



Managing Device and Credentials

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials, meant to be used by various network management applications. The Device and Credential Admin (DCA) provides an interface to administer DCR.

DCR helps multiple applications share device lists and credentials using a client-server mechanism, with secured storage and communications. The applications can read or retrieve the information. The applications can also update the information in DCR so that the updated information could be shared with other applications.

DCR provides:

- A central place where you can add or import new devices.
- Easier and faster access to device and credential data.
- Secure data persistence, access and transport.
- Rationalized and controlled replication, with less user-level data reconciliation.
- Better integration with third-party and Cisco network-management applications.

DCR also:

- Stores device attributes and credentials, permits dynamic creation of attribute types, and permits default grouping and filtering.
- Supports proxy device attributes, unreachable devices, and pre-provisioning of devices.
- Allows you to populate the repository via import from many sources, and to export device data for use with third-party network management systems such as HP Network Node Manager 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.

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.

Device attributes are unique to each device and they identify a device. The following attributes are stored in the repository:

Table 4-1 *Attributes and Description*

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 pre-provisioning devices. The value would be application specific.
display_name	Device name, as you want it to be represented in reports or graphical displays. Can be derived from Host Name, Management IP address or Device Identity.

Table 4-1 *Attributes and Description (continued)*

Attribute	Description
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.
DCR Device ID	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 Fields	DCA, by default, provides four user defined fields. These fields are used to store additional user-defined data for a device. You can add more User Defined fields.

The mandatory attributes are:

- Management IP address or Host Name or Device Identity.
- Display Name.

Individual applications interact with the repository to get the device list, device attributes, and device credentials.

The following credentials can be associated with a device in DCR:

Table 4-2 *Credentials and Description*

Credential	Description
Standard Credentials	
primary_username	Primary user name used to access the device.
primary_password	Password for the primary_username.

Table 4-2 **Credentials and Description (continued)**

Credential	Description
primary_enable_password	Console-enabled password for the device. Allows you to make configuration changes and provides access to a larger set of commands. Without the enable password, users are restricted to read-only operations.
snmp_v2_ro_comm_string	Device's SNMP V2 read-only community string.
snmp_v2_rw_comm_string	Device's SNMP V2 read/write community string.
snmp_v3_user_id	Device's SNMP V3 user ID.
snmp_v3_password	Device's SNMP V3 password.
snmp_v3_engine_ID	Device's SNMP V3 engine ID.
snmp_v3_auth_algorithm	SNMP V3 authorization algorithm used on the device. Can be MD5 or SHA-1.
http_username	Device's HTTP-interface user ID.
http_password	Device's HTTP-interface password.
Additional Credentials for Cluster Managed Devices	
dsbu_member_number	Number of the Cluster member. This number represents the order in which the device was added to the cluster.
parent_dsbu_id	DCR Device ID of the parent Cluster device.
Auto Update Server Specific Credentials	
aus_url	URL for the AUS device.
aus_port	Port number of the AUS service running on the AUS device.
aus_username	User login providing access to the AUS device.
aus_password	Password for the corresponding aus_username.
Auto Update Server Managed Device -Specific Credentials	
aus_username	User login providing access to the AUS-managed device.
aus_password	Password for the corresponding aus_username.
parent_aus_id	DCR Device ID of the managing AUS device.

DCR supports Cisco Cluster Management Suites, Auto Update Servers and the managed devices using a mix of standard and additional attributes and credentials.

- Clusters: All the attributes of the Cluster are the same as a normal DCR device.
- Cluster Members: Each cluster member has its own Host Name, sysObjectID, and MDF type, and uses the same Telnet credentials as the Cluster. Each cluster member has the following additional attributes:
 - Member Number: The number of the Cluster member. This number represents the order in which the device is added into the cluster.
 - Device ID of the parent Cluster record.
- Auto Update Server: The Auto Update Server has the following attributes and credentials:
 - URN
 - Username
 - Password
- Auto Update Server managed devices: Apart from having its own attributes and credentials like normal DCR devices in DCR, each Auto Update Server managed device has the following additional attributes:
 - Device Identity: The string value that uniquely identifies this device in the parent Auto Update Server.
 - The DCR Device ID of the parent Auto Update Server record.

DCR Architecture

The sharing of device list and credentials among various network management products is achieved through a Client-Server mechanism. The clients are network management applications that use DCR. The server is called the DCR Server.

DCR works based on a Master-Slave model. DCR Server can also be in Standalone mode.

Master DCR

The Master DCR server refers to the master repository of device list and credential data. The Master hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain which are running in Slave mode normally shares this list.

There is only one Master repository for each management domain, and it contains the most up-to-date device list and credentials.

Slave DCR

The Slave DCR refers to a repository that is an exact replica of the Master.

DCR Slaves are slave instance of DCR in other servers and provide transparent access to applications installed in those servers.

Any change to the repository data occurs first in the Master, and those changes are propagated to multiple Slaves. There can be more than one Slave in a management domain.

The Slave:

- Maintains an exact replica of the data managed by the Master for the management domain.
- Has a mechanism to keep itself in sync with the Master.
- Will first update Master and then update its own repository data. This is in case of repository data updates.

Standalone DCR

In Standalone mode, DCR maintains an independent repository of device list and credential data. It does not participate in a management domain and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other Master, Slave, or Standalone DCR.

DCR running in Master or Slave mode always has an associated DCR Group ID that indicates the Server's management domain. This Group ID is generated when a DCR is set to Master mode, and communicated to all Slaves later assigned to that Master.

