CHAPTER 11

Managing Resource Files

This chapter describes how to work with resource files in a policy used by the ACE Web Application Firewall Manager. It covers these topics:

Types of Resource Files

An ACE Web Application Firewall policy is made up of objects and configuration settings that control how the ACE Web Application Firewall processes traffic. One type of policy object is a resource file. Resource files are self-contained artifacts that can be used throughout the policy, and include:

- **Public/Private Keys**—Public/private keypairs are used to certify the identity of the ACE Web Application Firewall
- **Trusted Certificate Authorities**—X.509 certificate files that identity providers of certificates that the ACE Web Application Firewall instance is prepared to trust
- **Remote Server Certificates**—X.509 certificate files used to identify destination servers

This section describes how to upload and manage resource files. There is usually more than one way to upload a particular type of resource file in the ACE Web Application Firewall Manager web console—from the Resource Manager page in the console or from the page where a resource is applied. These instructions describe in general terms how to upload resources using the resource manager. Once the resource has been uploaded, it appears as a menu choice in applicable locations of the console.

It is often preferable to load resources from a URL location rather than from a filesystem location. This allows you to take advantage of URL-based resource refreshing. Resource refreshing is a process by which the ACE Web Application Firewall Manager checks for updates to resources loaded in the policy by checking whether there are updates to the source. If so, the resource can be updated. For more information, see "Reloading URL-Based Resources at Deployment" section on page 12-94.

Generating a CSR

A public/private keypair associated with the ACE Web Application Firewall enables you to secure the communication channel between the ACE Web Application Firewall and consumer or between the ACE Web Application Firewall and backend service. The first step in acquiring a certificate is to create a certificate signing request, or CSR, for submission to a certificate authority.

To generate certificate requests in the ACE Web Application Firewall Manager web console:

Step 1 Click the **Public/Private Keypairs** link in the **Resources** section of the navigation menu.

Step 2 Click the **Generate CSR** button at the bottom of the page.

Step 3 In the **Generate Certificate Signing Request** page, type in the **Resource Name** field the name that is to identify this resource in the policy.

Step 4 Type appropriate values into the following fields in the **Subject Identification Information** section:

Table 11-1 CSR settings

Field	Description
Common Name	This field should contain the external hostname of the ACE Web Application Firewall. Note that for a clustered Firewall configuration this would be the common host name that consumers use to address the cluster.
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 being certified.

Step 5 From the **Key Type** menu, choose the algorithm to use when generating the certificate's signature, from these options:

- **RSA**—The RSA public-key cryptosystem Secure Hash Algorithm. For more information, see the RSA-SHA1 Signature Suite page at the W3C web site.
- **DSA**—The Digital Signature Algorithm Secure Hash Algorithm. For more information, see the Digital Signature Standard (DSS) page at the US National Institute of Standards and Technology (NIST) web site.

Step 6 Optionally, choose an item from the **Key Size** menu to specify the size of the key to use when generating the certificate's signature:

- **512 bits**—Use a 512-bit key to generate the signature.
- **1024 bits**—Use a 1024-bit key to generate the signature. This is the default value.
- **2048 bits**—Use a 2048-bit key to generate the signature.

Step 7 Optionally, define additional attributes the certificate is to provide:

a. Click the **Add Attribute** button. An **Attribute OID** field and a **Value** field appear in the **Additional Attributes** section.

b. Type into the **Attribute OID** field the name of the additional attribute in OID format.

c. Type into the **Value** field the value of the additional attribute.

d. Repeat the preceding steps as necessary to add all of the attributes required.

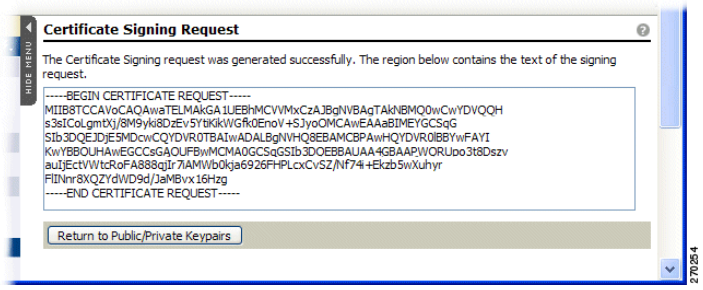
To remove an attribute, click the **Remove** button that appears at the end of its row in the list of custom attributes.

Step 8 When finished entering the information, click the **Generate Request** button.

Using the information you supplied, the ACE Web Application Firewall Manager generates a Certificate Signing Request (CSR) and displays it on the **Certificate Signing Request** page.

The generated request page appears similar to the following.

Figure 11-1 Generated Request Form



Step 9 Copy the CSR data (the part between the `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` strings) into a text file or an email message.

