.

Figure 5-9 Creating New Network Device Groups



Step 4 Click the **NDG2** link and in the Add AAA Client dialog box, add a device **D1** with IP address: **192.168.137.65**.

Figure 5-10 Creating New Network Device Groups



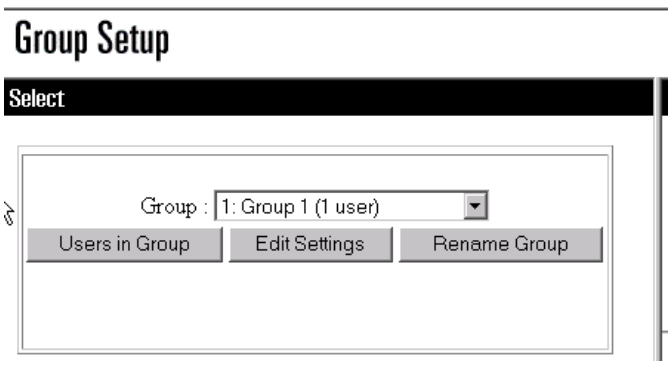
Step 5 Similarly, click on **NDG3** (see Figure 5-9 on page 5-8) and add a device **D2** with IP address: **92.168.137.69**.

Step 6 Assign User Groups a Network Administrator's role on Network Device Groups.

a. Assign *Group1* (Joe's user group) a Network Administrator's role on NDG2.

b. Click **Group Setup** (see Figure 5-11).

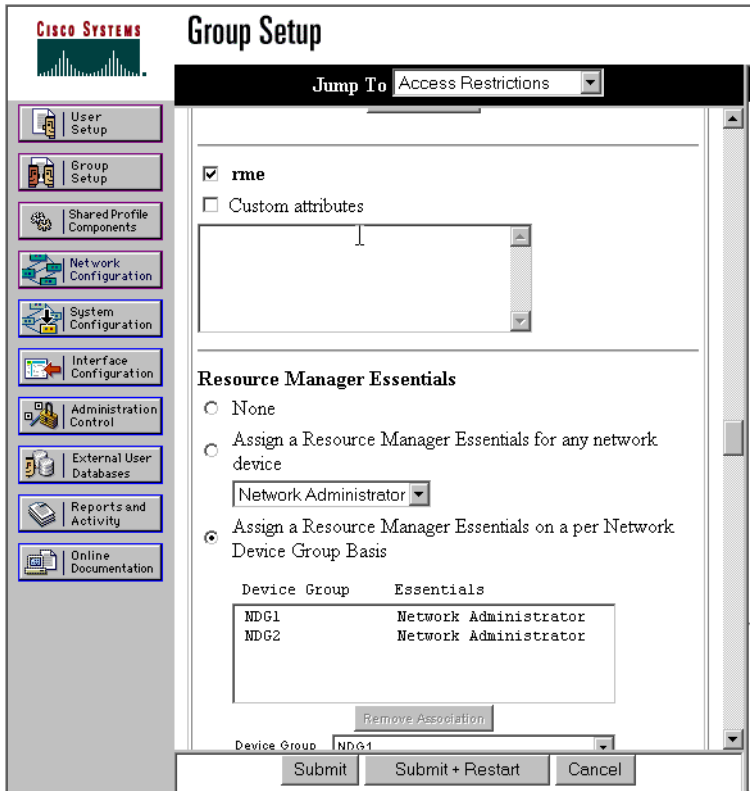
Figure 5-11 Creating New Network Device Groups



c. Select the group to which the user Joe belongs, then click **Edit Settings**.

Step 7 Create an association for this group with the Network Device Groups that contain the LMS Server (NDG1) and device D1 (NDG2) respectively (see Figure 5-12).

Figure 5-12 Creating An Association Between the LMS Server and a Device



Step 8 To update the settings, click **Submit+Restart**.

Step 9 In the same way, create the association for the group that contains the user Frank and Network Device Groups that contain the LMS Server (NDG1) and device D2 (NDG3) respectively.

Note In this example, a User Group is assigned a Network Administrator role for certain Network Device Groups in the RME application. This needs to be done for other applications as well.

