CHAPTER 30

Managing Web Console Users

This chapter describes how to manage ACE XML Manager web console users. It covers these topics:

About Console Users

As the development and monitoring point for key network security policies, access to the console needs to be carefully protected. Only authenticated users can access the ACE XML Manager web console. The web console enforces further restrictions by associating each user account to a set of privileges, which determine which operations that user may perform. Finally, each user of the ACE XML Manager web console can view or edit only those subpolicies to which an administrator of the ACE XML Manager has granted access.

By assigning user type, roles, and policy access rights appropriately, a console administrator can ensure that policy and configuration changes are made only by users authorized to make them.

To access the ACE XML Manager web console, you must first **authenticate** by submitting a username/password combination. The ACE XML Manager matches your authenticated user identity with a set of permissions in the web console. The following sections describe authentication and authorization schemes the ACE XML Manager supports, as well as how to configure it to use them.

Types of Web Console Users

The ACE XML Manager web console provides for several types of users. Administrator users have the most wide-ranging permissions and external developers the least. However, the specific actions a user can take are a function of the user's role and the access permissions associated with a particular policy. For example, access can be allocated to users to specific subpolicies in the console. A subpolicy contains a subset of the resources and objects that compose the entire ACE XML Gateway policy.

The types of console users are:

- **administrator** users have full access to all subpolicies and privileges in the console. The ACE XML Manager comes preconfigured with a user account named `administrator`, which has this user type.

- **privileged users** can change policy and configuration settings according to one of the following roles:
  - **Access control** role can configure settings that control who can access a protected resource.
  - **Routing** role can create and configure handlers, service descriptors, routes, and message transformations.
  - **Operations** role can approve the deployment of policies, deploy policies, move or archive policies, configure exception-handling, and configure logging functions.
  - **Message log** role can view the contents of message traffic logs, which may contain sensitive information.
- **policy view users** can view policy information but cannot edit it.
- **external developer** users has the most limited permissions: this user may view the ACE XML Manager's directory of provisioned services, and download WSDL files that the ACE XML Manager generates for those services, but they cannot do anything else.

Note For reference information on the privileges available to users by role, see the user privileges table in the "Console Privileges by User Type and Role" topic of the ACE XML Manager web console online help.

About the Administrator User

The ACE XML Manager web console comes with a predefined local user account with the username of `administrator`. You cannot delete this account or change its privileges.

The `administrator` account is intended for the user who performs maintenance and administration tasks on the ACE XML Gateway and Manager. For example, one of the significant tasks reserved for the `administrator` user is that of changing the means by which the ACE XML Manager authenticates users.

If desired, you can create additional user accounts that have the administrator role. The `administrator` user, or any user account with administrator privileges, has unrestricted access to every feature of the ACE XML Gateway and Manager, so great care should be taken in assigning this user type or in sharing the password for the built-in `administrator` account.

The built-in `administrator` user account is exempt from failed login attempt blocking. However, other users created with administrator privileges are not exempt, if that feature is enabled. For more information, see "Configuring Failed Login Attempt User Blocking" section on page 32-304.

Authentication Modes

The ACE XML Manager supports a flexible set of authentication schemes for user accounts. The default configuration of the system is to authenticate using local user accounts. Local user accounts are maintained by the ACE XML Manager itself.

The ACE XML Manager can optionally authenticate its users against LDAP or RADIUS servers instead of using local user accounts.

When choosing an authentication scheme, you should be aware that the ACE XML Manager uses the same authentication mechanism for all user accounts. For example, if your system is configured to use LDAP, then you cannot also configure it to authenticate using local accounts; you must choose one or the other.

Keep in mind that if you switch from local authentication to external authentication, your local user accounts will no longer be available and will need to be recreated on the external server. Because many users of the ACE XML Manager may be affected by such a change, make sure you consider carefully how to ensure necessary access to the ACE XML Manager before switching authentication modes.

When the ACE XML Manager is configured for external authentication, you cannot use the ACE XML Manager's tools to create working user accounts or change their roles. Because the user accounts and roles are defined and assigned by a separate server, any additions or changes you wish to make must be made on that server.

Whatever the authentication mode, the ACE XML Manager requires you to designate an administrator user. This user must be identified upon initial configuration of the ACE XML Manager, and whenever you change to a new authentication mechanism.

