CHAPTER 3

Security and Permissions in the Orchestrator System

Configuring Permissions for Delegated Administration

You can configure different levels of access to the Orchestrator network. This section describes its role-based security and permissions model.

Overview of the Orchestrator Security Model

Orchestrator uses a role-based approach to security:

- Roles are created for sets of permissions required to access particular administration tasks.
- To grant users access, add them to the roles that have the required permissions.
- The Windows user or group has no direct relationship with the Orchestrator task or component. Instead, roles represent business functions, such as Help Desk or Policy Administrator.

Using Roles for Delegated Administration

A built-in *Root Administrator* role gives members of that role access to the Orchestrator network. Anyone who has local administrator permissions on the Orchestrator server has root administrator access level.

When setting up delegated administration, a member in the root administrator role uses the Administrator console to:

- Add users and groups to the built-in administrator role.
- Create security roles for specific permissions sets.

- Configure system-wide or group-level permissions in the roles.
- Add users (or groups) to the roles and apply role permission sets to those users.

Permissions Categories

Security role categories:

- Global (server-wide)—Permission to manage a particular area of functionality across the entire Orchestrator network.
- Group level—Permission to perform specified management tasks on selected groups.

Security roles can have global, group, or both types of permissions. For example, the built-in Policy Administrator role has Manage policies (global) permission by default. You can also give this role Apply policies permission for specific groups.

For information about each setting and creating effective permissions, see the "Administrative Permissions and Descriptions" section on page 3-4.

Granting Root Administrator Permissions

A user or group that has root administrator permissions is granted access to all tasks and groups in the system.

Follow these search guidelines:

- Search results return users and groups that contain the search string that you enter. Wildcard characters * and ? are treated as text characters.
- Search operations are case insensitive for domain users and case sensitive for local users. For example:

  Searching for *admin* returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)

  Searching for *admin* returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)
  - BUILTIN\Administrators (local group)
  - Administrator (local user)

You must have local administrator permissions on the Orchestrator server computer to grant permissions.

Step 1 In the Administrator console, from the Permissions menu, choose **Edit Roles**.

Step 2 In the list of roles on the Configure Permission page, choose **Root Administrator**.

Step 3 On the Users tab, for each Windows user or group that you want toadd to the role, click **Add** to find and select the user.

Note Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a *user not found* message.

Step 4 When you are done adding users to the root administrator role, click **Save**.

Creating Additional Security Roles and Grant Permissions

To grant access to perform administrative tasks, create security roles, configure permissions sets for each role, and add users to the appropriate roles.

Before you complete this procedure, see the "Overview of the Orchestrator Security Model" section on page 3-1.

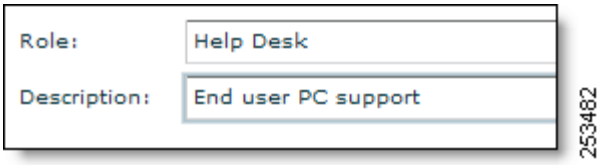
This procedure must be completed by a local administrator of the Orchestrator server who is also a member of the root administrator role in the Orchestrator Administrator console.

Step 1 In the Administrator console, from the Permissions menu, choose **Edit Roles**.

Step 2 On the Edit Roles page, click **New Role**, or select an existing role to customize or copy.

If you create, customize, or copy a role, give the new role a name and description (Figure 3-1).

Figure 3-1 Adding the Role Name and Description



Step 3 On the Users tab, for each Windows user or group that you want to include in the role, click **Add** to find and select the user.

Note Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a *user not found* message.

Step 4 Configure permissions for this role. For details about permission levels, see the "Administrative Permissions and Descriptions" section on page 3-4.

a. On the Device Groups tab, expand the tree to display the groups that you want this role to have access to, and select the appropriate permissions.

Note When you enable permissions on a group, they are also enabled on its subgroups.

b. If you want this role to have access to policies or group assignment rules across the entire system (independent from group-level permissions), on the Global Permissions tab, check the appropriate check box.