Secured Views is now operational for users Joe and Frank.

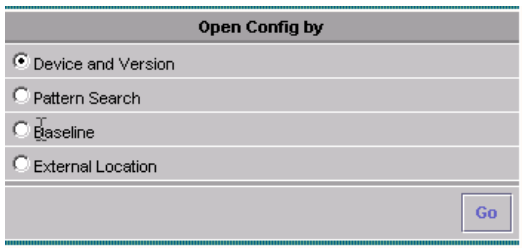
Step 10 Let's assume both Joe and Frank access the Config Editor screen:

a. Navigate to **RME** panel > **Config Management** > **Config Editor**.

b. Click **Config Files**.

c. Select the **Device and Version** option, then click **Go** (see Figure 5-13).

Figure 5-13 Open Config File by Device and Version



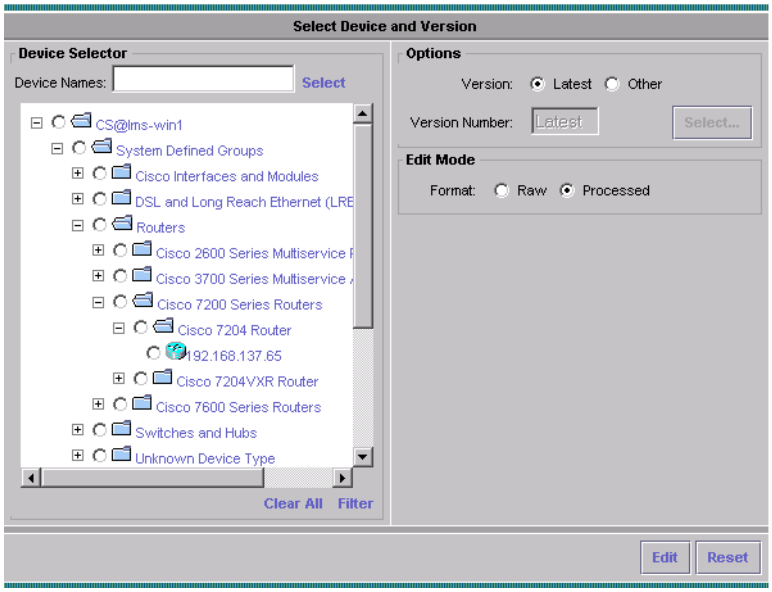
Assume group */CS@lms-sun1/System Defined Groups/ Routers/Cisco 7200 Series Routers/Cisco 7204 Router* contains two devices:

- 192.168.137.65
- 192.168.137.69

When the two users Joe and Frank access the same group in the Config Editor screen, they see different devices in the group.

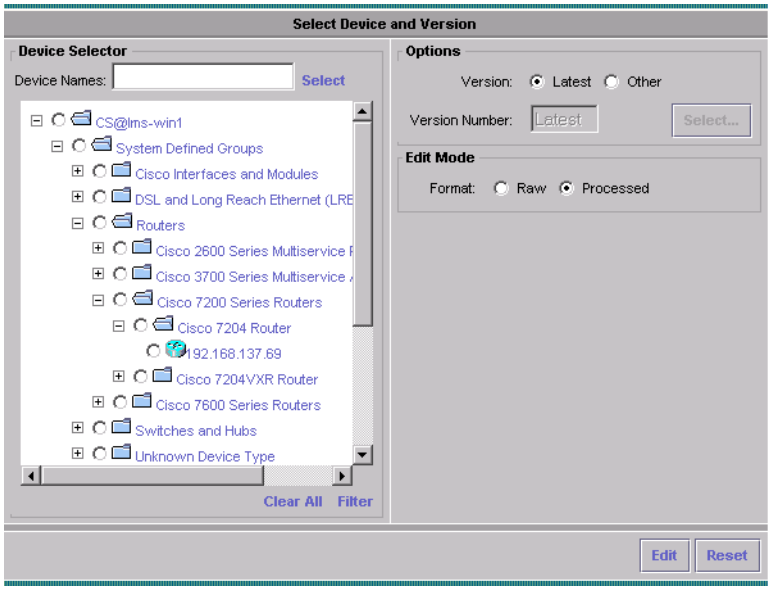
The view for Joe when he accesses the group */CS@lms-sun1/System Defined Groups/ Routers/ Cisco 7200 Series Routers/Cisco 7204 Router* will be as follows. He will see only the 192.168.137.65 device in it (as shown in Figure 5-14):