Creating User Accounts

This section describes how to create a user account, how to assign access privileges (roles) to it, and how to specify the authentication method the ACE XML Manager uses to authenticate all user accounts.

Creating Local User Accounts

A **local user account** is stored on the ACE XML Manager appliance itself. In contrast, LDAP authentication utilizes remote account data and authentication mechanism.

All other authentication schemes utilize local accounts and remote authentication: the accounts themselves reside on the ACE XML Manager appliance, and the ACE XML Manager calls an external RADIUS server or LDAP directory to authenticate users.

Note If you are planning to use LDAP authentication, skip this section and create your user accounts on the LDAP server, not locally. For more information, see "Switching to LDAP Authentication Mode" section on page 30-289.

To create local user accounts:

Step 1 While logged in to the ACE XML Manager web console as an `Administrator` user, click the **User Administration** link in **Administration** section of the navigation menu.

If the **User Administration** link is not visible, click the plus sign (**+**) next to the **Administration** banner to expand that menu.

The ACE XML Manager displays the **User Administration** page.

Step 2 Click the **Create a New User** button at the upper-right side of the page.

The ACE XML Manager displays the **New User** page.

Step 3 In the **Username** field, enter a username for the new account.

Step 4 In the **Password** field, enter a password for the new account.

If the strict passwords option is enabled (in **System Management > Manager Settings > User Authentication & Security**), the ACE XML Manager rejects easily guessed passwords, such as those that resemble dates, Social Security numbers, email addresses, many dictionary words, names, and various other patterns.

The password must be a minimum of eight characters long and must consist of alphanumeric characters only. For security reasons, do not use the same default password for all new accounts.

Step 5 In the **Repeat password** field, enter the same password you entered in the **Password** field.

The passwords must be an exact match, including use of uppercase and lowercase letters.

Step 6 Specify whether the account is active by choosing an item from the **User Status** menu.

By default, new accounts are created with **enabled** status. If you don't want the user to be able to log in yet, you can choose **disabled** instead, and change the account's status to **enabled** at a later time.

Step 7 Choose the user's type from these options in the menu:

- **Privileged User** to enable this user to edit policies and configuration settings.

  The ACE XML Manager enables the **Access Control**, **Routing**, **Operations**, and **Message Traffic Log** checkboxes.
- **Policy View User** to enable this user to view, but not edit, the subpolicies that are selected in the **Subpolicies** list box.
- **External Developer** to enable this user to view, but not edit, only the ACE XML Manager's directory of provisioned services.
- **Administrator User** to grant full privileges to this user, including the ability to modify any subpolicy and create and delete other users.

Note For reference information on the privileges available to users by role, see the user privileges table in the “Console Privileges by User Type and Role” topic of the ACE XML Manager web console online help.

You can change the user's type later if the need arises.

Step 8 If you assigned the **Privileged User** type, specify one or more roles for this user:

- To allow this user to create and modify authenticators, authorization groups, provisioning, and authentication resources, click the **Access Control** box.
- To allow this user to work with virtual services and message processing settings, click the **Routing** box.
- To allow this user to deploy policies, as well as to control processes and machine-level configuration of the ACE XML Gateway, click the click the **Operations** box.

Note For this role, the user must have access to at least the **Shared** subpolicy.

- To allow this user to view the contents of the Message Traffic Log (which may contain sensitive information), choose the **Message Traffic Log** option.

Note You cannot assign the **Message Traffic Log** role alone. To assign the **Message Traffic Log** role to a user, you must also assign at least one additional role to that user.

Step 9 Specify subpolicies the user can view or edit:

- To allow access to all policies, including those which may be created in the future, click **Allow this user to access any subpolicy**.

- To allow access to only the policies represented by highlighted list items, click **Allow this user to access these specified subpolicies**. When you choose this item, you must select at least one policy from the list that appears beneath it. Select multiple policies by holding down the control key while clicking.

  Users who need to be able to deploy a subpolicy need to have access to Shared as well as to the subpolicy.

  

  Note Granting access to every subpolicy in the list is not the same as granting "any subpolicy" access. If a new subpolicy is created, the user has access to the new policy only if granted "any subpolicy" access. If you allow access to all the subpolicies listed at the time you create the user account, then the user has access to those subpolicies, but not new ones.

Step 10 Click **Save Changes** to create the new account. To exit without creating the new account, click **Cancel**.

If you enabled the new account, its owner can now log in to the web console and use the tools available to the role assigned to the account. You do not need to deploy the policy for the user to log in.

