CHAPTER 5

AMC Administration

This chapter covers the Admin portion of AMC. It includes the following sections:

Note Only the System Administrator can perform all of the tasks described in this chapter. Other user types have limited abilities on the Admin Tab. See the "Assigning Roles to Users" section on page 5-3 for further details.

AON Licensing

AMC provides the ability to upload licenses that enable additional features and functionality. Contact your Cisco representative to obtain more information about licensing.

How to Get There

Go to **Admin** > **Licensing**, then click the Add button.

Actions to Take

Click the Browse button to navigate to the location on your PC where the license file is stored, then click the Upload button to send the file to the AMC.

Managing AON Users

AMC users fall into one of the following categories:

- Local users—these users are created and managed within AMC.
- External users—these users are created on and managed by an external LDAP server.

Note A new installation of AMC includes several local users with **aonsadmin** as their default password. To ensure that only authorized personnel have access to the AMC, change the default passwords or delete unneeded users.

Managing Local Users

Local users are created and managed by the AMC. You can use this page add to perform the following tasks:

- Add and delete users
- Display information about users
- Edit a user's information, including privileges.
- Change a user's password

How to Get There

Go to Admin > Users > Manage Local Users

Actions to Take

Click one of the following buttons:

- **New**—creates a new users. See Creating New Users, page 5-2
- **Show**—displays information on the selected user. See Displaying Information on Users, page 5-3
- **Edit**—changes information about the selected user. See Editing Users, page 5-3
- **Password**—changes the password of the selected user.
- **Delete**—removes the selected user from the system.

Creating New Users

AMC enables you to create new local users.

How to Get There

Go to **Admin > Users > Manage Local Users**, then click the New button.

Actions to Take

Enter the appropriate information for the user and select a role. Use Control+click to select multiple roles. For description of available roles, see Assigning Roles to Users, page 5-3.

After completing the fields, click the **Submit** button to save your changes.

Displaying Information on Users

You can use AMC to display information on a selected user, including name, email address, and roles assigned.

How to Get There

Go to **Admin > Users > Manage Local Users**, then select a user. Click the Show button to display the information.

Editing Users

AMC provides the ability to edit the properties of existing local users.

How to Get There

Go to Admin > Users > Manage Local Users, then select a user. Click the **Edit** button.

Actions to Take

Make changes as necessary. If you are changing the role of a user, see the "Assigning Roles to Users" section on page 5-3.

Once you have made your changes, click the **Submit** button to save them.

Deleting Users

The **Delete User Confirmation** page lists details of the user being deleted, including projects to which the user may be assigned. Click **No** to cancel the deletion and return to the previous page. Clicking **Yes** brings about one of the following options:

- If the user is not working on an open project, the user is immediately deleted.
- If the user is working on an open project, a new page will ask for final confirmation before deleting the user.

Assigning Roles to Users

AMC users can be given roles based on their need to perform certain actions on AMC. Each role grants specific privileges within AMC. For example, the Application Designer role can only access the project to which it is assigned and upload extensions to the AMC, however, a Network Administrator can access functions related to managing and monitoring nodes. To give a user full access to AMC, assign the System Administrator role to that user.

Role-Based Access Control

Two new user roles are introduced in AON Version 2.4. Users with the System Administrator role are permitted to access any project. Users with the Application Developer role are able to access only the projects to which they are assigned. Users that were assigned the roles Network Administrator, Security Administrator, and Application Administrator in previous AON releases are now assigned the role System Administrator, If a user does not have permission to access system-wide resources, AMC hides those resources from the user.

The table below shows the roles available in AMC, and the sections on each tab these roles can access.

Table 5-1 AMC User Roles

Role	Project Tab	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Application Admin	All actions on assigned projects except deletion and new project creation	—	• Application • JMS • Monitoring • AON Security • Service Profiles	All	All	• Keypairs • Public Certificates	• AMC Diagnostics • Extensions • AMC Security • Data Migration • Users
Application Designer	Open and view assigned projects only	—	—	—	—	—	• AMC Diagnostics • Extensions
Application Developer	Open and view assigned projects only	—	• Application • JMS • Monitoring • AON Security • Service Profiles	All	All	• Keypairs • Public Certificates	• AMC Diagnostics • Extensions • AMC Security • Data Migration • Users
Network Admin	Open and view all projects	All	Monitoring	—	All	—	—
Security Admin	Open and view all projects	—	• Authentication and Authorization • AON Security • Node Management Security	—	All	All	• Users • AMC Security
System Admin	All	All	All	All	All	All	All

Editable Roles

When you edit users' roles, you can assign only those roles that are equal to or less than your own role. For example, an application administrator cannot give the system administrator role to a user. The table below lists each role and the roles that user is able to edit.

