CHAPTER 9

Configuring SSL

Note The information in this chapter does not apply to the ACE NPE software version in which payload encryption protocols are removed (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

This chapter describes the steps required to configure your ACE appliance as a virtual Secure Sockets Layer (SSL) server for SSL initiation or termination.

Note When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

The chapter contains the following section:

SSL Overview

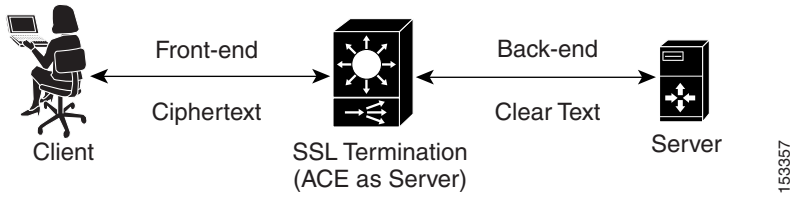
SSL is an application-level protocol that provides encryption technology for the Internet, ensuring secure transactions such as the transmission of credit card numbers for e-commerce Web sites. SSL initiation occurs when the ACE appliance acts as a client and initiates the SSL session between it and the SSL server. SSL termination occurs when the ACE, acting as an SSL server, terminates an SSL connection from a client and then establishes a TCP connection to an HTTP server.

SSL provides the secure transaction of data between a client and a server through a combination of privacy, authentication, and data integrity. SSL relies upon certificates and private-public key exchange pairs for this level of security.

Figure 9-1 shows the following network connections in which the ACE terminates the SSL connection with the client:

- Client to ACE—SSL connection between a client and the ACE acting as an SSL proxy server
- ACE to Server—TCP connection between the ACE and the HTTP server

Figure 9-1 SSL Termination with Client



The ACE uses parameter maps, SSL proxy services, and class maps to build the policy maps that determine the flow of information between the client, the ACE, and the server. SSL termination is a Layer 3 and Layer 4 application because it is based on the destination IP addresses of the inbound traffic flow from the client. For this type of application, you create a Layer 3 and Layer 4 policy map that the ACE applies to the inbound traffic.

If you have a need to delete any of the SSL objects (auth groups, chain groups, parameter maps, keys, CRLs, or certificates), you must remove the dependency from within the proxy service first before removing the SSL object.

Before configuring the ACE for SSL, see SSL Configuration Prerequisites, page 9-3.

SSL Configuration Prerequisites

Before configuring your ACE for SSL operation, you must first ensure:

- Your ACE hardware is configured for server load balancing (SLB).

Note During the real server and server farm configuration process, when you associate a real server with a server farm, ensure that you assign an appropriate port number for the real server. The default behavior by the ACE is to automatically assign the same destination port that was used by the inbound connection to the outbound server connection if you do not specify a port.

- Your policy map is configured to define the SSL session parameters and client/server authentication tools, such as the certificate and RSA key pair.
- Your class map is associated with the policy map to define the virtual SSL server IP address that the destination IP address of the inbound traffic must match.
- You must import a digital certificate and its corresponding public and private key pair to the desired ACE context.
- At least one SSL certificate is available.
- If you do not have a certificate and corresponding key pair, you can generate an RSA key pair and a *certificate signing request* (CSR). Create a CSR when you need to apply for a certificate from a *certificate authority* (CA). The CA signs the CSR and returns the authorized digital certificate to you.

RBAC User Role Requirements for SSL Configurations

For all SSL-related configurations on the ACE, a user with a custom role should include the following two rules as part of the assigned role:

- A rule that includes the SSL feature.
- A rule that includes the PKI feature.

For details on user roles and rules, see the "Creating User Roles" section in Chapter 15, "Managing the ACE Appliance."

Summary of SSL Configuration Steps

Table 9-1 describes the steps for using SSL keys and certificates.

Table 9-1 SSL Key and Certificate Procedure Overview

	Task	Description
Step 1	Create an SSL parameter map.	Create an SSL parameter map to specify the options that apply to SSL sessions such as the method to be used to close SSL connections, the cipher suite, and version of SSL or TLS. See Configuring SSL Parameter Maps, page 9-19.
Step 2	Create an SSL key pair file.	Create an SSL RSA key pair file to generate a CSR, create a digital signature, and encrypt packet data during the SSL handshake with an SSL peer. See Generating SSL Key Pairs, page 9-15.
Step 3	Configure CSR parameters.	Set CSR parameters to define the distinguished name attributes of a CSR. See Configuring SSL CSR Parameters, page 9-26.
Step 4	Create a CSR.	Create a CSR to submit with the key pair file when you apply for an SSL certificate. See Generating CSRs, page 9-27.
Step 5	Copy and paste the CSR into the Certificate Authority (CA) Web-based application or e-mail the CSR to the CA.	Using the SSL key pair and CSR, apply for an approved certificate from a Certificate Authority. Use the method specified by the CA for submitting your request.
Step 6	Save the approved certificate from the CA in its received format on an FTP, SFTP, or TFTP server.	When you receive the approved certificate, save it in the format in which it was received on a network server accessible via FTP, SFTP, or TFTP.
Step 7	Import the approved certificate and key pair into the desired virtual context.	Import the approved certificate and the associated SSL key pair into the appropriate context using ACE Appliance Device Manager. See the following topics: • Importing SSL Certificates, page 9-8 • Importing SSL Key Pairs, page 9-12
Step 8	Confirm that the public key in the key pair file matches the public key in the certificate file.	Examine the contents of the files to confirm that the key pair information is the same in both the key pair file and the certificate file.
Step 9	Configure the virtual context for SSL.	See Configuring Traffic Policies, page 12-1.
Step 10	Configure auth group.	Create a group of certificates that are trusted as certificate signers by creating an authentication group. See Configuring SSL Authentication Groups, page 9-32.

Table 9-1 SSL Key and Certificate Procedure Overview (continued)

	Task	Description
Step 11	Configure CRL.	See Configuring CRLs for Client Authentication, page 9-33.
Step 12	Configure an SSL OCSP service	See Configuring SSL OCSP Service, page 9-30.

For more information about using SSL with ACE appliances, see the *SSL Guide, Cisco ACE Application Control Engine*.

