CHAPTER 11

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 1-3).

This chapter describes how to configure Secure Sockets Layer (SSL) on the Cisco Application Control Engine (ACE) using Cisco Application Networking Manager (ANM).

Note When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), and dot (.). Spaces are not allowed.

If you are using ANM with an ACE module or ACE appliance and you configure a named object at the ACE CLI, keep in mind that ANM does not support all of the special characters that the ACE CLI allows you to use when configuring a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

This chapter includes the following sections:

SSL Overview

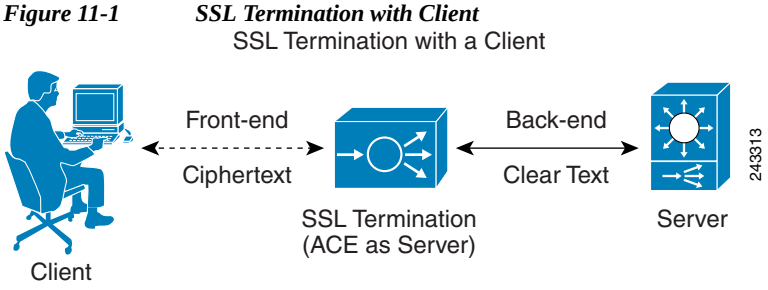
SSL is an application-level protocol that provides encryption technology for the Internet, ensuring secure transactions such as the transmission of credit card numbers for e-commerce websites. SSL initiation occurs when the ACE device (either an ACE module or an ACE appliance) acts as a client and initiates 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 11-1 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 11-1 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 need to delete any of the SSL objects (authorization 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 the "SSL Configuration Prerequisites" section on page 11-2.

SSL Configuration Prerequisites

This SSL configuration prerequisites are as follows:

- 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.

Note You cannot generate a CSR in Building Blocks (Config > Global > All Building Blocks); SSL CSR generation is available only in virtual context configuration.

Summary of SSL Configuration Tasks

Table 11-1 describes the tasks for using SSL keys and certificates.

Table 11-1 SSL Key and Certificate Procedure Overview

Task	Description
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 TSL. See the "Configuring SSL Parameter Maps" section on page 11-18.
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 the "Generating SSL Key Pairs" section on page 11-14.
Configure CSR parameters.	Set CSR parameters to define the distinguished name attributes of a CSR. See the "Configuring SSL CSR Parameters" section on page 11-24.
Create a CSR.	Create a CSR to submit with the key pair file when you apply for an SSL certificate. See the "Generating CSRs" section on page 11-26.
Copy and paste the CSR into the Certificate Authority (CA) web-based application or email 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.
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.

Table 11-1 SSL Key and Certificate Procedure Overview (continued)

Task	Description
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 ANM. For more information, see the following topics: • "Importing SSL Certificates" section on page 11-7 • "Importing SSL Key Pairs" section on page 11-11
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.
Configure the virtual context for SSL.	See the "Configuring Traffic Policies" section on page 14-1.
Configure authorization group.	Create a group of certificates that are trusted as certificate signers by creating an authentication group. See the "Configuring SSL Authentication Groups" section on page 11-31.
Configure CRL.	See the "Configuring CRLs for Client Authentication" section on page 11-33.

For more information about using SSL with ACE, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* or *Cisco Application Control Engine Module SSL Configuration Guide*.

SSL Setup Sequence

The SSL setup sequence provides detailed instructions with illustrations for configuring SSL on ACE devices from ANM (Figure 11-2). 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 windows already present in ANM. 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 device. 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 windows provide.

The tools and operations involved in typical SSL operations are as follows:

- SSL Import/Create Keys
- SSL Import Certificates
- SSL CSR generation
- SSL proxy creation

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

For more information on SSL configuration features, see the "Summary of SSL Configuration Tasks" section on page 11-3.