Figure 5-14 Joe's View of the Group



The following will be the view for Frank when he accesses the group */CS@lms-sun1/System Defined Groups/ Routers/ Cisco 7200 Series Routers/ Cisco 7204 Router*. He will see only the 192.168.137.69 device in it (as shown in Figure 5-15).

Figure 5-15 Frank's View of the Group



Why Do We Need to Create a New Role in ACS?

In ACS, the administrator can assign only one role for a user on a Network Device Group.

If a user requires privileges other than those associated with the current role, to operate on a Network Device Group, a custom role should be created. All necessary privileges to enable the user operate on the Network Device Group should be given to this role.

For example, if a user needs to have Approver and Network Operator privileges to operate on NDG1, you can create a new role with Network Operator and Approver privileges, and assign the role to the user so that he can operate on NDG1.

How to Create a New Role in ACS

To create a new role in ACS, follow these steps:

Step 1 Log in to the ACS server

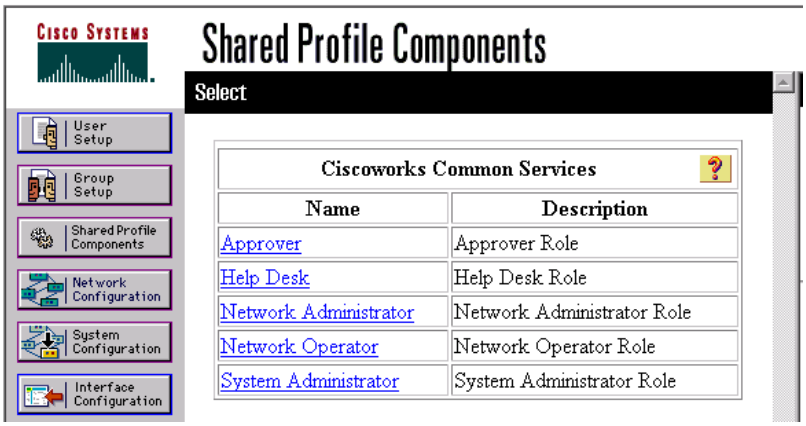
Step 2 Click **Shared Profile Components** (see Figure 5-16).

Figure 5-16 Shared Profile Components

Step 3 Choose the shared profile component (that is, the application in the CiscoWorks server) where you would like to create a new role.

In the example shown in Figure 5-17, **CiscoWorks Common Services** is selected.

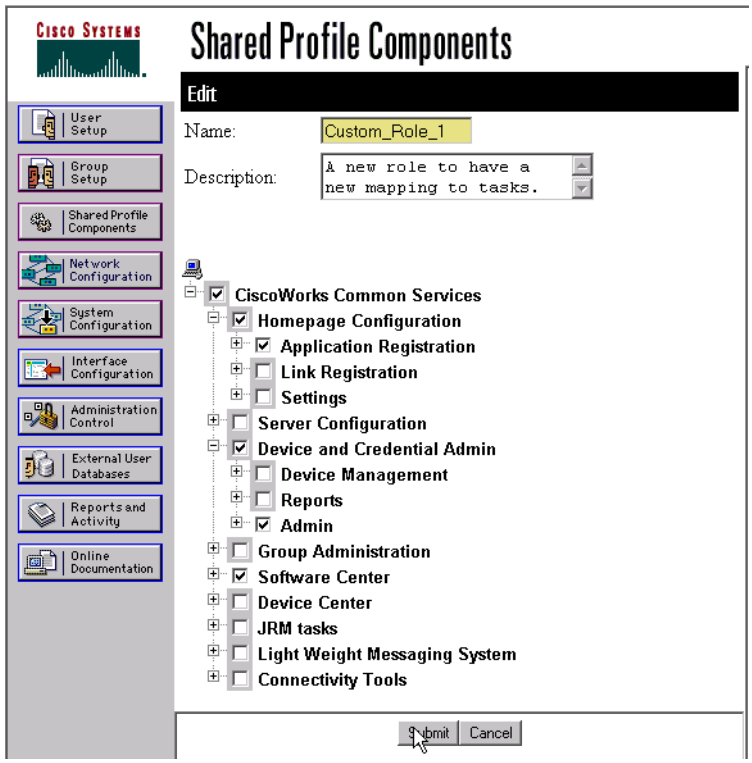
Figure 5-17 Selecting the CiscoWorks Application