Changing Roles

A **role** defines the operations a user can perform. Every user has at least one role. Only an administrator user can assign roles. The available roles are predefined and cannot be changed.

To change roles assigned to an existing user:

Step 1 As an `Administrator` user in the web console, click the **User Administration** link in the navigation menu.

The **User Administration** page displays this Manager appliance's user accounts. An **Edit** link for each user provides access to settings for that user account.

Step 2 Click the **Edit** link next to the user you want to modify.

Step 3 In the **Edit User** page, click a radio button to specify whether the user is to have a **Privileged User**, **Policy View user**, or **External Developer** account. You can choose only one type.

If you specified the **Privileged User** account type, the ACE XML Manager enables the **Access Control**, **Routing**, **Operations** and **Message Traffic Log** checkboxes.

Note For reference information on the privileges available to users by role, see the user privileges table in the "Console Privileges by User Type and Role" topic of the ACE XML Manager web console online help.

Step 4 If the user is a **Privileged User**, click the **Access Control**, **Routing**, **Operations** or **Message Traffic Log** checkboxes as appropriate to assign those roles.

Step 5 Click the **Save Changes** button to accept the new user account. To exit without creating the new account, click the **Cancel** button. The change takes effect immediately.

Enabling Access to Subpolicies

When a subpolicy is created, it is accessible only to web console users who have subpolicy access set to "any subpolicy." To grant access to users that do not have "any subpolicy" access, the administrator must edit the "specific subpolicy" access privileges of each user needs to be able to view or edit the subpolicy.

To configure user access to a subpolicy, you need to edit the access privileges of individual user accounts, as follows:

- To grant or deny the user's access to specific subpolicies, see "Granting or Denying Access to Specific Subpolicies" section on page 30-288.
- To allow the user to access any subpolicy, see the following section, "Granting Access to Any Subpolicy" section on page 30-288.

Granting Access to Any Subpolicy

This section describes how to enable access to any subpolicy, including those which may be created at a future date. Operations that require this kind of access include publishing to a UDDI server, configuring user access to subpolicies, creating new subpolicies, deploying policies, and approving subpolicies.

Note that access refers to the user's ability to view the subpolicy. The ability to edit the subpolicy is a function of the user's type and privileges.

To enable a specified user account to access any subpolicy:

Step 1 As an `Administrator` user in the console, click the **User Administration** link in the navigation menu.

If the **User Administration** link is not visible, click the plus sign (**+**) next to the **Administration** banner to expand that menu.

Step 2 Click the **Edit** button next to the user account to edit.

The **Edit User** page for the specified user appears.

Step 3 Choose the **Allow this user to access any subpolicy** option.

Step 4 Click the **Save Changes** button to commit the changes.

The **User Administration** page reflects your changes to the user's account.

Granting or Denying Access to Specific Subpolicies

This section describes how to enable user access only to the subpolicies you specify. This kind of access is appropriate for most users. Only users acting in some sort of administrative capacity, such as those who approve policies for deployment, should have the "any subpolicy" access the preceding section describes.

To enable a specified user account to access specified subpolicies:

Step 1 As an `Administrator` user in the ACE XML Manager web console, click the **User Administration** link in the navigation menu.

If the **User Administration** link is not visible, click the plus sign (**+**) next to the **Administration** banner to expand that section of the menu.

Step 2 In the **User Administration** page, click the **Edit** button to the right of the user.

The **Edit User** page for the specified user appears.

Step 3 Click the **Allow this user to access these specified subpolicies** button.

Step 4 In the list of subpolicies that appears beneath this button, click as necessary to grant or deny this user's access to a specific set of subpolicies.

The highlighted items in this list represent subpolicies the user can access. Subpolicies that are not highlighted are not visible or available to this user. To select multiple subpolicies, press the **Control** key while clicking items in this list.

Note To be able to deploy a subpolicy, a user needs to have access to that subpolicy as well as Shared.

Step 5 Click the **Save Changes** button to commit the changes.

The **User Administration** page reflects changes to the account.

Setting the Authentication Mode

The ACE XML Manager can be configured to authenticate users in a number of different ways, such as local, LDAP or RADIUS server. The ACE XML Manager uses one authentication scheme to authenticate all user logins.

By default new user accounts on the ACE XML Manager use local authentication. In this case, the ACE XML Manager maintains the user account information locally, on its own disk, and authenticates users itself, rather than by contacting an external authentication service.