Using the Device and Credential Admin

Device and Credential Admin (DCA) helps you in:

- [Managing Devices](#)
- [Generating Reports in DCA](#)
- [Managing Auto Update Servers](#)
- [Administering Device and Credential Repository](#)

Managing Devices

The Device Management option in DCA helps you manage the list of devices and their credentials. Device Management helps you in:

- [Adding Devices](#)
- [Deleting Devices](#)
- [Editing Device Credentials](#)
- [Importing Devices and Credentials](#)
- [Exporting Devices and Credentials](#)
- [Excluding Devices](#)
- [Viewing Devices List](#)

To perform any of these management functions, select:

Common Services > Device and Credentials > Device Management.

Adding Devices

You can use this feature to add devices, device properties or attributes, and device credentials to the DCA.

To add devices to the device list:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

The Device Management UI helps you perform operations on Standard Devices, Cluster Managed devices and Auto Update devices. Operations on Auto Update Servers can be performed only at the Auto Update Server Management UI.

The Device Summary window displays the devices and groups in DCA.

Step 2 Click **Add**.

The Device Properties page appears. The Device Information dialog box provides three device management types:

- [Standard Type](#)
 - [Auto Update Type](#)
 - [Cluster Managed Type](#)
-

Standard Type

You can add Routers, Switches, Hubs, and other devices using the Standard management type.

To add devices and credentials using Standard type:

-
- Step 1** Select the **Standard** radio button.
- Step 2** Enter the Device IP address, the host name, domain name, the device display name, and the device type in the corresponding fields.
- To select the Domain Name and the DeviceType, click **Select** and choose from the list.
- DCR uses a device record to represent a Cluster. A Cluster can be added in the Standard Management option by selecting the Device Type field as Cisco Cluster Management Suite.
- DSBU Clusters added this way, can then be selected in [Cluster Managed Type](#), for the field Cluster.
- Step 3** 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 4** Click **Next**.
- The Standard Credentials page appears.
- Step 5** Enter the credentials in the Add Credential Template. The following credentials can be added:
- Primary Credentials (Username, Password, Enable Password)
 - SNMP v2C credentials (Read-Only Community String, Read-Write Community String)
 - SNMPv3 Credentials (Username, Password, authentication Algorithm, Engine ID)
 - Rx Boot Mode Credentials (Username, Password)

Step 6 Click **Next**.

The Standard UDF dialog box appears.

Step 7 Enter your choices for User Defined Fields and click **Finish**.

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.

The attribute fields that appear here can be changed at **Device and Credentials > Admin > User Defined Fields**.

Auto Update Type

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 devices and credentials using Auto Update type:

Step 1 Select the **Auto Update** radio button.

Step 2 Enter the Device Type, Display Name, Auto Update Device ID, Host Name, Domain Name, and IP address in the corresponding fields.

To select Auto Update Server, Domain Name, and the Device Type click **Select** and select from the resulting popup windows. For Auto Update Server managed devices, Display Name and Device-Identity are enough for identity.

DCR uses a device record to represent an Auto Update Server. An Auto Update Server can be added in the Auto Update Server Management UI. Auto Update Server added this way can then be selected for the field Auto Update Server.

Step 3 Click **Add to List**.

The device gets 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 4 Click **Next**.

The Credential Template dialog box appears.

Step 5 Enter the Auto Update Server managed device credentials (Username, Password) in the corresponding fields and click **Next**.

The User Defined Fields dialog box appears.

Step 6 Enter your selections for User-defined fields and click **Finish**.

You can define four attribute fields for a device. These fields are used to store additional user-defined data for a device.

The attribute fields that appear here can be changed at **Device and Credentials > Admin > User Defined Fields**.

Cluster Managed Type

DCR supports Cisco Clusters and their member devices using a mix of standard and additional attributes and credentials.

To add devices and credentials using Cluster Managed type:

Step 1 Select the **Cluster Managed** radio button.**Step 2** Enter Device Type, Display Name, Device IP address, Device Host Name, Domain Name, Cluster, and Member Number in the corresponding fields. For member devices, member number and display name are enough for identity.

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.

Also, Cluster needs to 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 3 Click **Add to List**.

The device is added to the Added Device List in the window.

To remove a device from the Device List select the device and click **Remove from List**.

Step 4 Click **Next**.

The Cluster Manager credentials dialog box appears.

Step 5 Enter the device credentials in the corresponding fields and click **Next**.

The User Defined Field dialog box appears.

Step 6 Enter your selections for User-defined fields and click **Finish**.

You can define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

The attribute fields that appear here can be changed at **Device and Credentials > Admin > User Defined Fields**.

Deleting Devices

You can delete device information from DCR using this feature.

When a device is deleted, it will also get deleted in all the applications that use DCR.

To delete devices:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

Step 2 Select the device from the Device Summary dialog box and click **Delete**.

The device is removed from the device list. Also, all information about the selected device will be removed from DCR.

Editing Device Credentials

You can edit device information using this feature.

To edit device information:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

Step 2 Select one or more devices from the Device Summary List and click **Edit**.

The Device Properties page displays the Devices Information dialog box.

You can edit the attributes of individual devices here. The Devices column lists all the selected devices.

From the Devices column, you should separately select each device that needs to be edited, and make the required changes.

Step 3 Select the device for which you want to edit the device information, from the device list.

The current attributes are automatically populated in the device information fields.

Step 4 Edit the device information, on the right pane.