To configure ACE appliances for SSL, see the following topics:

- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL Proxy Service, page 9-28
- Configuring SSL OCSP Service, page 9-30

SSL Setup Sequence

The SSL setup sequence provides detailed instructions with illustrations for configuring SSL using the ACE Appliance Device Manager (Figure 9-2). The purpose of this option is to provide a visual guide for performing typical SSL operations, such as SSL CSR generation, SSL proxy creation, and so on. This option does not replace any existing SSL functions or configuration screens already present in ACE Appliance Device Manager. It is only intended as an additional guide for anyone unfamiliar or unclear with the SSL operations that need to be performed on the ACE. From the SSL setup sequence, you are allowed to configure all SSL operations, without duplicating the edit/delete/table/view operations that the other SSL configuration screens provide.

The purpose of this option is to provide details about typical SSL flows and the operations involved in performing typical SSL operations, including the following:

- SSL import/create keys
- SSL import certificates
- SSL CSR generation
- SSL proxy creation

Note The SSL Setup Sequence in the ACE Device Manager uses the terms *SSL Policies* and *SSL Proxy Service* interchangeably.

For more information on SSL configuration features, see Summary of SSL Configuration Steps.

Figure 9-2 SSL Setup Sequence

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL Proxy Service, page 9-28

Using SSL Certificates

You can display a list of the certificates and their matching key pairs that are installed on the ACE for a context by choosing **Config > Virtual Contexts >** *context* **> Certificates**. The Certificates window appears, displaying the list of installed certificates.

Digital certificates and key pairs are a form of digital identification for user authentication. Certificate Authorities issue certificates that attest to the validity of the public keys they contain. A client or server certificate includes the following identification attributes:

- Name of the Certificate Authority and Certificate Authority digital signature
- Name of the client or server (the certificate subject) that the certificate authenticates
- Issuer
- Serial number
- Subject's matching public key of the certificate
- Time stamps that indicate the certificate's start date and expiration date
- CA certificate

A Certificate Authority has one or more signing certificates that it uses for creating SSL certificates and certificate revocation lists (CRL). Each signing certificate has a matching private key that is used to create the Certificate Authority signature. The Certificate Authority makes the signing certificates (with the public key embedded) available to the public, enabling anyone to access and use the signing certificates to verify that an SSL certificate or CRL was actually signed by a specific Certificate Authority.

Note The ACE supports the creation of a maximum of eight CRLs for any context.

ACE appliances require certificates and corresponding key pairs for:

- SSL termination—The ACE appliance acts as an SSL proxy server and terminates the SSL session between it and the client. For SSL termination, you must obtain a server certificate and corresponding key pair.
- SSL initiation—The ACE appliance acts as a client and initiates the SSL session between it and the SSL server. For SSL initiation, you must obtain a client certificate and corresponding key pair.

The Matching Key column in the Certificates window (Config > Virtual Contexts > context > Certificates) displays the name of a key pair that ACE Appliance Device Manager was able to match up with certificate. If ACE Appliance Device Manager cannot detect a matching key pair for a certificate, it leaves the Matching Key table cell blank. If the number of unmatched certificates and key pairs exceeds 50, then ACE Appliance Device Manager leaves the entire Matching Key column blank, even when matching certificates and key pairs exist for the context. When this condition occurs, you can verify that a certificate and key pair match by using the SSL Setup Sequence feature.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Setup Sequence**.

The Setup Sequence window appears.

Step 2 In the Setup Sequence window, click **Configure SSL Polices**.

The Configure SSL Policies window appears.

Step 3 From the Certificate drop-down list in the Configure SSL Policies - Basic Settings section, choose a certificate.

Step 4 From the Keys drop-down list in the Configure SSL Policies - Basic Settings section, choose a key pair.

Step 5 Click **Verify Key**.

ACE Appliance Device Manager checks to see if the selected certificate and key pair match. A popup window appears to indicate if the two items match.

Note The ACE includes a preinstalled sample certificate and corresponding key pair. The certificate is for demonstration purposes only and does not have a valid domain. It is a self-signed certificate with basic extensions named *cisco-sample-cert.* The key pair is an RSA 1024-bit key pair named *cisco-sample-key.*

You can display the sample certificate and corresponding key pair files as follows:

- To display the cisco-sample-cert file, choose **Config** > **Virtual Contexts** > *context* > **SSL** > **Certificates**.
- To display the cisco-sample-key file, choose **Config** > **Virtual Contexts** > *context* > **SSL** > **Keys**.

You can add these files to an SSL-proxy service (see the "Configuring SSL Proxy Service" section on page 9-28) and are available for use in any context with the filenames remaining the same in each context.

The ACE allows you to export these files but does not allow you to import any files with these names. When you upgrade the ACE software, these files are overwritten with the files provided in the upgrade image. You cannot use the **crypto delete** CLI command to delete these files unless you downgrade the ACE software because a software downgrade preserves these files as if they were user-installed SSL files.

Related Topics

- Configuring SSL, page 9-1
- Exporting SSL Certificates, page 9-16
- Importing SSL Certificates, page 9-8
- Using SSL Keys, page 9-11
- Importing SSL Key Pairs, page 9-12
- Configuring SSL CSR Parameters, page 9-26
- Generating CSRs, page 9-27

Importing SSL Certificates

Use this procedure to import SSL certificates.

Note The ACE supports a maximum of 4,096 certificates.

Assumptions

- You have configured an ACE appliance for server load balancing. (See Load Balancing Overview, page 5-1.)
- You have obtained an SSL certificate from a certificate authority (CA) and have placed it on a network server accessible by the ACE appliance.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Certificates**. The Certificates table appears, listing any valid SSL certificates.

The cisco-sample-cert certificate is included in the list. For information on this sample certificate, see the "Using SSL Certificates" section on page 9-6.

Step 2 Click **Import**. The Import dialog box appears.

To import multiple SSL certificates, click **Bulk Import**. The Bulk Import dialog box appears.

Note SSL bulk import can take longer based on the number of SSL certificates being imported. It will progress to completion on the ACE. To see the imported certificates in the ACE Device Manager, perform a CLI synchronization for this context once the SSL bulk import has completed. For information on synchronizing contexts, see the "Synchronizing Virtual Context Configurations" section on page 4-79.