To use another authentication method, you must configure the account explicitly to do so, as described in the following sections:

- Switching to LDAP Authentication Mode, page 30-289
- Switching to RADIUS Authentication Mode, page 30-291

Switching to LDAP Authentication Mode

The ACE XML Manager can be configured for LDAP authentication. In this case, the Manager checks credentials submitted at the web console login against an external LDAP directory.

In addition to account information for users who are authorized to access the Manager web console, the directory must have group definitions that can be mapped to the standard Manager web console roles, such as Administrator, Access Control, and so on. Notice that access to specific subpolicies can be mapped to groups as well.

To enable LDAP authentication, first collect the following information:

- LDAP server's host address and port number. This is the URL under which the LDAP server appears on the network. Sometimes, this address specifies the number of the port on which the server listens for incoming requests; for example: ldap://example.com:389/dc=bar,dc=com

- LDAP binding information, including the username and password used to bind to the server. The username should be the bind DN. That is, the Distinguished Name that corresponds to an ACE XML Manager account username.
- Base DN. This is the DN at which to begin searching for a record in the LDAP directory.
- LDAP user records. Each ACE XML Manager user account must have a valid user record on the LDAP server.
- LDAP user groups. Each of the roles defined in the ACE XML Manager policy must be represented as a valid user group on the LDAP server. The name of the group need not be the same as the ACE XML Manager role it represents. For example, you could create an “Ops” group to represent the Operations role.
- LDAP user record representing the ACE XML Manager's administrative user. The ACE XML Manager administrator account is represented as a valid user record on the LDAP server. The name of the user does not have to be “Administrator,” as it does when using other authentication schemes.

When configuring LDAP authentication mode in the web console, you can use the test tool at the bottom of the LDAP Authentication Mode configuration page to confirm that your new settings are correct. If the test fails, you can correct errors before enabling LDAP authentication.

To set up the ACE XML Manager to use LDAP authentication mode:

Step 1 As an `Administrator` user in the web console, click the **System Management** link.

Step 2 Click the link labelled **Manager Settings**, which is located on the right side of the ACE XML Manager heading.

The ACE XML Manager displays the **Manager Settings** page.

Step 3 Click the **Switch to LDAP Authentication** button, which is in the **User Authentication & Security** section of the page.

The console displays the **LDAP Authentication Mode** page.

Step 4 At the top of the page, in the LDAP Server section, enter information used to bind to your LDAP server:

- **Host**. The Distinguished Name of the LDAP host to which the ACE XML Manager must bind.
- **Port**. The number of the port on which the LDAP host accepts incoming requests.

  Many LDAP servers accept incoming requests on port 389; for SSL requests, port 636 is typical. If you intend to use SSL, be sure to check the **Use SSL** checkbox, as the next step describes.
- **Use SSL**. To use SSL for LDAP requests, click this box it. If your LDAP server does not use SSL, the **Use SSL** box should be clear.

Step 5 If you need to execute a setup query, use the fields in the **Setup Query** section to enter information the ACE XML Manager uses to construct the query:

- **Bind with DN**. The Distinguished Name to which the username attribute binds.
- **Password**. The shared secret that authenticates a particular user to the LDAP server.
- **Base DN**. The DN at which to begin searching for a record in the LDAP directory.
- **Username Attribute**. The name of the LDAP attribute that specifies the username associated with a particular ACE XML Manager account.
- **Perform group query as this user**. The name of the group from which this user inherits privileges.

Step 6 In the right column of the **Subpolicy-To-Group Mapping** section, specify the valid LDAP group that corresponds to the ACE XML Manager subpolicy shown in the left column.

The left column in this section shows all available subpolicies of the current working policy. At the very least, this column always contains the Shared subpolicy. If other subpolicies exist in the policy, they appear here, too.

Step 7 In the right column of the **Role-To-Group Mapping** section, specify the valid LDAP group that corresponds to each ACE XML Manager role.

The left column shows all Manager user roles. In the right column, specify each LDAP group that corresponds to each role.

Step 8 In the **ACE XML Manager Administrator Authentication** section, specify information used to authenticate the LDAP user that is the administrator of the ACE XML Manager:

a. Enter the administrator's LDAP username in the **Administrator Username** field.

