



Administering Groups

The Groups feature in Common Services helps you to group devices managed by CiscoWorks applications. It helps in creating, managing, and sharing groups of devices. The groups created using this feature are shared across applications. The groups created in applications can also be viewed from Common Services too.

The following sections provides more information:

- [Basic Concepts](#)
- [Group Concept](#)
- [Secure Views](#)
- [Groups in a Single-Server Setup](#)
- [Groups in Multi-Server Setup](#)
- [DCR Mode Changes and Group Behavior](#)
- [Unregistering a Slave](#)
- [Group Administration](#)
- [System Defined and User Defined Attributes](#)

The following components are important:

- **Group Server:**
Manages groups of devices. It helps you to create, edit, delete, and refresh groups. It interfaces with an application service adapter (ASA) to evaluate group rules and retrieve devices of a particular group.
- **Application Service Adapters (ASAs):**
Application-specific information repository that serves as source of the devices and attributes that are grouped by the Groups Server. For Common Services, Device and Credential Repository (DCR) acts as the ASA. See [Chapter 5, “Managing Device and Credentials”](#) for detailed information on DCR.
- **Group Admin:**
Allows you to interact with the Group Server to create and manipulate groups using Group Admin.

Basic Concepts

- **Group Class:**
Representation of a set of devices belonging to DCR.
- **Group Object:**
Device in a group class. Each device in the group will have a set of attributes stored in DCR. Associated with every device is a unique and immutable device ID.
- **Group:**
Named aggregate entity comprising a set of devices belonging to a single class or a set of classes, with a common superclass. Groups can be shared between users or applications, subject to access-control restrictions. The membership of a group is determined by a rule.
- **Group Rule:**
Consists of one or more rule expressions combined by operators, which can be AND, OR or EXCLUDE.

Group Concept

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 hierarchical. Groups can be dynamic or static. They can be Private or Public.

This section has the following sub sections:

- [Group Hierarchy](#)
- [Dynamic Group](#)
- [Static Group](#)
- [Container Groups](#)
- [System-defined and User-defined Groups](#)
- [Common Groups and Shared Groups](#)

Group Hierarchy

Groups are managed in a hierarchical fashion that supports sub grouping. Each child group is a subgroup of a parent group, and its group membership will be a subset of its parent group.

Dynamic Group

A dynamic group is a group for which the membership list is always up-to-date.

Whenever you view a dynamic group, it always displays the latest group membership list.

Static Group

A static group is a group for which the membership is refreshed only when you explicitly request it. Between re-evaluations, 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 the ASA created the last time the group rule was evaluated.

Container Groups

Container groups are groups without a rule. The group membership is the union of the membership of its sub-groups. If a container group does not have sub-groups, the membership list will be blank.

System-defined and User-defined Groups

After you install Common Services, you get two predefined groups. They are:

- System-defined groups
System-defined groups are automatically created based on the device type information in DCR. When you add devices to DCR, the devices appear under the corresponding System-defined groups.
Just in Time groups (JIT) are groups that are automatically created/deleted as when devices are added/deleted/modified.
- User-defined groups
You can create groups here based on device attributes in DCR. This is possible only if you have administrator privileges.

These pre-defined groups come under the Provider group (or the root group), which, by default, is of the format `CS@hostname`. This Provider group is the parent of all Common Services groups found in the server.

You can change the Provider group name by changing the CiscoWorks Home Page Server Name. This can be configured at **Common Services > HomePage > Settings**. See [Setting Up CiscoWorks Homepage](#), for details.

You have to restart Daemon Manager after you change the Homepage server name, for the Provider group name change to take effect. After this, the Provider group name will be of the format `CS@Homepage Server Name`.

You can see these groups in Device and Credential Admin (DCA) and Device Center, and perform operations on the members of the group.

JIT groups are created based on the device types that are currently available in DCR. If all devices belonging to a single MDF type are deleted, the corresponding JIT group also gets deleted.

Common Groups and Shared Groups

Common group is the Common Services (CS) groups that are seen in the Groups UIs of Applications. Shared groups are the application groups other than the application's local group, that can be seen from the Common Services, and Groups UIs of Applications.

You have read-only access on shared groups. You can:

- Check group details
- Refresh group

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

For example, if you have a machine on which Common Services, RME, and Campus Manager are installed. If you invoke the Groups UI 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.

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

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

Here, RME@hostname is the local group.