Assigned Role	Editable Roles
System administrator	All
Application administrator	All application-related roles
Application designer	None
Application developer	None
Network administrator	None
Security administrator	All except system administrator

Note Do not remove the system administrator role from the user named **aonsadmin** unless you have first assigned that role to at least one other user.

To assign roles to a user, see one of the following sections:

- Creating New Users, page 5-2
- Editing Users, page 5-3
- Assigning Roles to External Users, page 5-6

Managing External Users

AMC provides the ability to use an existing LDAP server for user management. To do this, complete the following tasks in the order specified:

1. Creating an LDAP Profile, page 5-5
2. Assigning Roles to External Users, page 5-6
3. Creating an Authentication Realm, page 5-6

Creating an LDAP Profile

An LDAP profile provides the information needed by AMC to retrieve user data from an existing LDAP server.

How to Get There

Go to **Admin** > **Users** > **Manage Local Users** > **LDAP**, then click the **New** button.

Actions to Take

Complete the fields as appropriate for the LDAP server being used. Contact your LDAP administrator for details.

Assigning Roles to External Users

How to Get There

Go to **Admin > Users > Manage Local Users > Role Mapping**, then click the **New** button.

Data to Enter

Table 5-2 shows the field of the Role Mapping page.

Table 5-2

Entry	Description
Name	Name of your choosing for this property set.
LDAP Attribute Name	The LDAP attribute that is to be used to specify the AMC role.
Condition Operator	Choose one of the following from the drop-down list: • equals—information retrieved from LDAP server must match exactly with LDAP attribute value specified below. • contains—information retrieved from LDAP server must contain LDAP attribute value specified below. • defineRoles—information retrieved from LDAP will define the role of the user.
LDAP Attribute Value	The value for the attribute specified above.
Assign Roles	Click the **Edit List** button to choose roles that are to be assigned to users who match the LDAP attribute. See "AMC User Roles"

Actions to Take

After completing the fields, click the **Submit** button to save your changes.

Creating an Authentication Realm

The LDAP Authentication Realm binds the LDAP information specified in the "Creating an LDAP Profile" section on page 5-5 with the role mapping information specified in "Assigning Roles to External Users" section on page 5-6.

How to Get There

Admin > Users > Manage Local Users > Authentication Realm, then click the **New** button.

Data to Enter

Table 5-3 shows the Authentication Realm page.

Table 5-3 Authentication Realm

Entry	Description
Name	Name of your choosing for this property set.
Realm Name	Name of your choosing for the realm.

Table 5-3 Authentication Realm (continued)

Entry	Description
LDAP Connection Profile	Choose an available LDAP profile from the drop-down list. See the "Creating an LDAP Profile" section on page 5-5 to create a new profile.
Role Mapping Policies	Click the Edit List button to select from the available Role Mapping property sets. See the "Assigning Roles to External Users" section on page 5-6 to create a new property set.

Actions to Take

After completing the fields, click the Submit button to save your changes. Once you completed this task, the LDAP configuration appears in the drop-down list on the AMC log-in page.

Managing AMC Certificates

The AMC Security Page enables you to manage the keypairs and certificates used by AMC for secure communication.

- **Keypairs**–view, edit, or delete keypairs that have been assigned to AMC.
- **Public Certificates**–view, edit, or delete public certificates that have been assigned to AMC.
- **Root Certificates**–view, edit, or delete root certificates that have been assigned to AMC.

How to Get There

- Go to **Admin > AMC Security**

Note If no keypairs or certificates are present, you must use the Keystores tab to generate them.

Managing Extensions

The Extensions page enables you to upload custom software to adapt your AON environment to the specific business needs of your network. This page provides the ability to upload the following:

- JMS resources
- Schema packages
- Transform packages
- Transform parser packages
- Custom bladelets and extensions

If you have opened the System project, you can also upload the following:

- Adapter packages
- Adapter extension packages

Extensions are uploaded into and deployed from a particular project. Any property set categories included in the extension are accessible only to the project that uploaded the extension. Each project must upload its own unique extensions. An extension uploaded by an application project cannot be shared among other projects. However, extensions uploaded into the system project can be shared.

When an extension package is uploaded, AMC appends the project prefix to the package name. However, the prefix is not applied to the custom extension itself, nor is it applied to any custom policy categories and predefined property sets in the package.

AMC does not allow extension packages to have duplicate names. An attempt to upload a duplicate extension will fail. Additionally, AMC verifies that any custom property sets contained in an extension do not exist in other projects. If there is duplication, the upload attempt will fail.

Note Before you can upload an extension with AMC, you must use AON Development Studio to package it.

For more information about developing and packaging extensions, see the *AON Programming Guide*.