Step 3 Enter the applicable information:

- For the Import dialog box, see Table 9-2.
- For the Bulk Import dialog box, see Table 9-3.

Table 9-2 SSL Certificate Management Import Attributes

Field	Description
Protocol	Specify the method to be used for accessing the network server: • FTP—Indicates that FTP is to be used to access the network server when importing the SSL certificate. • SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL certificate. • TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL certificate. • TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IPv4 address of the remote server on which the SSL certificate file resides.
Remote File Name	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename of the certificate file on the network server.
Local File Name	Enter the filename to be used for the SSL certificate file when it is imported to the ACE appliance.
User Name	This field appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.
Passphrase	This field appears for FTP, TFTP, SFTP, and TERMINAL. Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.

Table 9-2 SSL Certificate Management Import Attributes (continued)

Field	Description
Confirm	This field appears for FTP, SFTP, and TERMINAL. Reenter the passphrase.
Non-Exportable	The ability to export SSL certificates allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting is similar to copying in that the original files are not deleted. Check the check box to indicate that this certificate file cannot be exported from the ACE appliance.
Import Text	This field appears for Terminal. Cut the certificate information from the remote server and paste it into this field.

Table 9-3 SSL Certificate Management Bulk Import Attributes

Field	Description
Protocol	SFTP is to be used to access the network server when importing the SSL certificates. SFTP is the only supported protocol for bulk import.
IP Address	Enter the IPv4 address of the remote server on which the SSL certificate files reside.
Remote Path	Path to the SSL certificate files that reside on the remote server. The ACE fetches only files specified by the path; it does not recursively fetch remote directories. Enter a filename path including wildcards (for example, /remote/path/*.pem). The ACE supports POSIX pattern matching notation, as specified in section 2.13 of the "Shell and Utilities" volume of IEEE Std 1003.1-2004. This notation includes the "*," "?" and "[" metacharacters. To fetch all files from a remote directory, specify a remote path that ends with a wildcard character (for example, /remote/path/*). Do not include spaces or the following special characters: ;<>|`@$&() The ACE fetches all files on the remote server that matches the wildcard criteria. However, it imports only files with names that have a maximum of 40 characters. If the name of a file exceeds 40 characters, the ACE does not import the file and discards it.
User Name	Enter the name of the user account on the network server.
Password	Enter the password for the user account on the network server.
Confirm	Reenter the password.
Passphrase	Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.
Confirm	Reenter the passphrase.
Non-Exportable	The ability to export SSL certificates allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted. Check the check box to specify that this certificate file cannot be exported from the ACE.

Step 4 Do the following:

- Click **OK** to accept your entries and to return to the Certificates table. The ACE Appliance Device Manager updates the Certificates table with the newly installed certificate.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Certificates table.

Related Topics

- Configuring SSL, page 9-1
- Using SSL Keys, page 9-11
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Using SSL Keys

An ACE appliance and its peer use a public key cryptographic system named Rivest, Shamir, and Adelman Signatures (RSA) for authentication during the SSL handshake to establish an SSL session. The RSA system uses *key pairs* that consist of a public key and a corresponding private (secret) key. During the handshake, the RSA key pairs encrypt the session key that both devices will use to encrypt the data that follows the handshake.

Use this procedure to view options for working with SSL and SSL keys.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Keys**. The Keys table appears.

Step 2 Continue with one of the following options:

- Generate a key pair—See Generating SSL Key Pairs, page 9-15.
- Import a key pair—See Importing SSL Key Pairs, page 9-12.
- Export a key pair—See Exporting SSL Key Pairs, page 9-18.
- Generate a CSR—See Generating CSRs, page 9-27.

Related Topics

- Generating SSL Key Pairs, page 9-15
- Importing SSL Key Pairs, page 9-12
- Generating SSL Key Pairs, page 9-15
- Exporting SSL Key Pairs, page 9-18
- Configuring SSL, page 9-1

Importing SSL Key Pairs

Use this procedure to import an SSL key pair file.

Note The ACE supports a maximum of 4,096 key pairs.

Assumptions

- You have configured an ACE appliance for server load balancing. (See Load Balancing Overview, page 5-1.)
- You have obtained an SSL key pair from a certificate authority (CA) and have placed the pair on a network server accessible by the ACE appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Keys**. The Keys table appears, listing existing SSL keys.

The cisco-sample-key key pair is included in the list. For information on this sample key pair, see the "Using SSL Certificates" section on page 9-6.

Step 2 Click **Import**. The Import dialog box appears.

To import multiple SSL key pairs, click **Bulk Import**. The Bulk Import dialog box appears.

Note SSL bulk import can take longer based on the number of SSL keys being imported. It will progress to completion on the ACE. To see the imported keys in the ACE Device Manager, perform a CLI synchronization for this *context* once the SSL bulk import has completed. For information on synchronizing contexts, see the "Synchronizing Virtual Context Configurations" section on page 4-79.

Step 3 Enter the applicable information as follows:

- For the Import dialog box, see Table 9-4.
- For the Bulk Import dialog box, see Table 9-5.

Table 9-4 SSL Key Pair Import Attributes

Field	Description
Protocol	Specify the method to be used for accessing the network server: • FTP—Indicates that FTP is to be used to access the network server when importing the SSL key pair file. • SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL key pair file. • TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL key pair file. • TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate and key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IPv4 address of the remote server on which the SSL key pair file resides.
Remote File Name	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename of the key pair file on the network server.
Local File Name	Enter the filename to be used for the SSL key pair file when it is imported to the ACE appliance.
User Name	This field appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.
Passphrase	This field appears for FTP, TFTP, SFTP, and TERMINAL. Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.
Confirm	This field appears for FTP, SFTP, and TERMINAL. Reenter the passphrase.
Non-Exportable	The ability to export SSL key pair files allows you to copy key pair files to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting is similar to copying in that the original files are not deleted. Check the check box to indicate that this key pair file cannot be exported from the ACE appliance. Clear the check box to indicate that this key pair file can be exported from the ACE appliance.
Import Text	This field appears for Terminal. Cut the key pair information from the remote server and paste it into this field.