If you are done with your editing and do not want to proceed, click **Finish**.

Step 5 Click **Next**, if you want to edit device credentials.

The Credential Template dialog box appears. According to your requirement, you can edit:

- Primary Credentials (Username, Password, Enable Password)
- SNMP v2C credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Username, Password, authentication Algorithm, Engine ID)
- Rx Boot Mode Credentials (Username, Password)
- Auto Update Server Managed Device credentials (Username, Password)

Any changes made here will apply to all devices selected in Step 2. This has one exception.

If in [Step 2](#), devices belonging to different device management types are selected, the changes made will apply only to devices of the appropriate type. That is, if a standard-device credential is changed, only the standard devices selected in [Step 2](#) are affected.

If you have completed editing, and do not want to proceed, click **Finish**.

Step 6 Click **Next**, if you want to edit User Defined Fields.

The User Defined Fields dialog box appears. Make the required changes in the user-defined fields, and click **Finish**.

The changes made here will apply to all devices selected in [Step 2](#) (irrespective of the device management type).

Auto Update Servers cannot be edited here. Even if they are selected in [Step 2](#), they will not be affected. See [“Editing Auto Update Server” section on page 4-25](#) for details on editing Auto Update Server information.

Also, you cannot change the device management type using the edit flow. That is, a standard device cannot be changed to a Cluster device.

Importing Devices and Credentials

You can import device lists, device properties or attributes and device credentials to the DCR and populate DCR using this feature. You can:

- [Import Using DCA Interface](#)
- or
- [Import Using CLI](#)

Import Using DCA Interface

To import devices using DCA Interface:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

Step 2 Click **Bulk Import**.

The Import Devices popup window appears. You can import from any of the following:

- File
 - Local NMS (Network Management Station)
 - Remote NMS
-

Importing From a File

To import from a file:

Step 1 Enter the file name.

Or,

Browse the file system and select the file using the Browse tab.

Step 2 Select CSV or XML file formats, as required.

Only CSV2.0 and CSV3.0 file formats are supported.

Step 3 Select either **Use data from Import source** or **Use data from DCR**, to resolve conflicts during import.

- If you select **Use data from Import source**, the credentials from the import source will be used, and credentials for the device in DCR will be modified.
- If you select **Use data from DCR**, the device credentials in DCR will be used.

- Step 4** Schedule the task. To do this:
- a. Select the RunType from the drop-down list.
You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance.
 - b. Select the date from the date picker.
- Step 5** Enter the Job description in the Job Info field.
- Step 6** Click **Import**.
-

Importing From Local NMS

To import from Local NMS:

-
- Step 1** Select the Network Management System type from the NMS type drop-down list. HPOV6.x and Netview7.x are supported.
- Step 2** Enter the install location in the Install Location field.
- Step 3** Select either **Use data from Import source** or **Use data from DCR**, to resolve conflicts during import.
- Step 4** Schedule the task. To do this:
- a. Select the RunType from the drop-down list.
You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance.
 - b. Select the date from the date picker.
- Step 5** Enter the Job description in the Job Info field.
- Step 6** Click **Import**.
-

Importing From Remote NMS

You should have permissions to log into the remote network management system (NMS), without a password. Common Services uses remote login to log into the Server and get device details.

The rhosts file should be modified to enable you to login without a password.

To import from a remote NMS:

-
- Step 1** Select the Network Management System type from the NMS type drop-down list. If you select ACS, enter:
- ACS Server Name or IP address in the Host Name field.
 - ACS admin user name in the User Name field.
 - ACS admin user password in the Password field.
 - Port number (default is 2002) in the Port field.
- Step 2** Select the Operating System type from the OS type drop-down list.
- Step 3** Enter the Host name, User name, and Install location in the corresponding fields.
- Step 4** Select either **Use data from Import source** or **Use data from DCR**, to resolve conflicts during import.
- Step 5** Schedule the task. To do this:
- a. Select the RunType from the drop-down list.
You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance.
 - b. Select the date from the date picker.
- Step 6** Enter the Job description in the Job Information field.
- Step 7** Click **Import**.
-

Exporting Devices and 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.

You can edit the Export Format file located at *NMSROOT\objects\dcrimpexp\conf\Export_Format_CSV.xml* or *Export_Format_XML.xml* to specify the credentials you need to export.

To see the list of attributes that can be exported:

Step 1 At the command prompt, enter *NMSROOT/bin/dcrcli -u username*.

Step 2 Enter the password corresponding to the user name.

Step 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.

You can:

- [Export Using DCA Interface](#)
- or
- [Export Using CLI](#)

Export Using DCA Interface

To export device credentials using DCA Interface:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

Step 2 Click **Export**.

The Device Export dialog box appears.

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.

We recommend that you use this option to export up to a maximum of 1000 devices.

Selecting From Device Selector

To select from device selector:

Step 1 Enter the output file name.

Or

Browse the file system and select the file using the Browse tab.

Step 2 Select CSV or XML file formats, as required.

