Role-based administration for System Center Configuration Manager

Applies to: System Center Configuration Manager (Current Branch)

With System Center Configuration Manager, you use role-based administration to secure the access that is needed to administer Configuration Manager. You also secure access to the objects that you manage, like collections, deployments, and sites. After you understand the concepts introduced in this topic, you can Configure role-based administration for System Center Configuration Manager.

The role-based administration model centrally defines and manages hierarchy-wide security access settings for all sites and site settings by using the following:

- *Security roles* are assigned to administrative users to provide those users (or groups of users) permission to different Configuration Manager objects. For example, permission to create or change client settings.
- *Security scopes* are used to group specific instances of objects that an administrative user is responsible to manage, like an application that installs Microsoft Office 2010.
- *Collections* are used to specify groups of user and device resources that the administrative user can manage.

  With the combination of security roles, security scopes, and collections, you segregate the administrative assignments that meet your organization's requirements. Used together, they define the administrative scope of a user, which is what that user can view and manage in your Configuration Manager deployment.

Benefits of role-based administration

- Sites are not used as administrative boundaries.
- You create administrative users for a hierarchy and only need to assign security to them one time.
- All security assignments are replicated and available throughout the hierarchy.
- There are built-in security roles that are used to assign the typical administration tasks. Create your own custom security roles to support your specific business requirements.
- Administrative users see only the objects that they have permissions to manage.
- You can audit administrative security actions.

When you design and implement administrative security for Configuration Manager, you use the following to create an *administrative scope* for an administrative user:

- Security roles
- Collections
- Security scopes

The administrative scope controls the objects that an administrative user views in the Configuration Manager console, and it controls the permissions that a user has on those objects. Role-based administration configurations replicate to each site in the hierarchy as global data, and then are applied to all administrative connections.

[!IMPORTANT]
Intersite replication delays can prevent a site from receiving changes for role-based administration. For information about how to monitor intersite database replication, see the Data transfers between sites in System Center Configuration Manager topic.

Security roles

Use security roles to grant security permissions to administrative users. Security roles are groups of security permissions that you assign to administrative users so that they can perform their administrative tasks. These security permissions define the administrative actions that an administrative user can perform and the permissions that are granted for particular object types. As a security best practice, assign the security roles that provide the least permissions.

Configuration Manager has several built-in security roles to support typical groupings of administrative tasks, and you can create your own custom security roles to support your specific business requirements. Examples of the built-in security roles:

- *Full Administrator* grants all permissions in Configuration Manager.
- *Asset Manager* grants permissions to manage the Asset Intelligence Synchronization Point, Asset Intelligence reporting classes, software inventory, hardware inventory, and metering rules.
- *Software Update Manager* grants permissions to define and deploy software updates. Administrative users who are associated with this role can create collections, software update groups, deployments, and templates.

[!TIP]
You can view the list of built-in security roles and custom security roles you create, including their descriptions, in the Configuration Manager console. To view the roles, in the **Administration** workspace, expand **Security**, and then select **Security Roles**.

Each security role has specific permissions for different object types. For example, the *Application MMM* security role has the following permissions for applications: Approve, Create, Delete, Modify, Modify Folders, Move Objects, Read/Deploy, and Set Security Scope.

You cannot change the permissions for the built-in security roles, but you can copy the role, make changes, and then save these changes as a new custom security role. You can also import security roles that you have exported from another hierarchy, for example, from a test network. Review the security roles and their permissions to determine whether you'll use the built-in security roles, or whether you have to create your own custom security roles.

To help you plan for security roles

1. Identify the tasks that the administrative users perform in Configuration Manager. These tasks might relate to one or more groups of management tasks, such as deploying

applications and packages, deploying operating systems and settings for compliance, configuring sites and security, auditing, remotely controlling computers, and collecting inventory data.

2. Map these administrative tasks to one or more of the built-in security roles.
3. If some of the administrative users perform the tasks of multiple security roles, assign the multiple security roles to these administrative users instead of in creating a new security role that combines the tasks.
4. If the tasks that you identified do not map to the built-in security roles, create and test new security roles.

For information about how to create and configure security roles for role-based administration, see Create custom security roles and Configure security roles in the Configure role-based administration for System Center Configuration Manager topic.

Collections

Collections specify the user and computer resources that an administrative user can view or manage. For example, for administrative users to deploy applications or to run remote control, they must be assigned to a security role that grants access to a collection that contains these resources. You can select collections of users or devices.

For more information about collections, see Introduction to collections in System Center Configuration Manager.

Before you configure role-based administration, check whether you have to create new collections for any of the following reasons:

- Functional organization. For example, separate collections of servers and workstations.
- Geographic alignment. For example, separate collections for North America and Europe.
- Security requirements and business processes. For example, separate collections for production and test computers.
- Organization alignment. For example, separate collections for each business unit.

For information about how to configure collections for role-based administration, see Configure collections to manage security in the Configure role-based administration for System Center Configuration Manager topic.

Security scopes

Use security scopes to provide administrative users with access to securable objects. A security scope is a named set of securable objects that are assigned to administrator users as a group. All securable objects must be assigned to one or more security scopes. Configuration Manager has two built-in security scopes:

- The *All* built-in security scope grants access to all scopes. You cannot assign objects to this security scope.

- The *Default* built-in security scope is used for all objects, by default. When you first install Configuration Manager, all objects are assigned to this security scope.

If you want to restrict the objects that administrative users can see and manage, you must create and use your own custom security scopes. Security scopes do not support a hierarchical structure and cannot be nested. Security scopes can contain one or more object types, which include the following:

- Alert subscriptions
- Applications
- Boot images
- Boundary groups
- Configuration items
- Custom client settings
- Distribution points and distribution point groups
- Driver packages
- Global conditions
- Migration jobs
- Operating system images
- Operating system installation packages
- Packages
- Queries
- Sites
- Software metering rules
- Software update groups
- Software updates packages
- Task sequence packages
- Windows CE device setting items and packages

There are also some objects that you cannot include in security scopes because they are only secured by security roles. Administrative access to these objects cannot be limited to a subset of the available objects. For example, you might have an administrative user who creates boundary groups that are used for a specific site. Because the boundary object does not support security scopes, you cannot assign this user a security scope that provides access to only the boundaries that might be associated with that site. Because a boundary object cannot be associated to a security scope, when you assign a security role that includes access to boundary objects to a user, that user can access every boundary in the hierarchy.

Objects that are not limited by security scopes include the following:

- Active Directory forests
- Administrative users
- Alerts
- Antimalware policies
- Boundaries
- Computer associations
- Default client settings
- Deployment templates
- Device drivers
- Exchange Server connector
- Migration site-to-site mappings
- Mobile device enrollment profiles
- Security roles
- Security scopes
- Site addresses
- Site system roles
- Software titles
- Software updates
- Status messages
- User device affinities

Create security scopes when you have to limit access to separate instances of objects. For example:

- You have a group of administrative users who must be able to see production applications and not test applications. Create one security scope for production applications and another for the test applications.
- Different administrative users require different access for some instances of an object type. For example, one group of administrative users requires Read permission to specific software update groups, and another group of administrative users requires Modify and Delete permissions for other software update groups. Create different security scopes for these software update groups.

For information about how to configure security scopes for role-based administration, see the Configure security scopes for an object in the Configure role-based administration for System Center Configuration Manager topic.