Table 9-5 SSL Key Pair Bulk Import Attributes

Field	Description
Protocol	SFTP is to be used to access the network server when importing the SSL key pairs. SFTP is the only supported protocol for bulk import.
IP Address	Enter the IPv4 address of the remote server on which the SSL key pair files resides.
Remote Path	Enter the path to the key pair files that reside on the remote server. The ACE fetches only files specified by the path; it does not recursively fetch remote directories. Enter a filename path including wildcards (for example, /remote/path/*.pem). The ACE supports POSIX pattern matching notation, as specified in section 2.13 of the "Shell and Utilities" volume of IEEE Std 1003.1-2004. This notation includes the "*," "?" and "[" metacharacters. To fetch all files from a remote directory, specify a remote path that ends with a wildcard character (for example, /remote/path/*). Do not include spaces or the following special characters: ;<>|`@$&() The ACE fetches all files on the remote server that matches the wildcard criteria. However, it imports only files with names that have a maximum of 40 characters. If the name of a file exceeds 40 characters, the ACE does not import the file and discards it.
User Name	Enter the name of the user account on the network server.
Password	Enter the password for the user account on the network server.
Confirm	Reenter the password.
Passphrase	Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.
Confirm	Reenter the passphrase.
Non-Exportable	Check this check box to specify that this certificate file cannot be exported from the ACE. The ability to export SSL key pairs allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted.

Step 4 Do the following:

- Click **OK** to accept your entries and to return to the Keys table. The ACE Appliance Device Manager updates the Keys table with the imported key pair file information.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Keys table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Configuring SSL Parameter Maps, page 9-19

- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Generating SSL Key Pairs

If you do not have any matching key pairs, you can use the ACE appliance to generate a key pair.

Use this procedure to generate SSL RSA key pairs.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Keys**. The Keys table appears.

Step 2 Click **Add** to add a new key pair. The Keys configuration screen appears.

Note You cannot modify an existing entry in the Keys table. Instead, delete the existing entry, and then add a new one.

Step 3 In the Name field, enter the name of the SSL key pair. Valid entries are alphanumeric strings with a maximum of 40 characters.

Step 4 In the Size field, select the key pair security strength. The number of bits in the key pair file defines the size of the RSA key pair used to secure Web transactions. Longer keys produce more secure implementations by increasing the strength of the RSA security policy. Options and their relative levels of security are as follows:

- 512—Least security
- 768—Normal security
- 1024—High security, level 1
- 1536—High security, level 2
- 2048—High security, level 3
- 4096—High security, level 4

Step 5 In the Type field, specify **RSA** as the public-key cryptographic system used for authentication.

Step 6 In the Exportable Key field, check the check box to indicate that the key pair file can be exported. Clear the check box to indicate that the key pair file cannot be exported.

Step 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Keys table.
- Click **Next** to save your entries and to define another RSA key pair.

After generating an RSA key pair, you can:

- Create a CSR parameter set. The CSR parameter set defines the distinguished name attributes for the ACE appliance to use during the CSR-generating process. For details on defining a CSR parameter set, see the Configuring SSL CSR Parameters, page 9-26.
- Generate a CSR for the RSA key pair file and transfer the CSR request to the certificate authority for signing. This provides an added layer of security because the RSA private key originates directly within the ACE appliance and does not have to be transported externally. Each generated key pair must be accompanied by a corresponding certificate to work. For details on generating a CSR, see Generating CSRs, page 9-27.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Exporting SSL Certificates

The ability to export SSL certificates allows you copy signed certificates to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting certificates is similar to copying in that the original certificates are not deleted.

Use this procedure to export SSL certificates from an ACE appliance to a remote server.

Assumption

- The SSL certificate can be exported. (See Importing SSL Certificates, page 9-8.)
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Certificates**. The Certificates table appears, listing any valid SSL certificates.

Step 2 Select the certificate you want to export, and then click **Export**. The Export dialog box appears.

Step 3 Enter the information in Table 9-6.

Table 9-6 SSL Certificate Export Attributes

Field	Description
Protocol	Specify the method to be used for exporting the SSL certificate: • FTP—Indicates that FTP is to be used to access the network server when exporting the SSL certificate. • SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL certificate. • TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL certificate. • TERMINAL—Indicates that you will export the certificate using cut and paste by pasting the certificate and key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IPv4 address of the remote server to which the SSL certificate file is to be exported.
Remote File Name	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename to be used for the SSL certificate file on the remote network server.
User Name	This field appears for FTP and SFTP. Enter the name of the user account on the remote network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the remote network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.

Step 4 Do the following:

- Click **OK** to export the certificate and to return to the Certificates table.
- Click **Cancel** to exit this procedure without exporting the certificate and to return to the Certificates table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Generating SSL Key Pairs, page 9-15
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Exporting SSL Key Pairs

The ability to export SSL key pairs allows you copy SSL key pair files to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting key pair files is similar to copying in that the original key pairs are not deleted.

Use this procedure to export SSL key pairs from an ACE appliance to a remote server.

Assumption

The SSL key pair can be exported (see Generating SSL Key Pairs, page 9-15).

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Keys**. The Keys table appears.

Step 2 Select the key entry you want to export, and then click **Export**. The Export dialog box appears.

Step 3 Enter the information in Table 9-7.

Table 9-7 SSL Key Export Attributes

Field	Description
Protocol	Specify the method to be used for exporting the SSL key pair: • FTP—Indicates that FTP is to be used to access the network server when exporting the SSL key pair. • SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL key pair. • TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL key pair. • TERMINAL—Indicates that you will export the key pair using cut and paste by pasting the key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IPv4 address of the remote server to which the SSL key pair is to be exported.
Remote File Name	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename to be used for the SSL key pair file on the remote network server.
User Name	This field appears for FTP and SFTP. Enter the name of the user account on the remote network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the remote network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.

Step 4 Do the following:

- Click **OK** to export the key pair and to return to the Keys table.
- Click **Cancel** to exit this procedure without exporting the key pair and to return to the Keys table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Generating SSL Key Pairs, page 9-15
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Configuring SSL Parameter Maps

An SSL parameter map defines the SSL session parameters that an ACE appliance applies to an SSL proxy service. SSL parameter maps let you apply the same SSL session parameters to different proxy services.