Note If this user does not authenticate successfully in the Admin role, the ACE XML Manager does not switch to LDAP authentication mode.

b. Enter the administrator's LDAP password in the **Administrator Password** field.

Step 9 In the **Test LDAP Configuration** section, test your settings before enabling LDAP authentication mode:

a. Enter a username and password that should work with the ACE XML Manager once LDAP authentication is activated.

b. Click the **Test** button.

The ACE XML Manager displays the results of your attempt to authenticate. If the attempt fails, review the LDAP settings with your LDAP administrator before continuing.

Step 10 To accept the new settings and enable LDAP authentication mode, click the **Switch to LDAP Authentication** button at the bottom of the page. To exit the **LDAP Authentication Mode** page without saving changes, click the **Cancel** button.

If you save changes and the changes are accepted, subsequent logins to the ACE XML Manager web console must use valid LDAP user accounts defined on the authentication server.

Switching to RADIUS Authentication Mode

To switch to RADIUS authentication mode:

Step 1 As an `Administrator` user in the console, click the **System Management** link in the navigation menu.

Step 2 Click the link labelled **Manager Settings**, which is located to the right of the ACE XML Manager heading.

The ACE XML Manager displays the **Manager Settings** page.

Step 3 Click the **Switch to RADIUS Authentication** button, which is in the **User Authentication & Security** section.

The ACE XML Manager displays the **RADIUS Authentication Mode** page.

Step 4 In the **Radius Server** section, enter the information needed to authenticate a connection with the RADIUS server:

- **Host**. URL of the RADIUS server.

- **Port**. The port on which the RADIUS server listens for incoming requests.
- **Account Port**. The port on which this account authenticates with the RADIUS server.
- **Shared Secret**. The value, token, or passphrase that authenticates a user to the RADIUS server.

Step 5 In the ACE XML Manager **Administrator Authentication** section, enter information used to authenticate the RADIUS user that is the administrator of the ACE XML Manager:

a. Enter the administrator's RADIUS username in the **Administrator Username** field.

Note This username must not match that of any other local ACE XML Manager account. This user inherits the Console Admin role. If the user does not authenticate successfully in the Console Admin role, the web console is not switched to RADIUS authentication.

b. Enter the administrator's RADIUS password (not Shared Secret) in the **Administrator Password** field.

Step 6 To accept the new settings and enable RADIUS authentication mode, click the **Switch to RADIUS Authentication** button at the bottom of the page. To exit the **RADIUS Authentication Mode** page without saving changes, click the **Cancel** button.

If you save changes and the changes are accepted, subsequent logins to the ACE XML Manager web console must use valid RADIUS user accounts defined on the authentication server.

Switching to Local Authentication Mode

While in LDAP or RADIUS authentication mode, the **User Authentication & Security** section of the **Manager Settings** page shows a **Switch To Standard Passwords** button that you can use to cause the ACE XML Manager to authenticate with local usernames and passwords.

To change the authentication mode from server-based to local authentication:

Step 1 As an `Administrator` user, click the **System Management** link in the navigation menu.

Step 2 Click the **Manager Settings** link, located to the right of the ACE XML Manager heading.

The ACE XML Manager displays the **Manager Settings** page.

Step 3 Click the **Switch To Standard Passwords** button, which is in the **User Authentication & Security** section.

The ACE XML Manager displays the **Standard Passwords Authentication Mode** page.

Step 4 To accept the new settings and enable local authentication mode, click the **Switch To Standard Passwords** button at the bottom of the page to accept the change. To exit the RADIUS or LDAP authentication mode page without saving changes, click the **Cancel** button.

If you save changes and the changes are accepted, subsequent logins to the web console must use valid local user accounts defined in the ACE XML Manager.

Step 5 If you switched from LDAP authentication mode, the ACE XML Manager creates a local user account for each LDAP account that has ever logged into the web console.

These accounts cannot be used until you assign passwords to them. Decide whether to activate these accounts, delete them, or create new local accounts:

- To activate an account, assign a password to it.
- To allow an account to remain inactive, you need not do anything to it.
- A local account created by the ACE XML Manager as a result of switching from LDAP mode has no password; it cannot be used unless you assign a password to it.
- To delete an account, click the **Delete** link next to it on the **Administration > User Administration** page.
- To create a new account, click the **Create A New User** button on the **Administration > User Administration page**. The name for the new account should not duplicate that of any existing account, including those created automatically when switching from LDAP authentication mode.