- Step 3** From the Device Selector, select the devices for which you need to export credentials.
- Step 4** Schedule the task. To do this:
- a. Select the RunType from the drop-down list.
You can schedule export immediately or schedule the export for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance.
 - b. Select the date from the date picker.
- Step 5** Enter the Job description in the Job Info field.
- Step 6** Click **OK**.
-

Getting Device List From File

To get device list from file:

-
- Step 1** In the Input File Selection panel, enter the input file name or select the input file (in CSV format) to get device list from, using the Browse tab.
- Step 2** In the Output File Information panel, enter the location for the output file or click Browse to select the file you require.
- Step 3** Select CSV or XML file formats radio buttons, as required.
- Step 4** Schedule the task. To do this:
- a. Select the RunType from the drop-down list.
You can schedule export immediately or schedule the export for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance.
 - b. Select the date from the date picker.
- Step 5** Enter the Job description in the Job Info field.
- Step 6** Click **OK**.
- You must populate DCR with devices before you export credentials from DCR selecting devices from a file.
-

Excluding Devices

This feature allows you to specify a file that contains the list of the devices that should not be added to DCR using the Add or Import operations.

During Add or Import operations, DCR makes sure that the device being added or imported is not listed in the Exclude Device List.

A device can be excluded based on its hostname+domainname, IP address and device-identity fields.

To exclude devices from Add or Import operations:

-
- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.
- The Device Management page appears.
- Step 2** Click **Exclude**.
- The Upload Exclude Devices File dialog box appears.
- Step 3** Enter the file name or click **Browse** to browse the file system and select the file.
- The file that needs to be uploaded must be in CSV format.
- Step 4** Click **Apply** to upload the file.
-

A Sample CSV Exclude File

```
; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV;
Version=3.0
;
;Start of section 0 - Basic Credentials
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,primary_username,primary_password,primary_enable_password
;
,Dev1Hostname,,
10.1.1.0.60,,,

```

```
,,,AUSID1
,Dev2Hostname,cisco.com,
;
;Start of section 2 - AUS managed;
;HEADER: aus_device_identity,parent_aus_id
;
;
;End of CSV file
```

Viewing Devices List

You can view the devices in the Device List Report using this feature.

To view devices in the Device List Report:

-
- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Device Management**.
The Device Management page appears.
 - Step 2** Select the devices you want from the Device Summary list and Click **View**.
The Device List Report dialog box appears.
 - Step 3** Select the device.
 - Step 4** Click **View**.
-

Generating Reports in DCA

You can use this feature to generate and view Device and Credential Admin reports.

To generate reports:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Reports**.

The Report Generator page appears.

Step 2 Select a report from the DCA Reports tree on the left panel to view a short description, summary, or parameters of the report.

You can select any of the following reports:

- DCA Device List Report—Displays the complete device list in DCA.
- DCA Audit Report—Displays the complete device list in DCA within a specified period of time.
- Excluded Devices Report—Displays the excluded devices list.
- Import Status Report—Displays the last imported device list.
- DCA devices that are not configured in ACS report—Displays the list of DCA devices that need to be configured in ACS.

Step 3 Select the report link in the Available Report pane and click **Generate Reports** to view the selected report.

You can export the report, or print the report.

To export the report:

Step 1 Click the Export Current Report button on top of the right hand side of the DCA Report list.

Step 2 Select the required radio button to export the report either in pdf or in CSV format.

Step 3 Enter the number of rows to be exported and click **OK**.

Managing Auto Update Servers

Auto Update Servers have the following credentials:

- Auto Update Server URL
- Username
- Password

Auto Update Server management feature helps you in:

- [Adding Auto Update Server](#)
- [Editing Auto Update Server](#)
- [Deleting Auto Update Server](#)

Adding Auto Update Server

To add Auto Update Server:

Step 1 In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Auto Update Server Management**.

The Auto Update Server Management page appears.

Step 2 Click **Add**.

The Auto Update Server dialog box appears.

Step 3 Enter the Display Name, IP address, Host, Port, URN, User name, and password in the corresponding fields. Re-enter the password in the Verify field.

DCR uses a device record to represent a Auto Update Server.

An Auto Update Server added in the Auto Update Server Management UI can be selected for the field Auto Update Server when you add devices using the Auto Update management type.

Step 4 Click **OK**.

Editing Auto Update Server

To edit Auto Update Server:

-
- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Auto Update Server Management**.
The Auto Update Server Management page appears.
- Step 2** Select the device you want to edit from the list and click **Edit**.
The Auto Update Server dialog box appears.
- Step 3** Edit Display Name, IP address, Port, URN, User name, and Password fields.
- Step 4** Click **OK**.
-

Deleting Auto Update Server

To delete Auto Update Servers:

-
- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Auto Update Server Management**.
The Auto Update Server Management page appears.
- Step 2** Select the device you want to delete from the list.
- Step 3** Click **Delete**.
-

Administering Device and Credential Repository

The DCA Admin feature allows you to do the following tasks:

- [Changing DCR Mode](#)
- [Adding User-defined Fields](#)
- [Renaming User-defined Fields](#)
- [Deleting User-defined Fields](#)

To perform these tasks, select **CiscoWorks Homepage > Device and Credentials > Admin**. The Admin page appears with the current DCA settings.

You can change the Mode Settings or modify User Defined fields.

Changing DCR Mode

To change Mode Settings:

Step 1 In the CiscoWorks Homepage, select **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 Click **Change Mode** to change the current mode.

The DCR Mode dialog box appears. You can select the required mode from this dialog box.