Use this procedure to create SSL parameter maps.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Parameter Maps**. The Parameter Maps table appears.

Step 2 Click **Add** to add a new SSL parameter map, or select an existing entry to modify, and then click **Edit**. The Parameter Map configuration screen appears.

Step 3 In the Parameter Map Name field, enter a unique name for the parameter map. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 In the Description field, enter a brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Enter double quotes as matching pairs.

Step 5 In the Queue Delay Timeout (Milliseconds) field, set the amount of time (in milliseconds) to wait before emptying the queued data for encryption. The default delay is 200 milliseconds, and can be adjusted from 0 (disabled) to 10000. If disabled (set to 0), the ACE encrypts the data from the server as soon as it arrives and then sends the encrypted data to the client.

Note The Queue Delay Timeout is only applied to data that the SSL module sends to the client. This avoids a potentially long delay in passing a small HTTP GET to the real server.

Step 6 In the Session Cache Timeout (Milliseconds) field, specify a timeout value of an SSL session ID to remain valid before the ACE requires the full SSL handshake to establish a new SSL session. This value allows the ACE to reuse the master key on subsequent connections with the client, which can speed up

the SSL negotiation process.The default value is 300 seconds (5 minutes), and can be adjusted from 0 (to indicate an infinite timeout, so that session IDs are removed from the cache only when the cache becomes full), up to 72000 seconds (20 hours). Specifying 0 causes the ACE to implement a least recently used (LRU) timeout policy. By disabling this option, the full SSL handshake occurs for each new connection with the ACE.

Step 7 In the Reject Expired CRLs field, click the check box to specify whether expired CRLs can be used. If checked, no expired CRLs are allowed.

Step 8 In the Close Protocol Behavior field, select the method to be used to close the SSL connection:

- Disabled—Indicates that the ACE appliance is to send a close-notify alert message to the SSL peer; however, the SSL peer does not expect a close-notify alert before removing the session. Whether the SSL peer sends a close-notify alert message or not, the session information is preserved, allowing session resumption for future SSL connections.
- None—Indicates that the ACE appliance is not to send a close-notify alert message to the SSL peer, nor does the ACE appliance expect a close-notify alert message from the peer. The ACE appliance preserves the session information so that SSL resumption can be used for future SSL connections.

Step 9 In the SSL Version field, enter the version of SSL be to used during SSL communications:

- All—Indicates that the ACE appliance is to use both SSL v3 and TLS v1 in its communications with peer ACE appliances.
- SSL3—Indicates that the ACE appliance is to use only SSL v3 in its communications with peer ACE appliances.
- TLS1—Indicates that the ACE appliance is to use only TLS v1 in its communications with peer ACE appliances.
- TLS1_1—Indicates that the ACE appliance is to use only TLS Version 1.1 in its communication with peer ACE appliances.
- TLS1_2—Indicates that the ACE appliance is to use only TLS Version 1.2 in its communication with peer ACE appliances.
- Upto_TLS1_1—Indicates all SSL versions upto TLS 1.1.
- Upto_TLS1_2—Indicates all SSL versions upto TLS 1.2.

Note For TLS1_1 and TLS1_2 SSL versions, only certain ‘Ciphers’ are supported as mentioned in the tables below. If the user tries to configure any unsupported SSL version or unsupported Cipher, an error message will be displayed.

Folowing tables shows the list of supported cipher suites for TLS1_1 and TLS1_2 in ACE”

Table 9-8 Cipher suites supported by TLS 1.1

Cipher Suite Name	Cipher Suite Number
RSA_WITH_RC4_128_MD5	{ 0x00,0x04 }
RSA_WITH_RC4_128_SHA	{ 0x00,0x05 }
RSA_WITH_DES_CBC_SHA	{ 0x00,0x09 }
RSA_WITH_3DES_EDE_CBC_SHA	{ 0x00,0x0A }
RSA_WITH_AES_128_CBC_SHA	{ 0x00,0x2F }
RSA_WITH_AES_256_CBC_SHA	{ 0x00,0x35 }

Table 9-9

Table 9-10 Cipher suites supported by TLS 1.2

Cipher Suite Name	Cipher Suite Number
RSA_WITH_RC4_128_MD5	{ 0x00,0x04 }
RSA_WITH_RC4_128_SHA	{ 0x00,0x05 }
RSA_WITH_3DES_EDE_CBC_SHA	{ 0x00,0x0A }
RSA_WITH_AES_128_CBC_SHA	{ 0x00,0x2F }
RSA_WITH_AES_256_CBC_SHA	{ 0x00,0x35 }

Step 10 In the Ignore Authentication Failure field, check the check box to ignore expired or invalid client or server certificates and to continue setting up the SSL connection. Clear the check box to return to the default setting of disabled. This field allows the ACE appliance to ignore the following nonfatal errors with respect to either client certificates for SSL termination configurations, or server certificates for SSL initiation configurations:

- Certificate not yet valid (both)
- Certificate has expired (both)
- Certificate revoked (both)
- Unknown issuer (both)
- No client certificate (client certificate only)
- CRL not available (client certificate only)
- CRL has expired (client certificate only)
- Certificate has signature failure (client certificate only)
- Certificate other error (client certificate only)

Step 11 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The updated Parameter Map screen appears along with the Parameter Map Cipher table. Continue with Step 12.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Parameter Map table.
- Click **Next** to save your entries and to define another parameter map.

Step 12 In the Parameter Map Cipher table, click **Add** to add a cipher, or select an existing cipher, and then click **Edit**. The Parameter Map Cipher configuration screen appears.

Enter the information in Table 9-11.

Table 9-11 SSL Parameter Map Cipher Configuration Attributes

Field	Description
Cipher Name	Cipher to use. For more information on the SSL cipher suites that ACE supports, see *SSL Guide, Cisco ACE Application Control Engine*.
Cipher Priority	Priority that you want to assign to this cipher suite. The priority indicates the cipher's preference for use. Valid entries are from 1 to 10 with 1 indicating the least preferred and 10 indicating the most preferred. When determining which cipher suite to use, the ACE chooses the cipher suite with the highest priority.