Figure 11-2 SSL Setup Sequence

Related Topics

- Configuring SSL, page 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL Proxy Service, page 11-27

Using SSL 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
- Time stamps that indicate the certificate's start date
- Time stamps that indicate the certificate's expiration date
- CA certificate

A Certificate Authority has one or more signing certificates that it uses for creating SSL certificates and certificate revocation lists (CRLs). 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 For the ACE module A2(3.0), ACE appliance A4(1.0), or later releases of either device type, the ACE supports a maximum of eight CRLs for any context. For earlier releases of either device type, the ACE supports a maximum of four CRLs for any context.

All certificates have an expiration date, usually one year after the certificate was issued. You can monitor certificate expiration status by going to Monitor > Devices > *context* > Dashboard. ANM issues a warning email daily before the certificate expiration date. You establish how many days before the expiration date that the warning email messages begin in the Threshold Groups settings window, which you can access using either of the following methods:

- Choose **Monitor** > **Alarm Notifications** > **Thresholds Groups**.
- Click the **Configure Certificate Expiry Threshold Alarms** button in the Certificates window (Config > Devices > *context* > SSL > Certificates).

Note The Certificates window (Config > Devices > context > SSL > Certificates) contains the Expiry Date field, which displays the certificate expiration date. Due to a known issue with the ACE module and appliance, it is possible that this field displays either "Null" or characters that are unparseable or unreadable. When this issue occurs, ANM is unable to track the certificate expiration date. If the certificate is defined in a threshold group configured for certificate expiration alarm notifications and this issue occurs, ANM may not issue an expiration alarm when expected or it may issue a false alarm. If you encounter this issue, remove the certificate from the ACE, reimport it, and then verify that the correct expiration date displays in the Certificates window.

For more information about configuring the certificate expiration alarm notification, see the "Configuring Alarm Notifications on ANM" section on page 17-61.

The ACE requires certificates and corresponding key pairs for the following:

- SSL Termination—The ACE 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 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.

Note The ACE includes a preinstalled sample certificate and corresponding key pair. This feature is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type.

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

You can add these files to an SSL-proxy service (see the "Configuring SSL Proxy Service" section on page 11-27) 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 11-1
- Exporting SSL Certificates, page 11-15
- Importing SSL Certificates, page 11-7
- Using SSL Keys, page 11-10
- Importing SSL Key Pairs, page 11-11
- Configuring SSL CSR Parameters, page 11-24
- Generating CSRs, page 11-26
- Configuring SSL Proxy Service, page 11-27

Importing SSL Certificates

You can import SSL certificates from a remote server to the ACE, which can support the following number of certificates and key pairs depending on the installed software version:

- ACE Module:
  - A2(3.x) and earlier—3800 certificates and 3800 key pairs
  - A4(1.0)— 4096 certificates and 4096 key pairs
- ACE Appliance:
  - A3(1.x) and earlier—3800 certificates and 3800 key pairs
  - A3(2.x) and later (including A4(1.0))—4096 certificates and 4096 key pairs

Assumptions

This topic assumes the following:

- You have configured the ACE for server load balancing. (See the "Information About Load Balancing" section on page 7-1.)
- You have obtained an SSL certificate from a certificate authority (CA) and have placed it on a network server accessible by the ACE.

Note You cannot import SSL certificates in Building Blocks (Config > Global > All Building Blocks); SSL certificate imports are available only in virtual context configuration.

Procedure

Step 1 To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Certificates**.

The Certificates table appears, listing any valid SSL certificates.

The cisco-sample-cert certificate is included in the list only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type. For information on this sample certificate, see the "Using SSL Certificates" section on page 11-5.

Step 2 In the Certificates table, do one of the following:

- To import a single SSL certificate, click **Import**. The Import dialog box appears.
- To import multiple SSL certificates, click **Bulk Import**. The Bulk Import dialog box appears.

Note The SSL bulk import feature is available only for ACE module A2(2.0), ACE appliance A4(1.0), or later releases of either device type. If you attempt to use the bulk import feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the bulk import configuration for the ACE.

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 ANM, perform a CLI Sync for this context once the SSL bulk import has completed. For information on synchronizing contexts, see the "Synchronizing Virtual Context Configurations" section on page 6-110.

Step 3 Enter the applicable information:

- For the Import dialog box, see Table 11-2.
- For the Bulk Import dialog box, see Table 11-3 (ACE module A2(2.0), ACE appliance A4(1.0), and later releases of either device type only).