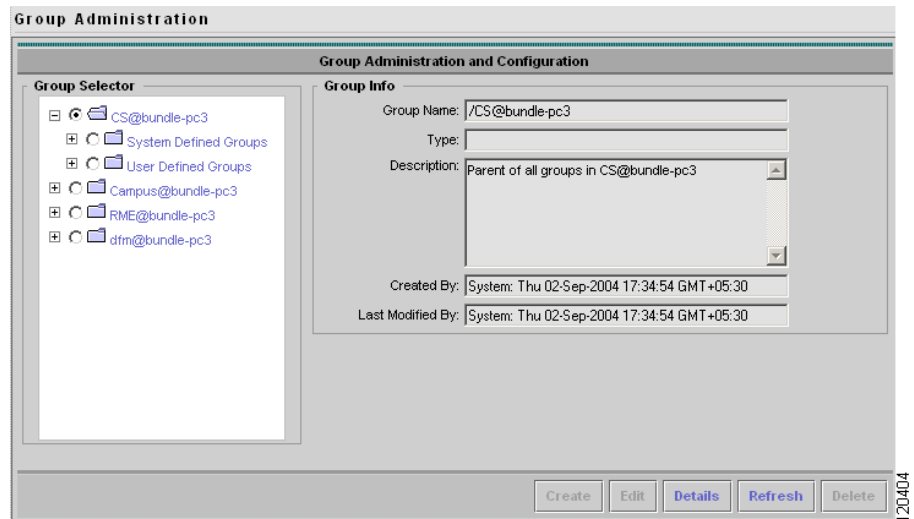
CS@hostname is the common group, and Campus@hostname is a shared group.

Similarly, in the Groups UI in Campus Manager, Campus@hostname is the local group.

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

Figure 6-1, a screen shot taken from the Group Administration UI in Common Services, on a machine (machine name : bundle-pc3) that has Common Services, Campus Manager, RME, and DFM installed, illustrates the concept.

Figure 6-1 Common Services Group Administration Window



In the Group Selector pane in the Group Administration page, you can see:

- CS@bundle-pc3
- Campus@bundle-pc3
- RME@bundle-pc3
- DFM@bundle-pc

Here, CS@bundle-pc3 is the local group, and the rest are shared groups.

Secure Views

Secure Views allow access to devices of a group to be restricted. Secure Views enables filtering of group membership based on the user and the application task context in which a request is made. Filtering will be performed only when operating in ACS mode.

While operating in Non ACS mode, no filtering will be performed, and evaluating a group results in all devices of that group being returned.

For example, assume there are two users A and B configured in ACS with different sets of privileges such that A can operate on devices D1, D2, D3 and B can operate on D4 and D5.

If B tries to perform any operation on the group to which all the above devices belong, B will be able to see only D4 and D5. This is because B is authorized to perform operations only on those two devices. For details on ACS login mode see [“Setting the Login Module to ACS” section on page 4-30](#).

Groups in a Single-Server Setup

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

For example, if there are Common Services, Campus Manager, and RME installed on a server, you can see the following groups in the Groups UIs of Common Services, Campus Manager, and RME.

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

For example, if 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 UI in Common Services.

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

Assume that 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 UI in RME, the number of devices you will see may be less than 30. This depends on whether RME is managing those devices.

Groups in Multi-Server Setup

Groups you create in Common Services groups UI in the Master get synchronized with the Slave. This does not happen in the case of applications.

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

However, 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 appear under the application's shared group in the Slave.

**Note**

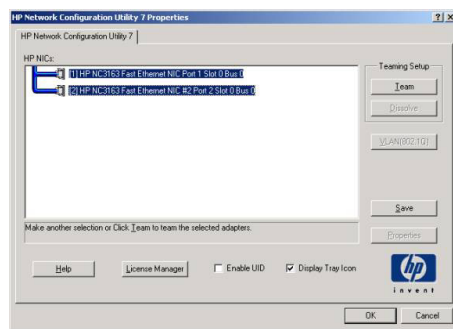
You cannot create groups in Common Services if it is in Slave mode. However, for applications, you can create groups even if the server on which they are installed is in Slave mode.

For example, if you have two servers M and S, where M is in Master mode, and S is in Slave mode. Assume both the machines have Common Services and RME installed.

In M, you can see the following groups:

- *CS@master hostname*
- *RME@master hostname*
- *RME@slave hostname*

Figure 6-2 Common Services Groups Window in a Multi-server Setup



In [Figure 6-2](#), you can see the groups displayed in the CS Groups UI, in a multi server scenario.

