CHAPTER 35

Configuring the Manager Web Console

This chapter describes how to configure the ACE XML Manager web console settings. It covers these topics:

Changing the Manager SSL Certificate

An SSL certificate is used to secure connections between web browsers and the ACE XML Manager web console (on the management port, by default, 8243). At installation time, a temporary certificate is used to secure this connection. You should replace it with a permanent certificate you generate in the ACE XML Manager as described here.

Note The ACE XML Manager is unable to generate private keys in UTF8 format. The ACE XML Manager can import pre-existing certificates and keys in UTF8 format, but cannot generate them.

Generating a CSR for the Manager

To generate a certificate signing request (CSR) for the ACE XML Manager SSL certificate, take the following steps:

Step 1 As the `administrator` user, click the **Cluster Management** link in the **Administration** section of the navigation menu.

The Cluster Management page shows the clusters in the administrative control of this Manager. If not using multiple clusters, only a single cluster appears in the list, the Default Cluster.

Step 2 Click the **Manage SSL Certificates** button.

Step 3 To generate a Certificate Signing Request (CSR), click the **Manage Certificates** button, and then **Generate New CSR** (in the **Outstanding Certificates Signing Requests** area of the Manager SSL Certificates page.

Step 4 In the Generate Certificate Signing Request page, complete the following fields:

Field	Description
Common Name	The name of the individual or entity whose identity is being certified.
E-mail Address	The email address that is to receive the signed certificate, in response to the CSR.
Company (O)	The name of the Organization or company with which the CN is associated.
Department (OU)	The name of an organizational unit or sub-group within the organization.
City	The Locality or City of the entity being certified.
State	The State or Province of the entity being certified.
ISO Country Code	The two-letter International Standards Organization (ISO) code for the country of the entity.

Step 5 When finished entering the information, click **Generate Request**. Using the information you supplied, the ACE XML Manager generates a Certificate Signing Request (CSR) and displays it on the *Certificate Signing Request* page.

Step 6 Copy the CSR data (the part between the `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` strings) into a text file or an email message. Send the CSR data to your preferred certificate authority for transformation into a signed X.509 certificate.

Note CA request forms may ask you to specify a certificate type. If so, request an Apache-style certificate for use with the ACE XML Manager.

Step 7 When the signed certificate arrives, install it on the ACE XML Manager as described in "Setting the Manager SSL Certificate" section on page 35-354.

Note The CA may not return the certificate quickly. In some cases, it may take days to fulfill the certificate signing request.

Setting the Manager SSL Certificate

After receiving a signed certificate in response to the request generated, you can replace the ACE XML Manager's SSL certificate with a CA-signed certificate:

Step 1 After receiving a signed certificate from the CA, return to the Cluster Management page as the `administrator` user.

Step 2 Click **Manage Certificates**, and then the **Upload Signed Cert** link (in the **Outstanding Certificate Signing Requests** pane).

Step 3 In the Upload New ACE XML Manager Certificate page, specify the certificate to upload either from a file system or a network location, or by copying the text of the certificate into the text field.

Step 4 Click the **Upload** button.

Step 5 To apply the certificate to a Manager, click the **Exit to Cluster Management** button.

Step 6 In the Cluster Management page, click the **edit** link next to the cluster for which you want to use the certificate. If not managing multiple clusters from this ACE XML Manager, click **edit** next to Default Cluster.

The **SSL Certificate** field shows the certificate currently in use. If this value is “Temporary Certificate, Please Regenerate,” the default certificate has not been replaced yet. This deployment should not be considered secure until you replace this default certificate with one signed by a CA.

Step 7 In the **SSL Certificate** field, choose the certificate you uploaded and click **Save Changes**.

Prompting URL-Based Resource Reload at Deployment

For security reasons, the ACE XML Manager never automatically retrieves any remote resources used in a policy. To ensure that you have the latest versions of any remotely hosted resources, such as schemas or certificates obtained from URLs, you may need to reload such resources before deploying a policy.

Optionally, you can configure the ACE XML Manager to prompt console users to reload resources before deploying a policy.

Note For more information, see “Reloading URL-Based Resources at Deployment” section on page 29-288.

To enable resource-reloading prompting in the console:

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

Step 2 In the System Management page, click the **Manager Settings** link next to the ACE XML Manager heading.

Step 3 In the **Workflow** pane of the general settings, click the **Prompt users to reload URL-based resources** checkbox.

Step 4 Click the **Save Changes** button at the bottom of the page.

Step 5 To verify that resource-reloading prompts are active, initiate a deployment attempt by clicking the **Deploy Policy** button at the top of the page.

The **Step 1 of 4: URL Resource Refresh** page appears if resource-reloading prompts are enabled. If this page does not appear as the first screen you see after clicking the **Deploy Policy** button, resource-reloading prompts are not enabled.