- [Changing the Mode to Standalone](#)
 - [Changing the Mode to Master](#)
 - [Changing the Mode to Slave](#)
-

Master-Slave Configuration Prerequisites

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

If machine M is to be the Master and S is to be the Slave:

-
- Step 1** In M add a Peer Server User and password.
See [“Setting up Peer Server Account” section on page 3-18](#) for details.
- Step 2** In S add a System Identity user and password. This should be same as the Peer Server User set up in M.
See [“Setting up System Identity Account” section on page 3-21](#), for details.
- Step 3** Copy the Self-Signed Certificate of S to M. Also, copy the Self-Signed Certificate of M to S.
See [“Creating Self Signed Certificate” section on page 3-9](#), for details on creating Self-Signed Certificate.
See [“Setting up Peer Server Certificate” section on page 3-22](#), for details on copying Peer Certificate.
- Step 4** Now configure S as Slave and M as Master.
-

Changing the Mode to Standalone

-
- Step 1** Select the **Standalone** radio button.
- Step 2** Click **Apply** to change mode.
The default DCR mode is Standalone.
-

Changing the Mode to Master

Before you change the mode to Slave, ensure that [Master-Slave Configuration Prerequisites](#) are in place.

-
- Step 1** Select the **Master** radio button.
- Step 2** Click **Apply** to change mode.
-

Changing the Mode to Slave

Before you change the mode to Slave, ensure that [Master-Slave Configuration Prerequisites](#) are in place.

You need to perform the following tasks:

-
- 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's Self Signed Certificate.

- Step 3** Specify the SSL port of the master. 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 Slave will be added to the new Master. However, any duplicates will be discarded.
- Step 4** Click **Apply**.
-

Changing the hostname of a Master

Changing the hostname of a Master is equivalent to pointing Slaves to a new Master.

When you point a Slave/Standalone to a new Master, DCR checks whether the new Master has the same Domain ID as the current machine.

If Domain ID is the same, DCR displays an error message saying that Master cannot be configured since the new Master has the same Domain ID.

In this case, you need to convert the Slave to Standalone, and then register the machine with the new Master.

On re-registration, the applications on Slave will clean up the device list.

When you change the host name of the current Master, you need to change the Slave's mode to Standalone, and then re-register the machine as a Slave by providing the new Master hostname. However, when the machine is re-configured as Slave, the applications will clean up the device list.

Let us say we have a Master M and Slave S. If M's hostname is changed, the Slave S has to be made standalone. Then it has to be re-configured as Slave of M. But when S is re-configured as Slave, the applications on S will clean up their device lists.

Therefore, you have to be aware of the fact that while changing the hostname of a Master, an application data is cleaned up on all Slaves.

Adding User-defined Fields

To add a user defined field:

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

The Admin page appears with the current settings.

Step 2 Click the **User-defined Fields** link.

The User-defined Fields page appears.

Step 3 Click **Add** to add a User-defined field.

- Step 4** Enter the field label and description in the corresponding fields.
 - Step 5** Click **Apply** to add the User-defined Field.
-

Renaming User-defined Fields

To rename a user-defined field:

- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Admin**.
The Admin page appears with the current DCA settings.
 - Step 2** Click **User-defined Fields** link.
The User-defined Field dialog box appears.
 - Step 3** Select the radio button corresponding to the User-defined Field you want to rename.
 - Step 4** Click **Rename**.
The User-defined Field dialog box appears.
 - Step 5** Enter the field label and description in the corresponding fields.
 - Step 6** Click **Apply**.
-

Deleting User-defined Fields

To delete a user-defined field:

-
- Step 1** In the CiscoWorks Homepage, select **Common Services > Device and Credentials > Admin**.
The Admin page appears with the current DCA settings.
 - Step 2** Click the **User-defined Fields** link in the TOC.
The User-defined Fields dialog box appears.
 - Step 3** Select a User-defined Field, then click **Delete**.
-

Sample CSV File

CSV 2.0 or CSV 3.0 file formats are supported for import.

A Sample CSV 2.0 File

```
;
; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0;
Type = Csv
;
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 19 are optional.
; Col# = 1: Name (including domain or simply an IP)
; Col# = 2: RO community string
; Col# = 3: RW community string
; Col# = 4: Serial Number
; Col# = 5: User Field 1
; Col# = 6: User Field 2
; Col# = 7: User Field 3
; Col# = 8: User Field 4
; Col# = 9; Name = Telnet password
; Col# = 10; Name = Enable password
```

```

; Col# = 11; Name = Enable secret
; Col# = 12; Name = Tacacs user
; Col# = 13; Name = Tacacs password
; Col# = 14; Name = Tacacs enable user
; Col# = 15; Name = Tacacs enable password
; Col# = 16; Name = Local user
; Col# = 17; Name = Local password
; Col# = 18; Name = Rcp user
; Col# = 19; Name = Rcp password
;
; Here are the rows of data.
;
172.20.118.156,public,,FHH080600dg,,,,,,,,,,,,,
172.20.118.150,public,,FHH0743W022,,,,,,,,,,,,,

```

A Sample CSV 3.0 File

```

; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCsv;
Version=3.0
;
;Start of section 0 - Basic Credentials
;
;HEADER:
management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,user_defined_field_0,user_defined_field_1
;
10.77.202.40,Switch6009,cisco.com,,Switch2,1.3.6.1.4.1.9.1.281,0,268438100,public,private,field0,field1
10.77.202.10,Router7000,cisco.com,,Router1,1.3.6.1.4.1.9.1.8,0,278464493,public,private,field0,field1
10.77.202.30,Switch4006,cisco.com,,Switch1,1.3.6.1.4.1.9.5.46,0,268438086,public,private,field0,field1
10.77.202.20,Router6400,cisco.com,,Router2,1.3.6.1.4.1.9.1.180,0,269214543,public,private,field0,field1

;End of CSV file

```



Note

For a complete list of attributes and their description, use the `lsattr` command in `dcrcli`. See [“Listing the Attributes” section on page 4-40](#) for usage details.