Step 13 In the Parameter Map Cipher table, do one of the following:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map Cipher table.
- **Next** to save your entries and to add another entry to the Parameter Map Cipher table.

Step 14 Click the **Redirect Authentication Failure** tab and click **Add** to add a redirect or choose an existing redirect, and click **Edit**.

Enter the information in Table 9-12.

Note The Redirect Authentication Failure feature is only for SSL termination configurations in which the ACE performs client authentication. The ACE ignores these attributes if you configure them for an SSL initiation configuration.

Table 9-12 SSL Parameter Map Redirect Configuration Attributes

Field	Description
Client Certificate Validation	Select the type of certificate validation failure to redirect. From the drop-down list, choose the type to redirect: • Any—Associates any of the certificate failures with the redirect. You can configure the authentication-failure redirect any command with individual reasons for redirection. When you do, the ACE attempts to match one of the individual reasons before using the any reason. You cannot configure the authentication-failure redirect any command with the authentication-failure ignore command. • Cert-expired—Associates an expired certificate failure with a redirect. • Cert-has-signature-failure—Associates a certificate signature failure with a redirect. • Cert-not-yet-valid—Associates a certificate that is not yet valid failure with the redirect. • Cert-other-error—Associates a all other certificate failures with a redirect. • Cert-revoked—Associates a revoked certificate failure with a redirect. • CRL-has-expired—Associates an expired CRL failure with a redirect. • CRL-not-available—Associates a CRL that is not available failure with a redirect. • No-client-cert—Associates no client certificate failure with a redirect. • Unknown-issuer—Associates an unknown issuer certificate failure with a redirect.
Redirect Type	Select the redirect type to use: • Server Farm—Specifies a server farm for the redirect. • URL—Specifies a static URL path for the redirect.
Server Farm Name	This field appears when the Redirect Type is set to Server Farm. The ACE Device Manager displays all configured host and redirect server farms. Choose one of the available server farm options or click **Plus** (+) to open the server farm configuration popup and configure a redirect server farm (see the "Configuring Server Farms" section on page 6-18).
Redirect URL	This field appears when the Redirect Type is set to URL. Enter the static URL path for the redirect. Enter a string with a maximum of 255 characters and no spaces.
Redirect Code	This field appears when the Redirect Type is set to URL. Enter the redirect code that is sent back to the client: • 301—Status code for a resource permanently moving to a new location. • 302—Status code for a resource temporarily moving to a new location.

Step 15 In the Redirect Authentication Failure table, do one of the following:

- Click **Deploy Now** to deploy the Redirect Authentication Failure table on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Redirect Authentication Failure table.
- Click **Next** to deploy your entries and to add another entry to the Redirect Authentication Failure table.

Step 16 In the Parameter Map table, do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map table.
- Click **Next** to deploy your entries and to add another entry to the Parameter Map table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Generating SSL Key Pairs, page 9-15
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Configuring SSL Chain Group Parameters

A chain group specifies the *certificate chains* that the ACE appliance sends to its peer during the handshake process. A certificate chain is a hierarchal list of certificates that includes the ACE appliance's certificate, the root certificate authority certificate, and any intermediate certificate authority certificates. Using the information provided in a certificate chain, the certificate verifier searches for a trusted authority in the certificate hierarchal list up to and including the root certificate authority. If the verifier finds a trusted authority before reaching the root certificate authority certificate, it stops searching further.

Use this procedure to configure certificate chains for a virtual context.

Assumption

At least one SSL certificate is available.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Chain Group Parameters**. The Chain Group Parameters table appears.

Step 2 Click **Add** to add a new chain group, or select an existing chain group, and then click **Edit** to modify it. The Chain Group Parameters configuration screen appears.

Step 3 In the Name field, enter a unique name for the chain group. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The updated Chain Group Parameters screen appears along with the Chain Group Certificates table. Continue with Step 5.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Parameters table.
- Click **Next** to save your entries and to add another entry to the Chain Group Parameters table.

Step 5 In the Chain Group Certificates table, click **Add** to add an entry. The Chain Group Certificates configuration screen appears.

Note You cannot modify an existing entry in the Chain Group Certificates table. Instead, delete the entry, and then add a new one.

Step 6 In the Certificate Name field, select the certificate to add to this chain group.

Step 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Certificates table.
- Click **Next** to save your entries and to add another certificate to this chain group table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Generating SSL Key Pairs, page 9-15
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL Proxy Service, page 9-28

Configuring SSL CSR Parameters

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. The CSR contains information that identifies the SSL site, such as location and a serial number, and a public key that you choose. A corresponding private key is not included in the CSR, but is used to digitally sign the request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for more information.

If the request is successful, the certificate authority returns a digitally signed (with the private key of the certificate authority) identity certificate.

CSR parameters define the *distinguished name* attributes the ACE appliance applies to the CSR during the CSR-generating process. These attributes provide the certificate authority with the information it needs to authenticate your site. Defining a CSR parameter set lets you to generate multiple CSRs with the same distinguished name attributes.

Each context on an ACE appliance can contain up to eight CSR parameter sets.

Use this procedure to define the distinguished name attributes for SSL CSRs.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > CSR Parameters**. The CSR Parameters table appears.

Step 2 Click **Add** to add new set of CSR attributes, or select an existing entry to modify, and then click **Edit**. The CSR Parameters configuration screen appears.

Step 3 In the Name field, enter a unique name for this parameter set. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 In the Country field, enter the name of the country where the SSL site resides. Valid entries are 2 alphabetic characters representing the country, such as *US* for the United States. The International Organization for Standardization (ISO) maintains the complete list of valid country codes on its Web site (www.iso.org).

Step 5 In the State field, enter the name of the state or province where the SSL site resides.

Step 6 In the Locality field, enter the name of the city where the SSL site resides.

Step 7 In the Common Name field, enter the name of the domain or host of the SSL site. Valid entries are alphanumeric strings with a maximum of 64 characters. The ACE supports the following special characters: , . / = + - ^ @ ! % ~ # $ * ( ).