Step 6 Deploy or click the **Cancel Deployment** button to return to the **Policy Manager** page without deploying.

Configuring User Idle Time-Out Settings

For security purposes, the ACE XML Manager web console can log an idle user off of the console after a configurable period. By default, the idle timeout session period is 1800 seconds, or 30 minutes.

To change the ACE XML Manager web console's idle time-out period:

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

Step 2 Click the **Manager Settings** link.

Step 3 Type a new idle timeout value in seconds in the **Idle Session Timeout** field, which appears with the **User Authentication & Security** settings.

Step 4 When finished, click **Save Changes**. The change takes effect immediately.

Configuring Failed Login Attempt User Blocking

If a console user fails a consecutive number of login attempts (three, by default), the ACE XML Manager can block subsequent attempts by the user to access the console. The user account remains suspended until an administrator enables it directly.

If desired, failed login blocking can be disabled, as described below. Also, note that the built-in `administrator` user is never blocked. However, additional user accounts with the Administrator role are subject to failed login blocking.

To re-enable a user who has been blocked:

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

Step 2 Click the **Edit** button next to the disabled user.

Step 3 Change the User Status from disabled to enabled.

Step 4 Click **Save Changes**.

To configure general behavior of this feature, as the Administrator user:

Step 1 Click the **System Management** link in the navigation menu.

Step 2 Click the **Manager Settings** link in the System Management page.

Step 3 Configure this feature using the controls labelled **Disable User After**. With this option enabled, a user is blocked from logging in after the specified number of failed login attempts.

Step 4 When finished, click **Save Changes**.

The changes take effect immediately.

Setting the Display Time Zone

The ACE XML Gateway uses Greenwich Mean Time (GMT) for its internal clock. GMT is used for timestamp verification, internal log data, and other time-based service processing activities.

You can, however, change the time zone that the ACE XML Manager uses to display information without interfering with the normal operation of the ACE XML Manager or Gateways.

To change the ACE XML Manager's time zone for display:

Step 1 Click the **System Management** link in the navigation menu.

Step 2 Click the **Manager Settings** link in the System Management page.

Step 3 In the interface section of the page, choose the **Display Time Zone** from the menu.

Step 4 Click **Save Changes**.

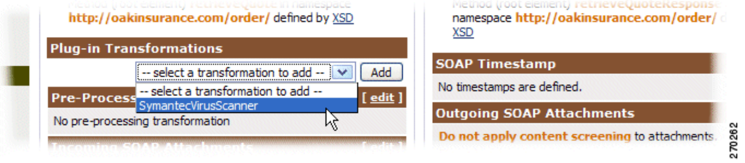
Integrating SDK Extensions with the Web Console

You can customize and expand the capabilities of the ACE XML Gateway by creating system extensions. The ACE XML Gateway SDK contains tools for creating custom modules for access control, message transformations, and service traffic protocols.

Note SDK extensions can be applied to traffic handled at virtual service interfaces only; they are not applicable to traffic processing for virtual web applications.

After creating the extension, load it to the ACE XML Manager appliance filesystem to make it available in the policy. The settings for configuring the extension are exposed in the ACE XML Manager web console alongside the standard, built-in configuration parameters.

Figure 35-1 Applying an Extension in the Console



http://oakinsurance.com/order/ defined by XSD

namespace http://oakinsurance.com/order/ XSD

No pre-processing transformation

No timestamps are defined.

Do not apply content screening to attachments.

Plug-in Transformations
-- select a transformation to add --
Add
-- select a transformation to add --
SymantecVirusScanner
Pre-Process
[edit]
SOAP Timestamp
Outgoing SOAP Attachments
270262

When you deploy the policy, the extension is automatically moved to the ACE XML Gateway along with the policy.

Note For information on creating extensions, see the *Cisco ACE XML Gateway Developer's Guide.*

Viewing Available Extensions

You can view information on the extensions added to the ACE XML Manager from the System Management page, as follows:

Step 1 Click the **System Management** link in the navigation menu.

Step 2 In the ACE XML Manager settings section of the page, click the **view status page** link next to the **Extensions Status** label.

The **Extensions Status** page appears.

Step 3 To see detailed information on an extension, click the expand control next to the extension name.

Extension Development Mode

Developing an extension is usually an iterative process that involves repeated stages for development and testing on the ACE XML Manager. Setting the ACE XML Manager to extension development mode makes this process easier.

In SDK development mode, the ACE XML Manager automatically reloads extensions that are placed in the extension directory on the appliance filesystem, without having to restart the ACE XML Manager. It also causes logging events to be written in-line in the event logs.

To set the ACE XML Manager to SDK development mode:

Step 1 Click the **System Management** link in the navigation menu.

Step 2 Click the **Manager Settings** link in the System Management page.

Step 3 In the **General** settings section of the page, select the **Enable extension development mode** checkbox.

Step 4 Click **Save Changes**.

The change takes effect immediately.