Sample CSV 3.0 File for Auto Update Server Managed Devices

```

; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCsv;
Version=3.0
;
;Start of section 0 - Basic Credentials
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,
sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw
_comm_string,
snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,
snmp_v3_auth_algorithm,primary_username,primary_password,primary_enable_password
;
1.1.1.1,ons_host1,cisco.com,AUS_ID,ONS1,1.3.6.1.4.1.9.1.406,0,27361289
2,,,,,,,,,
10.10.10.1,aus_server,cisco.com,,AUS_SERV1,UNKNOWN,3,UNKNOWN,,,,,,,,,
;
;Start of section 1 - AUS proxy
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,aus_username,aus_password,aus_url
;
1.1.1.1,ons_host1,cisco.com,AUS_ID,ONS1,admin,admin,
10.10.10.1,aus_server,cisco.com,,AUS_SERV1,admin,admin,autoupdate/Auto
UpdateServlet
;
;Start of section 2 - AUS managed
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,parent_aus_id
;
1.1.1.1,ons_host1,cisco.com,AUS_ID,ONS1,display_name=AUS_SERV1
;End of CSV file

```

Sample CSV 3.0 File for Cluster Managed Devices

```

; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV;
Version=3.0
;
;Start of section 0 - Basic Credentials
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,
sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw
_comm_string,
snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,primary_username,
primary_password,primary_enable_password
;
1.1.1.1,ons_dev_1,cisco.com,,ONS1,1.3.6.1.4.1.9.1.406,0,273612892,,,,,
,,,,
10.10.10.1,host1,cisco.com,,cluster1,Unknown,1,278283831,,,,,,,,,
;
;Start of section 3 - DSBU managed
;
;HEADER:
management_ip_address,host_name, domain_name,device_identity,display_name,
dsbu_member_number,parent_dsbu_id
;
1.1.1.1,ons_dev_1,cisco.com,,ONS1,1,display_name=cluster
;End of CSV file

```

Mapping CSV 2.0 to CSV 3.0 Fields

The following table provides a mapping between the fields in CSV 2.0 and CSV 3.0:

CSV 2.0	CSV 3.0
Name (including domain or simply an IP)	host_name and display_name
RO community string	snmp_v2_ro_comm_string
RW community string	snmp_v2_rw_comm_string
Serial Number	Not used in CSV 3.0
User Field 1	user_defined_field_0
User Field 2	user_defined_field_1
User Field 3	user_defined_field_2
User Field 4	user_defined_field_3
Telnet password	primary_password
Enable password	primary_enable_password
Enable secret	primary_enable_password
Tacacs user	primary_username
Tacacs password	primary_password
Tacacs enable user	Not used in CSV 3.0
Tacacs enable password	primary_enable_password
Local user	primary_username
Local password	primary_password
Rcp user	Not used in CSV 3.0
Rcp password	Not used in CSV 3.0

Telnet password, Tacacs password, and Local password are matched to primary_password.

The Enable password, Enable secret, and Tacacs enable password are matched to primary_enable_password.

The Tacacs user and Local user are matched to primary_username.

The order of preference used to set these values in CSV 3.0:

- If Tacacs username, password, enable password are set, then these values will be set as primary_username, primary_password and primary_enable_password.
- If Local username and password are set, then the values will be set as primary_username and primary_password.
- If Telnet password, Enable Password, and Enable Secret are set, then the values will be set as primary_password, and primary_enable_password (for both Enable Password, and Enable Secret).

Sample XML File

Sample XML File (Standard)

```
<?xml version="1.0"?>
<DEVICES>
  <DEVICE>
    <SET Name="Basic Credentials">
      <DEVATTRIB
Name="management_ip_address">10.77.202.40</DEVATTRIB>
      <DEVATTRIB Name="host_name">Switch6009</DEVATTRIB>
      <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
      <DEVATTRIB Name="display_name">Switch2</DEVATTRIB>
      <DEVATTRIB
Name="sysObjectID">1.3.6.1.4.1.9.1.281</DEVATTRIB>
      <DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
      <DEVATTRIB Name="mdf_type">268438100</DEVATTRIB>
      <DEVATTRIB Name="snmp_v2_ro_comm_string">public</DEVATTRIB>
      <DEVATTRIB
Name="snmp_v2_rw_comm_string">private</DEVATTRIB>
      <DEVATTRIB Name="primary_username">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_password">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_enable_password">lab</DEVATTRIB>
    </SET>
  </DEVICE>
</DEVICES>
```

**Note**

For a complete list of attributes and their description, use the `lsattr` command in `dcrcli`. See [“Listing the Attributes”](#) section on page 4-40 for usage details. Also, see [Attributes and Description](#) and [Credentials and Description](#).