Note that the machine bundle-pc12 is the Master, and the machine bundle-sun280r1 is the Slave, in the figure.

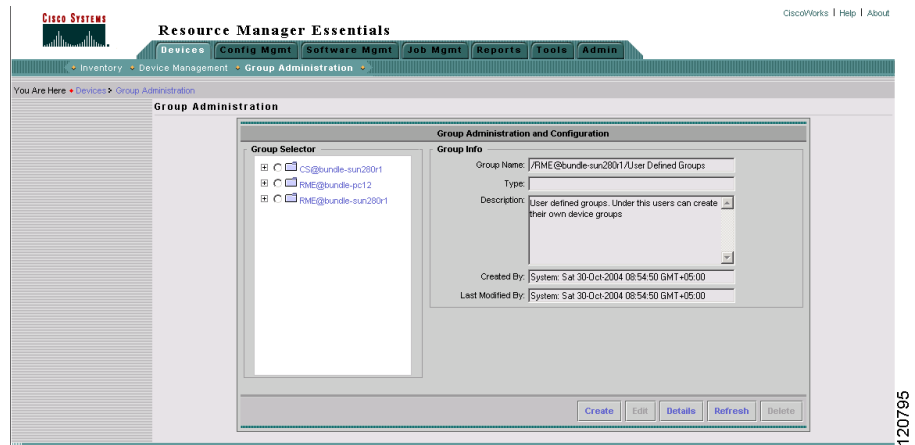
In the CS groups UI you can see:

- *CS@bundle-pc12* (The local CS group of the Master)
- *RME@bundle-pc12* (Application group pertaining to the Master)
- *RME@bundle-sun280r1* (Application group pertaining to the Slave)

Similarly, in S you can see the following groups:

- *CS@slave hostname*
- *RME@master hostname*
- *RME@slave hostname*

Figure 6-3 Groups Window in Application in a Multi-server Setup



In Figure 6-3, you can see the groups displayed in the Application (RME) Groups UI, in a multi server scenario.

Note that bundle-pc12 is the Master, and bundle-sun280r1 is the Slave, in the figure.

You can see:

- CS@bundle-sun280r1 (The local CS group of the Slave)
- RME@bundle-pc12 (Application group pertaining to the Master)
- RME@bundle-sun280r1 (Application group pertaining to the Slave)

If you have created a sub group under CS@*master hostname*, in S, you can see this subgroup under CS@*slave hostname*.

However, if you create a sub group in M under RME@*master hostname*, this sub group appears in S under RME@*master hostname*, and not under RME@*slave hostname*.

In a cluster if you have M as the Master, and S1 and S2 as M's slaves, and you want to evaluate S1's groups from S2, you need to import the certificate of S1 to S2 and vice versa.

DCR Mode Changes and Group Behavior

The DCR modes have a bearing on how groups are displayed in the Groups UI. Also the DCR mode decides whether you can perform any operation on the groups.

In Standalone mode, the groups you create in the CS Groups UI is propagated to the application Group instances of the applications installed in the same machine.

To perform operations on application groups, you should launch Groups UI from the application.

In Slave mode, the CS group admin UI is disabled. You cannot create any CS groups when the machine is in Slave mode. The UI is enabled automatically when the mode changes to Master or Standalone.

So, in a cluster that has several Slaves and a Master, if you need to create CS group, you need to go to the CS Groups UI in the Master and create the group. The group you create there will be synchronized with the Slaves.

The following table gives details of DCR mode changes and implications on Groups.

Table 6-1 DCR Mode Changes and Group Behavior

The initial mode	Mode Changed to:		
	Standalone	Slave	Master
Standalone	Not applicable.	<p>Master will get all the Slave groups. That is, if Slave has App-1 installed, Master will have all the groups that belong to App-1 on Slave.</p> <p>All these groups appear under the root group, /App-1@Slave.</p> <p>Also, Slave will get Master's groups. Group UI gets disabled.</p>	No change in the Group hierarchy.
Slave	<p>Groups UI gets enabled. The groups pertaining to Master and Slaves will be removed.</p> <p>The Slave's groups will disappear from the Master.</p> <p>The groups pertaining to the Slave whose mode was changed will disappear from other Slaves in the cluster.</p>	Not applicable.	Groups UI gets enabled. Groups pertaining to the previous Master and the associated Slaves will be removed.
Master	<p>All dependent Slaves will switch to Standalone mode.</p> <p>All groups pertaining to other machines will be removed. Groups UI will be enabled on all machines in the cluster.</p>	<p>If you select the Inform current Slaves of new Master Hostname check box when you change the mode to Slave, all the Slaves in the domain, switch to the new Master.</p> <p>In this case, application groups of all the Slaves in the domain, and the groups in the Master will be seen in the new Slave.</p> <p>The Groups UI will be disabled.</p> <p>If this check box is not selected, the new Slave will pickup the groups of the new Master. Other Slaves in the domain will move to Standalone mode.</p>	Not applicable.