Step 8 In the Serial Number field, enter a serial number to assign to the certificate. Valid entries are alphanumeric strings with a maximum of 16 characters.

Step 9 In the Organization Name field, enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 10 In the Email field, enter the site e-mail address. Valid entries are alphanumeric strings with a maximum of 40 characters.

Step 11 In the Organization Unit field, enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 12 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the CSR Parameters table.
- Click **Next** to save your entries and to define another set of CSR attributes.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL Proxy Service, page 9-28

Generating CSRs

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. Create a CSR when you need to apply for a certificate from a certificate authority. When the certificate authority approves a request, it signs the CSR and returns the authorized digital certificate to you. This certificate includes the private key of the certificate authority. When you receive the authorized certificate and key pair, you can import them for use (see Importing SSL Certificates, page 9-8 and Importing SSL Key Pairs, page 9-12).

Use this procedure to generate SSL CSRs.

Assumption

- You have configured SSL CSR parameters (see Configuring SSL CSR Parameters, page 9-26).
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Keys**. The Keys table appears.

Step 2 Select a key in the table, and then click **Generate CSR**. The Generate a Certificate Signing Request dialog box appears.

Step 3 In the CSR Parameter field, select the CSR parameter to be used.

Step 4 Do the following:

- Click **OK** to generate the CSR. The CSR appears in a popup window which you can now submit to a certificate authority for approval. Work with your certificate authority to determine the method of submission, such as e-mail or a Web-based application. Click **Close** to close the popup window and to return to the Keys table.
- Click **Cancel** to exit this procedure without generating the CSR and to return to the Keys table.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL Proxy Service, page 9-28

Configuring SSL Proxy Service

SSL proxy service defines the SSL parameter map, key pair, certificate, and chain group an ACE appliance uses during SSL handshakes. By configuring an SSL proxy *server* service on an ACE appliance, the ACE appliance can act as an SSL server.

Use this procedure to define the attributes that the ACE appliance is to use during SSL handshakes so that it can act as an SSL server.

Assumption

You have configured at least one SSL key pair, certificate, chain group, or parameter map to apply to this proxy service.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Proxy Service**. The Proxy Service table appears.

Step 2 Click **Add** to add a new proxy service, or select an existing service, and then click **Edit** to modify it. The Proxy Service configuration screen appears.

Step 3 In the Name field, enter a unique name for this proxy service. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 In the Keys field, select the key pair that the ACE appliance is to use during the SSL handshake for data encryption.

Caution When choosing the key pair from the drop-down list, be sure to choose the keys that correspond to the certificate that you choose.

Note If you use SSL Setup Sequence to create the proxy service, ACE appliance Device Manager selects the keys that correspond to the certificate that you choose. If ACE appliance Device Manager cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ACE appliance Device Manager verify that the keys correspond to the selected certificate. ACE appliance Device Manager displays a message to let you know that your key pair selection either matches or does not match the selected certificate. For more information about SSL Setup Sequence, see the "SSL Setup Sequence" section on page 9-5.

The **cisco-sample-key** option is available for the sample key pair. For information about this sample key pair, see the "Using SSL Certificates" section on page 9-6.

Step 5 In the Certificates field, select the certificate that the ACE appliance is to use during the SSL handshake to prove its identity.

Caution When choosing the certificate from the drop-down list, be sure to choose the certificate that corresponds to the keys that you choose.

Note If you use SSL Setup Sequence to create the proxy service, ACE appliance Device Manager selects the keys that correspond to the certificate that you choose. If ACE appliance Device Manager cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ACE appliance Device Manager verify that the keys correspond to the selected certificate. ACE appliance Device Manager displays a message to let you know that your key pair selection either matches or does not match the selected certificate. For more information about SSL Setup Sequence, see the "SSL Setup Sequence" section on page 9-5.

The **cisco-sample-cert** option is available for the sample certificate. For information on this sample certificate, see the "Using SSL Certificates" section on page 9-6.

Step 6 In the Chain Groups field, select the chain group that the ACE appliance is to use during the SSL handshake.

Step 7 For the Auth Groups field, perform either of the following:

- Select N/A when authentication is not applicable for this proxy service. Then, proceed to Step 11.
- Select the auth group name that the ACE is to use during the SSL handshake. To create an auth group, see Configuring SSL Authentication Groups, page 9-32.

Step 8 Check the CRL Best-Effort check box to allow the ACE appliance to search client certificates for the service to determine if it contains a CRL in the extension. The ACE appliance then retrieves the value, if it exists.

Clear the check box to display the CRL name field to select the CRL name.

Step 9 For the CRL Name field, perform either of the following:

- Select N/A when the CRL name is not applicable.
- Select the CRL name that the ACE used for authentication.

Step 10 Check the OCSP Best-Effort check box to allow the ACE appliance to extract the extension to find the OCSP server information from the certificate itself where, from the revocation status, information about the certificate could be obtained. If this extension is missing from the certificate and the best effort OCSP server information is configured with the SSL proxy, the cert is considered revoked.

Clear the check box to display the OCSP server field to select the available OCSP server.

Step 11 In the Parameter Maps field, select the SSL parameter map to associate with this SSL proxy server service.

Step 12 For the Revcheck priority order, select one of the following to set the priority for the revocation check:

- N/A—Indicates that this field is not applicable.
- CRL-OCSP—The ACE uses the CRLs first to determine the revocation status, and then the OCSP servers.
- OCSP-CRL—The ACE uses the OCSP servers first to determine the revocation status, and then the CRLs.

Step 13 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Proxy Service table.
- Click **Next** to save your entries and to add another proxy service.

Related Topics

- Configuring SSL, page 9-1
- Importing SSL Certificates, page 9-8
- Importing SSL Key Pairs, page 9-12
- Configuring SSL Parameter Maps, page 9-19
- Configuring SSL Chain Group Parameters, page 9-25
- Configuring SSL CSR Parameters, page 9-26
- Configuring SSL OCSP Service, page 9-30

Configuring SSL OCSP Service

SSL Online Certificate Status Protocol (OCSP) service defines the host server for certificate revocation checks using OCSP. The OCSP server, also known as the OCSP responder, maintains or obtains the information about the certificates issued by different CAs that are revoked and possibly non-revoked, and provides this information when requested by OCSP clients. OCSP can provide latest information about the revocation status of the certificate. Use of OCSP removes the need to download and cache the CRLs which could be very large in sizes and impose large memory requirements on systems.