Step 4 Click **Add**.

The following dialog box appears (see Figure 5-18

Figure 5-18 Defining the New Role



Step 5 Provide a new role name and description of the role to task mapping and select a list of tasks that the users of this role can perform.

Step 6 When satisfied with your settings, click **Submit**.

Accessing the CiscoWorks User Guides

This appendix describes how you can access the following CiscoWorks user guides:

- *CiscoWorks Common Services User Guide*
- *CiscoWorks Integration Utility User Guide*

Accessing the CiscoWorks Common Services User Guide

The *CiscoWorks Common Services User Guide* provides more in-depth information on all the topics discussed in this document.

You can access the *CiscoWorks Common Services User Guide* from both the CiscoWorks installation and the following URL.

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/usrguide/dcr.htm

To launch *CiscoWorks Common Services User Guide* from the CiscoWorks installation:

Step 1 Log in to CiscoWorks Home Page.

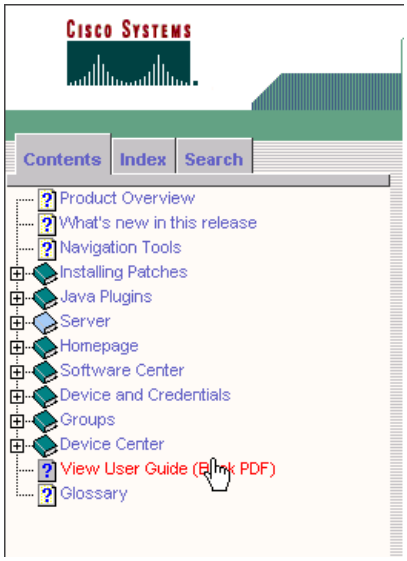
Step 2 From the Common Services Panel, choose **Server** > **Security**.

Step 3 Click the **Help** link in the top right-hand corner of the page.

The Server Overview Help page is displayed.