Unregistering a Slave

The Unregister Slave utility helps you unregister a Slave which is no longer part of the domain.

The utility is useful in the following scenarios:

- Change in Slave's mode due to backup and restore. That is, if data is restored from Standalone/Master belonging to a different domain.
- When you uninstall CiscoWorks from slave.
- Change in Slave's mode, when master is not reachable. If the Master is down when the Slave's mode changes, the Master will not be aware of the Slave's mode change, when it comes up.

The Master will not receive any data from the Slave, but the Slave information will still be present in the its registry. A redundant group (such as CS@Slave) will still appear in the Master's Groups UI.

In the case of DCR, any device operation on Master will update the Slave list. But the same does not happen in the case of Groups.

You can run the UnregisterSlave utility to remove any unwanted slave information:

From the CLI, run:

```
NMSROOT /bin/perl NMSROOT/bin/UnregisterSlave.pl slave host name
```

You have to enter the hostname of the machine you want to unregister.

For information on effects of backup-restore on data, DCR modes, and Groups, see [“Effects of Backup-Restore on DCR” section on page 4-53](#) and [“Effects of Backup-Restore on Groups” section on page 4-55](#).

Group Administration

The Group Administration and Configuration UI helps you to create, manage, view, and delete groups.

**Note**

Group Administration UI will be enabled only on servers in which DCR is in Master or Standalone mode. The groups created in DCR master will be copied to Group Administration instances on servers where DCR is in Slave mode.

The following sections provide information on how to perform group administrative tasks in Common Services:

- [Creating Groups](#)
- [Modifying Group Details](#)
- [Viewing Group Details](#)
- [Refreshing Groups](#)
- [Deleting Groups](#)

Creating Groups

To create a new device group:

Step 1 Go to the CiscoWorks Homepage and select **Common Services > Groups**

The Groups Administration page appears.

The Group Administration and Configuration dialog box in the Group Administration page provides a Group Selector pane.

The System Defined Groups shows sub groups only after Device and Credential Admin (DCA) is populated.

The Group Selector field contains two groups:

- System Defined Groups
- User Defined Groups

These are the predefined (higher level) groups.

Step 2 Select the group from the groups listed in Group Selector to create a new sub group.

The group you select here is the Parent group for the new group you are about to create.

You can create a new group only under User Defined Group.

The default limit of User Defined Groups you can create is 100. If you try to create more than 100 User Defined Groups, you will get a message saying that you have exceeded the limit.

The Group Info fields on the right pane display details of the selected group.

You can change the Parent group later, if required.

The following tasks have to be performed:

1. [Specifying Group Properties](#)
2. [Defining Group Rules](#)
3. [Assigning Group Membership](#)

While creating a new group you must complete all the three tasks in this sequence to create a group.

If you exit the wizard at any stage by clicking **Cancel**, the details you have specified will be lost and the group will not be created.

Specifying 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.

To complete the tasks in this phase:

Step 1 Go to the CiscoWorks Homepage and select **Common Services > Groups** .

The Groups Administration page appears.

Step 2 Click the Create button in the Group Administration and Configuration dialog box

The Properties:Create dialog box opens.

- Step 3** Enter a name for the group in the Group Name field in the Properties:Create dialog box.
- The group name should 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 4** Click **Select Group**, if you want to copy attributes of an existing group.
- The Replicate Attributes dialog box appears.
- Step 5** Select the group you need from the Replicate Attributes list and click **OK**.
- Step 6** Click **Change Parent**, to change the Parent group.
- The Group Selector page appears.
- Step 7** Select the group you need from the Select Parent list.
- Step 8** Click **OK**.
- The Group Administration wizard changes the Parent group to the one you selected, and returns to the Properties:Create window.
- Step 9** Enter a description for the group.
- Typically, you can enter a detailed description of the group identifying its characteristics in this field.
- Step 10** Select the Membership Update mode for the group.
- The modes of membership updates available are:
- **Automatic:**
The membership of the group is automatically recomputed each time the group is invoked.
 - **Only Upon User Request:**
The membership of the group is recomputed only when an explicit request is made, using the Refresh option.
- If you select Automatic, the group will be a Dynamic group. If you select Only Upon User Request, the group will be a Static group.
- Step 11** Select either **Public** or **Private** radio button to specify the visibility scope.
- Step 12** Click **Next** to get to the Rule:Create dialog box.
-

Defining Group Rules

In the Rules:Create 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 Rules:Create 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 Rules>Create 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.