Sample XML File for Auto Update Server Managed Devices

```
<?xml version="1.0"?>
<DEVICES>
  <DEVICE>
    <SET Name="Basic Credentials">
      <DEVATTRIB
Name="management_ip_address">1.1.1.1</DEVATTRIB>
      <DEVATTRIB Name="host_name">ons_host1</DEVATTRIB>
      <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
      <DEVATTRIB Name="device_identity">AUS_ID</DEVATTRIB>
      <DEVATTRIB Name="display_name">ONS1</DEVATTRIB>
      <DEVATTRIB
Name="sysObjectID">1.3.6.1.4.1.9.1.406</DEVATTRIB>
      <DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
      <DEVATTRIB Name="mdf_type">273612892</DEVATTRIB>
    </SET>
    <SET Name="AUS proxy">
      <DEVATTRIB Name="aus_username">admin</DEVATTRIB>
      <DEVATTRIB Name="aus_password">admin</DEVATTRIB>
    </SET>
    <SET Name="AUS managed">
      <DEVATTRIB Name="device_identity">AUS_ID</DEVATTRIB>
      <DEVATTRIB
Name="parent_aus_id">display_name=AUS_SERV1</DEVATTRIB>
    </SET>
  </DEVICE>
  <DEVICE>
    <SET Name="Basic Credentials">
      <DEVATTRIB
Name="management_ip_address">10.10.10.1</DEVATTRIB>
      <DEVATTRIB Name="host_name">aus_server</DEVATTRIB>
      <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
      <DEVATTRIB Name="display_name">AUS_SERV1</DEVATTRIB>
      <DEVATTRIB Name="sysObjectID">UNKNOWN</DEVATTRIB>
      <DEVATTRIB Name="dcr_device_type">3</DEVATTRIB>
      <DEVATTRIB Name="mdf_type">UNKNOWN</DEVATTRIB>
    </SET>
    <SET Name="AUS proxy">
      <DEVATTRIB Name="aus_username">admin</DEVATTRIB>
```

```

        <DEVATTRIB Name="aus_password">admin</DEVATTRIB>
    <DEVATTRIB
Name="aus_url">autoupdate/AutoUpdateServlet</DEVATTRIB>
    </SET>
</DEVICE>
</DEVICES>

```

Sample XML File for Cluster Managed Devices

```

<?xml version="1.0"?>
<DEVICES>
    <DEVICE>
        <SET Name="Basic Credentials">
            <DEVATTRIB
Name="management_ip_address">1.1.1.1</DEVATTRIB>
            <DEVATTRIB Name="host_name">ons_dev_1</DEVATTRIB>
            <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
            <DEVATTRIB Name="display_name">ONS1</DEVATTRIB>
            <DEVATTRIB
Name="sysObjectID">1.3.6.1.4.1.9.1.406</DEVATTRIB>
            <DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
            <DEVATTRIB Name="mdf_type">273612892</DEVATTRIB>
        </SET>
        <SET Name="DSBU managed">
            <DEVATTRIB Name="dsbu_member_number">1</DEVATTRIB>
            <DEVATTRIB
Name="parent_dsbu_id">display_name=cluster1</DEVATTRIB>
        </SET>
    </DEVICE>
    <DEVICE>
        <SET Name="Basic Credentials">
            <DEVATTRIB
Name="management_ip_address">10.10.10.1</DEVATTRIB>
            <DEVATTRIB Name="host_name">host1</DEVATTRIB>
            <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
            <DEVATTRIB Name="display_name">cluster1</DEVATTRIB>
            <DEVATTRIB Name="sysObjectID">Unknown</DEVATTRIB>
            <DEVATTRIB Name="dcr_device_type">1</DEVATTRIB>
            <DEVATTRIB Name="mdf_type">278283831</DEVATTRIB>
        </SET>
    </DEVICE>
</DEVICES>

```

Using DCR Features Through CLI

Using Command Line Interface, you can add, delete, and modify devices, and change the DCR modes. You can also view the list of attributes that can be stored in DCR, and view the current DCR mode. The `dcrcli` utility provided with Common Services helps you perform these tasks using CLI.

Adding Devices Using `dcrcli`

To add devices using `dcrcli`:

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

Step 2 Enter the password corresponding to the username

Step 3 Enter `add ip=value hn=value di=value dn=value -a attname=value`

Enter either the IP address (ip), Hostname (hn), or Device Identity (di).

Enter the Display Name (dn) and the Attribute name (-a attname). The attribute `sysObjectID` is mandatory. You can add multiple attributes. For example,

```
add ip=1.1.1.1 hn=device1 dn=cisco.com
-a sysObjectID=1.3.6.1.4.1.9.1.6
```

Deleting Devices Using `dcrcli`

To delete device using `dcrcli`:

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

Step 2 Enter the password corresponding to the username.

Step 3 Enter `del id=value`.

`id` is the Device ID. For example,

```
del id=54340
```

Editing Devices Using dcrcli

To modify devices using dcrcli

-
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
- Step 2** Enter the password.
- Step 3** Enter `mod id=value ip=value hn=value di=value dn=value -a attrname=value`
 Enter the Device ID (id).
 Enter either the IP Address (ip), Hostname (hn), or Device Identity (di).
 Enter the Display Name (dn) and the Attribute name (-a attrname). You can add multiple attributes. For example,
- ```
mod id=54341 ip=2.2.2.2 dn=cisco.com -a display_name=new_name
```
- 

## Listing the Attributes

To view the list of all attributes:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
- Step 2** Enter the password corresponding to the username
- Step 3** Enter `lsattr`
- This lists Attribute Name, Attribute Description, and Attribute Type.  
 Attribute Type is a constant that identifies an Attribute Name.  
 Example:  
 Attribute Type 1072 identifies the attribute name display\_name
-

## Viewing the Current DCR Mode Using `dcrcli`

To view the current DCR mode:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
  - Step 2** Enter the password corresponding to the username
  - Step 3** Enter `lsmode`

It lists the DCR ID, the DCR Group ID, the current DCR mode, and the associated Master/Slaves.