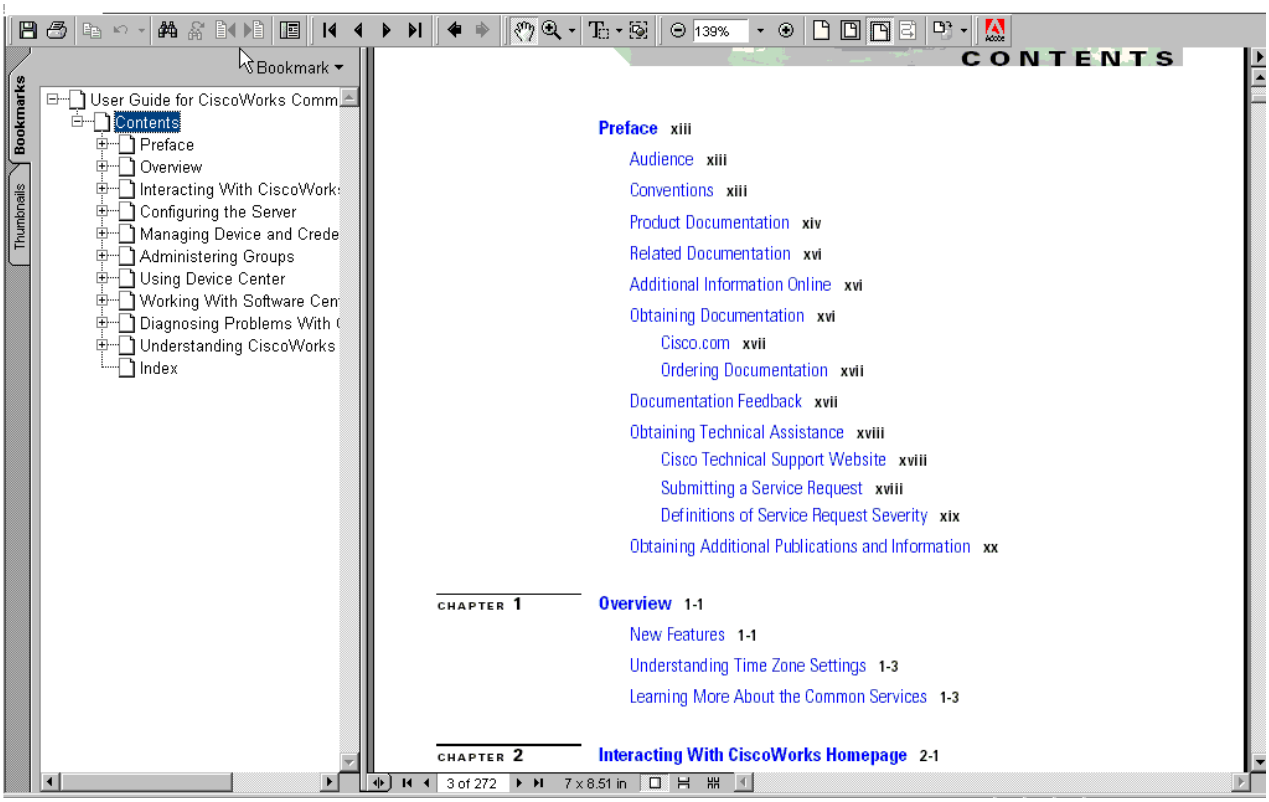
Step 4 In the Contents pane (on the left side of the page), choose **View User Guide** (as shown in Figure A-1).

Figure A-1



The *CiscoWorks Common Services User Guide* is displayed in a separate window as shown below. All the topics in the user guide are shown as links in the right frame.

Figure A-2 CiscoWorks Common Services User Guide Displayed



Accessing the CiscoWorks Integration Utility User Guide

To access the *CiscoWorks Integration Utility User Guide*, navigate to the following link:

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/nmim_ug/index.htm

A

AAA Authentication, authorization, and accounting (AAA) is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

accounting In the AAA framework, accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

ACS Access Control Server. Cisco Secure Access Control Server for Windows is AAA server software from Cisco Systems that provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications.

AUS Auto Update Server. The Auto Update server supports a pull model of configuration that can be used for the initial configuration, configuration updates, operating system updates and periodic configuration verification. The Auto Update server is ideal for remote PIX firewall network (including SOHO), remote sales agent, and educational networks. The Auto Update server also supports the management of remote firewalls that are dynamically addressed with DHCP or networks with intermittent connectivity.

authentication Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

authorization Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

C

cluster managed device SOHO or commercial devices that support the formation of a cluster such as the Cisco Catalyst 2900XL series or Cisco Catalyst 3750 series switches.

CDP The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all Cisco manufactured equipment, including routers, bridges, access servers, and switches. CDP Version-2 is the most recent release of the protocol and provides more intelligent device tracking features.

Certificate Setup This feature allows the creation of self-signed security certificates, which can be used to enable SSL connections between the client browser and management server.

Common Services Common Services provides an operating foundation that allows CiscoWorks applications to share data and system resources. It also provides a common desktop for launching CiscoWorks applications and centralizes login, user role definitions, and access privileges. Periodic updates to CiscoWorks Common Services 3.0 are made available for download.

CWHP CiscoWorks Home Page. A web page that a CiscoWorks user accesses after logging into a CiscoWorks server.

D

DCR Device and Credentials Repository (DCR) is part of Common Services and acts as a central secure repository for all the device and credential information. All applications within LMS request DCR for device credential information. Since there is a common device and credentials repository, devices populated in DCR can be automatically populated in different applications.