Click **View Parent Rules** to display the rules defined for its ancestor groups.

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. To do so:

Step 1 Delete the rules displayed in the Rule Text field, and click any other field.

Step 2 Select appropriate parameters for Object Type, Variable, and Operator. See [System Defined and User Defined Attributes](#) for details on the variables.

Enter the value for the variable you have selected.

Step 3 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.

For example, the rule type:

```
:CMF:DCR:Device.DisplayName equals "joe"
```

will select the device with the DisplayName *joe*.

The Rules>Create dialog box refreshes and displays the Boolean operator field before the Object Type field in Rules Expression. You can form composite rules using the OR, AND, or EXCLUDE options in the Boolean operator field.

The OR, AND, EXCLUDE drop down list appears only when there is at least one rule expression in the text area.

You can validate rules that are entered directly into the Rules Text field or rules formed using the Add Rules Expression option in the dialog box.

To check whether the syntax is valid, click **Check Syntax**.

To view the rules defined for the parent groups, click **View Parent Rules**.

Step 4 Click **Next**.

The wizard takes you to the Membership>Create dialog box, where you can further refine the group definition by adding or deleting specific devices from the group.

Assigning Group Membership

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.

To add devices to the group you have created:

-
- Step 1** Select one or more devices in Available Objects From Parent Group column.
To select multiple devices, hold the Ctrl or Shift keys down and click.
- Step 2** Click **Add**.
The selected devices are removed from Available Objects From Parent Group and added to the Object Matching Membership Criteria column.
-

Removing Devices

To remove devices from the group:

-
- Step 1** Select one more devices in Object Matching Membership Criteria column.
To select multiple devices, hold the Ctrl or Shift keys down and click.
- Step 2** Click **Remove**.
The selected devices are removed from the Object Matching Membership Criteria column and added to Available Objects From Parent Group.
- Step 3** Click **Next**.
The Summary:Create window appears. It displays the group name, the parent group, description, the membership update type, group rules, and the visibility scope of the group you created.
If you want to change the parameters, click **Back** to go back to the previous windows and make changes.
- Step 4** Click **Finish** to create the group based on the parameters specified.
-

Viewing Group Details

To view the details of a group:

-
- Step 1** Go to the CiscoWorks Homepage and select **Common Services > Groups**
The Group Administration page appears.
- Step 2** Select a group from the Group Selector pane.
The Group Info pane on the right side displays the high-level properties of the selected group.

Step 3 Click **Details**.

The Group Administration wizard displays the details of the group in Properties:Details window.

- Click **View Parent Rules** to display the rules set for the parent group.
The rules set for the parent group are displayed in the Show Parent Rules window.
- Click **Membership Details** to display a list of devices and their corresponding object types.
The membership details are displayed in Membership:Details window.
In the Membership:Details window, you can:
 - Click on the column headers to sort the entries in the table.
 - Select the number of rows to be displayed in the table in the Rows per page option.
- Click **Property Details** to return to the Property:Details window.

Step 4 Click **Cancel** to return to the Group Administration and Configuration page.

Modifying Group Details

You can modify some of the details for a group using this feature.

To modify the details of a group:

Step 1 Go to the CiscoWorks Homepage and select **Common Services > Groups > Group Admin**.

The Group Administration page appears.

Step 2 Select a group from the Group Selector pane.

The Group Info fields on the right side displays details of the selected group.

Step 3 Click **Edit**.

The Group Administration wizard guides you through the process of editing a group. It displays the details of the group in Properties>Edit window.

Step 4 Change the Group Name, Description, Membership Update, and Visibility Scope in the Properties>Edit dialog box.

You cannot change the Parent group or copy attributes from a different group in Edit mode.

Step 5 Click **Next**.

The wizard takes you to the Rules>Edit window.

Step 6 Change the rules as required. For details on creating the rules, see [“Defining Group Rules” section on page 6-12](#).**Step 7** Click **Next**.

The wizard takes you to the Membership>Edit window.