---

## Viewing Device Details

To view device details using `dcrcli`:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
  - Step 2** Enter the password corresponding to the username.
  - Step 3** Enter `details id=DeviceID`

This lists all the details about the device with the ID you have specified. For example,

`detail id=54341` lists the details for the device with device ID 54341.

---

## Changing DCR Mode Using dcrcli

To change mode to Master:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
- Step 2** Enter the password corresponding to the username
- Step 3** Enter `setmaster`
- The DCR mode gets changed to Master.
- 

To change mode to Standalone:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
- Step 2** Enter the password corresponding to the username
- Step 3** Enter `setstand`
- The DCR mode gets changed to Standalone.
- 

To change mode to Slave:

- 
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`.
- Step 2** Enter the password corresponding to the username
- Step 3** Enter `setslave master=value`
- You have to specify the Master for this slave.
- The DCR mode gets changed to Slave. For example,
- ```
setslave master=1.2.1.3 port=443
```
-

Import Using CLI

You can import using the Command Line Interface.

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

Step 2 Enter the password corresponding to the user name.

- To Import from file:

Enter `impFile fn=file name ft=file type`

fn—the file name

ft—the file type; CSV and XML are the valid values.

Example:

```
impFile fn=/opt/CSCOpX/test.csv ft=csv
```

- To Import from Local NMS:

Enter `impNms nt=NMS type il=Installation location`

nt—NMS type. Valid values are HPOV6.x and Netview7.x

il—Installation location of the NMS

Example:

```
impNms nt=HPOV6.x il=/opt/OV
```

- To import from Remote NMS:

Enter `ImpRNms nt=NMS type hn=hostname un=Remote User Name`

`il=Installation location ot=OS Type`

nt — NMS type. Valid values are HPOV6.x and Netview7.x

hn — Remote Host Name or IP address

un — Remote User Name

il — Installation location of the NMS

ot— OS Type; Valid values are HPUX, AIX, or SOL

Example:

```
impRNms nt=HPOV6.x hn=1.2.3.4 un=root il=/opt/OV ot=SOL
```

- To import from ACS:

Enter `ImpACS ot=OS Type hn=ACS Server Name or IP address un=ACS admin user name pwd=ACS admin password prt=port number`

ot— Operating System Type

hn — ACS Server Name or IP address

un — ACS admin user name

pwd— ACS admin password

prt — port number. Default is 2002.

Example:

```
impAcs ot=WIN2K hn=1.2.3.4 un=acsadmin pwd=acspwd prt=2002
```

Export Using CLI

You have the option to export using Command Line Interface.

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

Step 2 Enter the password corresponding to the user name.

Step 3 Enter `exp fn=filename ft=filetype`.

For *filetype*, CSV or XML are valid values. You can edit the Export Format file located at `NMSROOT\objects\dcrimpexp\conf\Export_Format_CSV.xml`.

Or,

Export_Format_XML.xml to specify the credentials. For example,

```
exp fn=/opt/CSCOpX/test.csv ft=csv
```



Note

For a complete list of attributes and their description, use the `lsattr` command in `dcrcli`. See [Listing the Attributes](#) for usage details. Also, see [Attributes and Description](#) and [Credentials and Description](#).

Implications of ACS Login Module on DCR

When Common Services is in ACS mode, you can perform operations in Device and Credential Repository (DCR) based on role assignment in ACS.

See [Setting the Login Module to ACS](#) for details on ACS login module.



Note

A device in DCR is mapped to a device in ACS based on IP address of that device in DCR and ACS. If a device in DCR has no IP address, then its `display_name` in DCR is mapped to host-names available in ACS.

In DCR, you can see the buttons enabled or disabled, based on the role assigned to you.

For example, if a user `U1` is assigned Approver role in ACS, he can see only the View button enabled in DCR. Further a user can see only those devices in DCR 's device-selector for which he has `View Devices` task assigned in ACS.

When performing operations in DCR, eventhough you select some devices and click the appropriate button, the operation will not be performed on all selected devices (unlike in CiscoWorks local mode). This is because the operation will be done only on those devices for which the you have the required privileges.

For example, a user `U2` is assigned Helpdesk role for device `D1` and System Administrator role for device `D2` in ACS. Now `U2` is able to select both `D1` and `D2` in DCR. But when the user clicks on **Delete**, only device `D2` will be deleted.

This is because `U2` has Helpdesk role for `D1`. Helpdesk role does not allow you to perform the Delete task.

Custom Roles and DCR

You can create new roles in ACS and assign a new combination of tasks to that role. In ACS, if a Custom role is created, a few points should be considered for DCR related tasks because certain DCR tasks have interdependencies. If certain tasks are included in the custom role, there will be other tasks which must also be assigned to the role to help you carry out the operations successfully.

The following table gives the details.

Task	Dependent Tasks
View Devices	View Devices task. Necessary to see a device in DCR device-selector. This needs to be assigned for all tasks which require device selection.
Add	View Devices task is necessary for seeing AUS or Cisco Cluster in Add wizard.
Edit	View Devices task is necessary to see a device's details in Edit wizard.
Bulk import	Add and Update tasks are necessary.
Export	View Devices task is necessary.
Delete	None.
Reports	None.
Change Mode	None.
Add User Defined Fields in DCR	None.
Modify User Defined Fields in DCR	None.
Delete User Defined Fields from DCR	None.
Register/Unregister 3rd Party Application in DCR	None.