G

Groups user interface Any user interface in CiscoWorks in which groups are shown in a device selector window.

I

IOS Internetwork Operating System. It is an operating system that runs Cisco routers and switches. You use the command line interface to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

IP SLA Cisco IOS IP Service Level Agreement (SLA), a network performance measurement feature in Cisco IOS software, provides a scalable, cost-effective solution for service level monitoring. It eliminates the deployment of dedicated monitoring devices by including the operation capabilities in the routers.

L

LAN Management Solution (LMS) CiscoWorks LAN Management Solution (LMS) provides the integrated management tools needed to simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. It provides IT organizations an integrated system for sharing device information across management applications, automation of device management tasks, visibility into the health and capability of the network, and identification and localization of network trouble.

N

Network Device Grouping (NDG) In CiscoSecure Access Control Server, Network Device Grouping (NDG) is an advanced feature that allows you to view and administer a collection of network devices as a single logical group. To simplify administration, each group can be assigned a convenient name that can be used to refer to all devices within that group. This creates two levels of network devices within CiscoSecure ACS—single discrete devices such as an individual router, NAS, or PIX firewall, and an NDG; that is, a collection of routers or AAA servers.

NMIM Network Management Integration Module.

NMS Network Management System.

P

Peer Server Account Setup This feature helps you create users who can programmatically log in to CiscoWorks servers and perform certain tasks. These users should be set up to enable communication between multiple CiscoWorks servers.

Peer Server Certificate Setup You can add the certificate of another CiscoWorks server into its trusted store. This will allow one CiscoWorks Server to communicate to another. If a CiscoWorks server needs to communicate to another CiscoWorks server, it must possess the certificate of the other server. You can add certificates of any number of peer CiscoWorks servers to the trusted store.

Per-VLAN Spanning Tree + (PVST+) Per VLAN Spanning Tree Plus (PVST+) maintains a spanning tree instance for each VLAN configured in the network and allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST+ treats each VLAN as a separate network, it has the ability to load balance traffic (at Layer 2) by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop. It uses 802.1Q trunking technology rather than ISL. PVST+ is an enhancement to the 802.1Q specification and is not supported on non-Cisco devices.

pre-deployed device state The predeployed device state indicates that the devices are not reachable from the management server—either they are not in the network or sufficient credentials have not been provided.

R

RADIUS Remote Authentication Dial-In User Service. A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

RWAN CiscoWorks Routed WAN Management. This suite of solution applications provides increased visibility into network behavior and quickly identifies performance bottlenecks that can impact short and long-term performance trends. It also provides sophisticated configuration tools to optimize bandwidth and utilization across critical WAN links in the network.

S

Single Sign On (SSO) Single Sign On (SSO) helps the user to use a single session to navigate to multiple Cisco Works servers without having to authenticate to each of them. Communication between multiple Cisco Works servers is enabled by a trust model addressed by certificates and shared secrets.

SNMP Simple Network Management Protocol.

SNMS CiscoWorks Small Network Management Solution.

SSH Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities—slogin, SSH, and SCP—that are secure versions of the earlier UNIX utilities, rlogin, RSH, and RCP.

System Identity Setup Communication between multiple CiscoWorks servers is enabled by a trust model addressed by Certificates and shared secrets. For communication to occur in multi-server scenarios, System Identity setup should be used to create a “trust” user on slave and standard servers.

T

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ allows a separate access server (the TACACS+ server) to provide the services of authentication, authorization, and accounting independently. Each service can be tied into its own database or can use the other services available on that server or on the network. The overall design goal of TACACS+ is to define a standard method for managing dissimilar Network Access Servers from a single set of management services such as a database. A NAS provides connections to a single user, to a network, or subnetwork, and interconnected networks.

V

VMS CiscoWorks VPN/Security Management Solution. VMS contributes to organizational productivity by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, network intrusion detection systems, and host intrusion prevention systems. CiscoWorks VMS also includes network device inventory, change audit, and software distribution features.

A

B

C

D

E

G

H

I

M

N

P

R

S

U