Step 8 Add or remove devices from the list of objects in Objects Matching Membership Criteria as required. For details on creating the rules, see [“Assigning Group Membership” section on page 6-14](#).

Step 9 Click **Next**.

The wizard takes you to the Summary window.

If you want to change the parameters specified, click **Back** to go back to the previous windows and make changes to the properties or rules.

Step 10 Click **Finish** to modify the group.**Step 11** Click **OK**.

The Group Administration wizard copies the attributes of the selected group and displays it in the corresponding fields in Properties>Create window.

Note that the Parent group you have selected for the group does not change even if you are copying attributes from a group that belongs to a different Parent group.

Refreshing Groups

You can recompute the membership of a group by re-evaluating the group's rule. The membership of Automatic groups is recomputed dynamically.

The membership of Only-upon-user-request groups is recomputed only when explicitly refreshed with this option.

To refresh a group:

Step 1 Go to the CiscoWorks Homepage and select **Common Services > Groups > Group Admin**.

The Group Administration page appears.

Step 2 Select a group from the Group Selector pane.

The Group Info fields on the right pane displays details of the selected group.

Step 3 Click **Refresh**.

The Group Administration pop-up window prompts you for confirmation.

Step 4 Click **Yes**.

The selected group is recomputed and the window, refreshed.

Deleting Groups

You can delete a group from the Group Selector. When you delete a group, all the child groups under the group are also deleted.

To delete a group:

-
- Step 1** Go to the CiscoWorks Homepage and select **Common Services > Groups > Group Admin**.
The Group Administration page appears.
- Step 2** Select the group from Group Selector.
The Group Info fields on the right pane displays details of the selected group.
- Step 3** Click **Delete**.
The Group Administration and Configuration dialog box prompts you for confirmation.
- Step 4** Click **Yes**.
The selected group is deleted.
-

Deleting Stale Groups Using CLI

You can delete groups that belonged to users removed from CiscoWorks.

To delete a stale group, you must run the DeleteStaleGroups utility.

To run the DeleteStaleGroups utility:

On Windows:

-
- Step 1** Enter `NMSROOT\bin`
- Step 2** Enter `DeleteStaleGroups -user username -pfile passwordfile -staleuser StaleUser`
-

On Solaris:

-
- Step 1** Enter `NMSROOT/bin`
- Step 2** Enter `DeleteStaleGroups.sh -user username -pfile passwordfile -staleuser StaleUser`
-

The explanation for these entries is:

-user: Current user who has the necessary privileges to delete Groups.

-pfile: Absolute Path of the text file with user's CiscoWorks login password in one line.

-staleuser: The user whose group has to be deleted.

System Defined and User Defined Attributes

The following table provides details on the System Defined attributes that are available in Common Services. These are pre-defined attributes, available by default.

Attribute	Description
DisplayName	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.
ManagementIpAddress	IP address used to access the device. Both IPv4 and IPv6 address types are supported.
HostName	Device Host name.
DomainName	Domain name of the device.
DeviceIdentity	Identifies pre-provisioning devices. The value would be application specific.
SystemObjectID	sysObjectID value. It may be UNKNOWN in the case the facility that is populating the repository does not know the value.
Category	Category in which the device falls. The first level entries in the Device Type tree in DCR Device Management UI. For example, <code>Routers</code> is a category.
Series	Series to which the device belong. The second level entries in the Device Type tree in DCR Device Management UI. For example, <code>Cisco 3100 Series Routers</code> , that falls under the category <code>Routers</code> .
Model	Model of the device. The third level entries in the Device Type tree in DCR Device Management UI. For example, the model <code>Cisco 3101 Router</code> falls under the <code>Cisco 3100 Series Routers</code> , which comes under the category <code>Routers</code> .
MDFId	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.

The User Defined Fields available in the Variable drop-down list is taken from DCR. You can create Used Defined Fields at **Common Services > Device and Credentials > Admin**. For details, see [Adding User-defined Fields](#).

If you create a User Defined Field which is similar to one of the predefined System Defined attributes, an `_UDF` suffix is appended to the User Defined field you add, to distinguish these two attributes.

For example if you create a User Defined Field called `DisplayName` (which is one of the pre-defined attribute present in the Variable drop-down list), this will be displayed as `DisplayName_UDF`.



Note

You should not create a User Defined fields in the format *System Defined Field*_UDF, where System Defined Field stands for any attribute listed in the above table.

By default, four user defined fields are available. You can create 12 user defined fields in DCR. The maximum number of user defined fields that can be added in the Variable drop-down list is 16.