You can configure a maximum of 64 OCSP server configurations system-wide on the ACE. You can configure all of these servers in a single or multiple contexts.

Use this procedure to define the attributes that the ACE appliance is to use during SSL handshakes so that it can act as an SSL server.

Assumption

Configure OCSP on an associated proxy service.

You can configure both OCSP and CRLs for authentication.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > OCSP Service**. The OCSP Service table appears.

Step 2 Click **Add** to add a new OCSP service, or select an existing service, and then click **Edit** to modify it. The OCSP Service configuration screen appears.

Step 3 In the Name field, enter a unique name for this OCSP service. Valid entries are alphanumeric strings with a maximum of 64 characters. This name is used when you apply this configuration to an SSL proxy service.

Step 4 In the URL field, enter an HTTP based URL for the OCSP host name and optional port ID in the form of http://*ocsp_hostname*.com:*port_id*. If you do not specify a port ID, the ACE uses the default value of 2560.

Step 5 Optionally, in the Request Signer's Certificate field, you can select a file name for the signer certificate to sign the requests to the server. By default, the request is not signed.

Step 6 Optionally, in the Response Signer's Certificate field, you can select a file name for the signer certificate to verify the signature on the server responses. By default, the responses are not verified.

Step 7 Check the Enable Nonce check box to enable the inclusion of the nonce in the requests to the server. By default, nonce is disabled (unchecked).

Clear the check box to disable the inclusion of the nonce in requests to the server.

Step 8 In the TCP Connection Inactivity Timeout field, enter an integer from 2 to 3600 to specify the TCP connection inactivity timeout in seconds. The default is 300 seconds.

Step 9 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the OCSP Service table.
- Click **Next** to save your entries and to add another proxy service.

Related Topics

- Configuring SSL, page 9-1
- Configuring SSL Proxy Service, page 9-28

Enabling Client Authentication

During the flow of a normal SSL handshake, the SSL server sends its certificate to the client. Then the client verifies the identity of the server through the certificate. However, the client does not send any identification of its own to the server. When you enable the client authentication feature enabled on the ACE, it will require that the client send a certificate to the server. Then the server verifies the following information on the certificate:

- A recognized CA issued the certificate.
- The valid period of the certificate is still in effect.
- The certificate signature is valid and not tampered.
- The CA has not revoked the certificate.

- At least one SSL certificate is available.

Use the following procedures to enable or disable client authentication:

- Configuring SSL Proxy Service, page 9-28
- Configuring SSL Authentication Groups, page 9-32
- Configuring CRLs for Client Authentication, page 9-33

Configuring SSL Authentication Groups

On the ACE, you can implement a group of certificates that are trusted as certificate signers by creating an authentication group. After creating the authentication group and assigning its certificates, then you can assign the authentication group to a proxy service in an SSL termination configuration to enable client authentication. For information on client authentication, see Enabling Client Authentication, page 9-31.

For information on server authentication and assigning an authentication group, see Configuring SSL Proxy Service, page 9-28.

Use this procedure to specify the certificate authentication groups that the ACE uses during the SSL handshake and enable client authentication on this SSL-proxy service. The ACE includes the certificates configured in the group along with the certificate that you specified for the SSL proxy service.

Assumptions

- At least one SSL certificate is available.
- Your ACE appliance supports authentication groups.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Auth Group Parameters**.

The Auth Group Parameters table appears.

Step 2 Click **Add** to add a authentication group, or select an existing auth group, and then click **Edit** to modify it. The Auth Group Parameters configuration screen appears.

Step 3 In the Name field, enter a unique name for the auth group. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE. The updated Auth Group Parameters screen appears along with the Auth Group Certificates table. Continue with Step 5.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
- Click **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.

Step 5 In the Auth Group Certificate field, click **Add** to add an entry. The Auth Group Certificates configuration screen appears.

Note You cannot modify an existing entry in the Auth Group Certificates table. Instead, delete the entry, and then add a new one.

Step 6 In the Certificate Name field, select the certificate to add to this auth group.

Step 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
- Click **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.

Step 8 You can repeat the previous step to add more certificates to the auth group or click **Deploy Now**.

Step 9 After you configure auth group parameters, you can configure the SSL proxy service to use a CRL. See Configuring CRLs for Client Authentication, page 9-33.

Note When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

Related Topics

- Configuring SSL Chain Group Parameters, page 9-25
- Configuring CRLs for Client Authentication, page 9-33

Configuring CRLs for Client Authentication

By default, ACE does not use certificate revocation lists (CRLs) during client authentication. You can configure the SSL proxy service to use a CRL by having the ACE scan each client certificate for the service to determine if it contains a CRL in the extension and then retrieve the value, if it exists. For more information about SSL termination on the ACE, see the *SSL Guide, Cisco ACE Application Control Engine*.

Note The ACE supports the creation of a maximum of eight CRLs for any context.

Note When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

Use this procedure to configure ACE to scan for CRLs and retrieve them.

Assumption

A CRL cannot be configured on an SSL proxy without first configuring an auth group.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> SSL > Certificate Revocation Lists (CRL)**. The Certificate Revocation List table appears.

Step 2 Click **Add** to add a CRL or select an existing CRL, and then click **Edit** to modify it. The Certificate Revocation List screen appears.

Step 3 Enter the information in Table 9-13.

Table 9-13 SSL Certificate Revocation List

Field	Description
Name	Enter the CRL name. Valid entries are unquoted alphanumeric strings with a maximum of 64 characters.
URL	Enter the URL where the ACE retrieves the CRL. Valid entries are unquoted alphanumeric strings with a maximum of 255 characters. Only HTTP URLs are supported. ACE checks the URL and displays an error if it does not match.

Step 4 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE. The updated Certificate Revocation List table appears.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Certificate Revocation List table.
- Click **Next** to deploy your entries and to add another entry to the Certificate Revocation List table.

Related Topics

- Configuring SSL Proxy Service, page 9-28
- Configuring SSL Authentication Groups, page 9-32