Omit this step when granting only group-level permissions.

Step 5 When you complete assigning permissions, click **Save**.

Administrative Permissions and Descriptions

This section describes the permission types that you can enable across the system or on specific device groups to set up an administration environment.

Permission Types

You can assign permission types to roles that you create in the Administrator console:

- Global (server-wide)—Permission to manage a particular area of functionality across the Orchestrator system.
- Group level—Permission to perform specified management tasks on selected groups.

For example, a Policy Administrator role can have permission to create and edit policies across the system but not to apply policies to devices. A Help Desk role might only have permission to change the power state of devices in specific groups.

Global Permissions

In the Administrator console, you can give administrative permissions across the Orchestrator system.

- Manage policies—Create a new power management policy; modify any component of an existing policy, including scheduling schemes, power state transitions and policy assignment rules; and give permission to delete policies.
- Manage group assignment rules—Create, modify, or delete group assignment rules and criteria that move devices from one organizational tree location to another.

Global permissions expand the access of a role to some group-level tasks. See the "Effective Permissions" section on page 3-5.

Caution Global permissions grant access to the selected area over the entire Orchestrator system. If you use these permissions, consider your changes carefully. Evaluate how the changes would affect existing policies and devices.

Group-Level Permissions

Note Permissions that you enable on a group are inherited by all of its subgroups.

Table 3-1 Group-Level Permissions

Permission	Allowed Access Level
Manage group	Adds, deletes, and edits settings on groups or subgroups and removes devices from groups (for example, renaming a group or changing its parent). Does not give access to policies. You can move devices from one group to another when you have Manage groups permission for both groups. However, if you have Manage groups permission on the source group but not the destination group (as defined in the rule criteria), you can manually run group assignment rules for a set of devices.
Assign policy	Assigns policies to new devices and different policies to existing devices. Does not give access to create, modify, or delete policies.
Change device state	Changes the power state of a device. For example, wake the device, and change it to standby mode.
Edit devices	Changes device properties, such as whether a device can receive a license, its description, and EnergyWise properties. Does not give access to policies.

Effective Permissions

If a user is a member of multiple roles, the effective permissions that the user has on a group is the set that provides the highest level of access. This is true whether or not the role is given permissions directly on the group or indirectly through inheritance from an ancestor group.

Sometimes global permissions for an area can effectively expand group-level permissions:

- *Assign policies* permission is granted at the group level. However, members of a role with global *Manage policies* permissions can change settings on existing policies or delete policies that are assigned to devices. Either is a form of policy assignment.
- Enabling the global permissions set *Manage group assignment rules* gives access to create rules that move any device to any location in the organizational tree. Moving devices among groups is a management task that can be done through this global permissions set even if the *Manage group* permission is not enabled at the group level.

Configuring Windows Firewall To Allow Server Access to Web Components

If you use Orchestrator components that access the server through HTTP and Windows Firewall is enabled on the server, make sure that TCP port 80 is added to the exceptions list.

You need to access the server through HTTP to:

- Use the Sustainability Dashboard when the dashboard is not installed on the server computer.
- Enable Wake for Remote Access so that end users can wake their computers from off-site.

Tip Wake for Remote Access is an add-on component that comes with Orchestrator. See the *Cisco EnergyWise Orchestrator Wake for Remote Access Administrator Guide*.

- Administer the server from a remote computer, for example, as you would if you set up delegated administration.

Step 1 On the server computer, go to **Windows Start** menu > **Control Panel** > **Windows Firewall**.

Step 2 On the Exceptions tab, click **Add Port**.

Step 3 In the Add a Port dialog box:

a. Enter a name that shows that the exception is for power management components. This name appears in the exceptions list.

b. Specify port 80.

c. Select TCP.

Step 4 Click **OK**, and click **OK** in the Windows Firewall dialog box.

For additional information, see the *Add a Port to the Firewall Rules List* Microsoft TechNet topic.