Step 10 Send the CSR data to your preferred CA for transformation into a signed X.509 certificate.

Note When you are submitting a request, the CA may ask you to specify the type of certificate required. The ACE Web Application Firewall works with what are usually identified as Apache-style certificates.

When the signed certificate arrives, install it on the ACE Web Application Firewall as described in the following section.

Uploading a Keypair Resource

A keypair resource is a file that stores a PKI public/private keypair. The ACE Web Application Firewall Manager uses keypair resource files to implement SSL connectivity between it and a browser attempting to access the web console. Service traffic can also be secured by the system public/private keypair.

The **Public/Private Keypairs** page lists all keypair resources in the currently active subpolicy. Entries on this page represent keypair resources that reside on the system in encrypted form.

When the ACE Web Application Firewall Manager compiles and deploys a policy that uses keypair resources, it transmits keypair data to the target Firewalls in a proprietary binary format. The keypair is never in clear-text form.

You can upload a keypair to the ACE Web Application Firewall Manager by itself or as part of a certificate. A certificate resource is a file that the ACE Web Application Firewall Manager uses to store digital certificate data; optionally, the certificate resource can store the certificate's associated keypair data. Like the keypair resource, a certificate resource exists in the policy in encrypted form only.

To upload a keypair resource to the policy in the ACE Web Application Firewall Manager:

Step 1 While logged in to the Manager web console as an Administrator user or a Privileged user with the Routing role, set the active subpolicy to the one that is to use the keypair.

Step 2 Click the **Public/Private Keypairs** link in the navigation menu.

Step 3 Click the **Add a New Public/Private Keypair** button at the top of the page. (Alternatively, use the **Upload Separate Certificate and Key Files** if the certificate and key files are not in the same file.)

The **Upload Public/Private Keypair Resource** page appears. You can also reach this page from the HTTP(S) port settings page.

Step 4 In the **Resource Name** field, type a unique name for the keypair resource. This name identifies the keypair in the ACE Web Application Firewall Manager's user interface.

Step 5 Identify the keypair to use from a filesystem location or from a network location by URL.

Step 6 Type the password for the keypair in the **Password** field. Note that the password is obscured in the field as you type.

Step 7 **Click the Upload** button.

The ACE Web Application Firewall Manager uploads the keypair resource and displays it as a resource in the **Public/Private Keypairs** page. If the resource does not pass a basic validity test—for example, if it does not provides a pair of valid PEM keys—an error message appears in red text on the **Upload Public/Private Keypair Resource** page.

When complete, you can use the keypair when configuring SSL connections in the policy.

Uploading a Certificate Authority Resource

Uploading the certificate of a Certificate Authority (CA) establishes a trust relationship for the ACE Web Application Firewall with that CA. The ACE Web Application Firewall can accept certificates based on the trust status of the CA that signed the certificate. By default, the policy does not include any pre-installed CA certificates; you will need to import the certificates of any CA to be trusted.

You can upload a CA resource to the ACE Web Application Firewall Manager as a file or from a location specified by URL. You can also import the necessary information from an LDAP server. The **Trusted Certificate Authorities** page lists all Certificate Authorities available to the currently active subpolicy. These resources appear as named items in menus on pages that create or edit services requiring digital certificates.

To upload a CA resource file to the ACE Web Application Firewall Manager web console:

Step 1 As an Administrator user or a Privileged user with the Routing role in the console, set the active subpolicy to the one in which you want to use the keypair.

To make the keypair available to all subpolicies, add it to the **Shared** subpolicy.

Step 2 Click the **Trusted Certificate Authorities** link in the **Resources** section of the navigation menu.

Step 3 In the **Trusted Certificate Authorities** page, click the **Add a New Certificate Authority Resource** button, near the top of the page.

The **Upload Certificate Authority Resource** page appears.

Step 4 Type a name for the certificate authority resource in the **Resource Name** field. This is simply a descriptive name for the resource used within the policy.

Step 5 Specify the certificate from either a file system location in the **Local File** field or from a network location, by typing the network address of the resource in the **URL** field.

You can populate the **Local File** field automatically by clicking the **Browse** button, and navigating to the certificate file.

Step 6 Optionally, type a URL for the certificate revocation list in the **CRL URL** field. The ACE Web Application Firewall rejects connections that use certificates that appear in the certificate revocation list.

Leave this field blank to not have the ACE Web Application Firewall check any certificate revocation list.

Step 7 If you configured a certificate revocation list, also specify how often the ACE Web Application Firewall should retrieve the list.

Step 8 When finished, click **Upload** to have the resource uploaded to the ACE Web Application Firewall Manager.

After uploading the CA certificate, you can configure requirements based on this trust relationship. For instance, in the SSL connection settings for an HTTP server, you can require that server certificates be signed by the trusted CA.