Table 11-2 SSL Certificate Management Import Attributes

Field	Description
Protocol	Method to use for accessing the network server: • **FTP**—FTP is to be used to access the network server when importing the SSL certificate. • **SFTP**—SFTP is to be used to access the network server when importing the SSL certificate. • **TERMINAL**—You will import the file using cut and paste by pasting the certificate information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format. • **TFTP**—TFTP is to be used to access the network server when importing the SSL certificate.
IP Address	Field that appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server on which the SSL certificate file resides.
Remote File Name	Field that appears for single-file SSL certificate importing and FTP, TFTP, and SFTP. Enter the directory and filename of the single certificate file on the network server.
Local File Name	Filename to use for the single SSL certificate file when it is imported to the ACE.
User Name	Field that appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	Field that appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	Field that appears for FTP and SFTP. Reenter the password.
Passphrase	Field that 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	Field that appears for FTP, SFTP, and TERMINAL. Reenter the passphrase.

Table 11-2 SSL Certificate Management Import Attributes (continued)

Field	Description
Non-Exportable	Check box that specifies that this certificate file cannot be exported from the ACE. 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.
Import Text	Field that appears for Terminal. Cut the certificate information from the remote server and paste it into this field.

Table 11-3 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	IP 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	Name of the user account on the network server.
Password	Password for the user account on the network server.
Confirm	Password confirmation.
Passphrase	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	Passphrase confirmation.
Non-Exportable	Check box to specify that this certificate file cannot be exported from the ACE. 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.

Step 4 Do one of the following:

- Click **OK** to accept your entries and to return to the Certificates table. ANM 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 11-1
- Using SSL Keys, page 11-10
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

Using SSL Keys

You can display options for working with SSL and SSL keys. The ACE 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.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Keys**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **Keys**.

The Keys table appears.

Step 2 In the Keys table, continue with one of the following options:

- Generate a key pair—See the "Generating SSL Key Pairs" section on page 11-14.
- Import a key pair—See the "Importing SSL Key Pairs" section on page 11-11.
- Export a key pair—See the "Exporting SSL Key Pairs" section on page 11-16.
- Generate a CSR—See the "Generating CSRs" section on page 11-26.

Related Topics

- Generating SSL Key Pairs, page 11-14
- Importing SSL Key Pairs, page 11-11
- Generating SSL Key Pairs, page 11-14
- Exporting SSL Key Pairs, page 11-16
- Configuring SSL, page 11-1

Importing SSL Key Pairs

You can import an SSL key pair file from a network server to an ACE, which can support the following number of certificates and key pairs depending on the installed software version:

- ACE Module:
  - A2(3.x) and earlier—3800 certificates and 3800 key pairs
  - A4(1.0)— 4096 certificates and 4096 key pairs
- ACE Appliance:
  - A3(1.x) and earlier—3800 certificates and 3800 key pairs
  - A3(2.x) and later (including A4(1.0))—4096 certificates and 4096 key pairs

Assumptions

This topic assumes the following:

- You have configured the ACE for server load balancing. (See the "Information About Load Balancing" section on page 7-1.)
- 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.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Keys**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **Keys**.

The Keys table appears, listing existing SSL keys.

For the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of both either type, 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 11-5.

Step 2 Do one of the following:

- To import a single SSL key pair, in the Keys table, click **Import**. The Import dialog box appears.
- To import multiple SSL key pairs, click **Bulk Import**. The Bulk Import dialog box appears.

Note The SSL bulk import feature is available only for ACE module A2(2.0), ACE appliance A4(1.0), and later releases of either device type. If you attempt to use the bulk import feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the bulk import configuration for the ACE.

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 ANM, perform a CLI Sync for this context once the SSL bulk import has completed. For information on synchronizing contexts, see the "Synchronizing Virtual Context Configurations" section on page 6-110.

Step 3 Enter the applicable information as follows:

- For the Import dialog box, see Table 11-4.
- For the Bulk Import dialog box, see Table 11-5 (ACE module A2(2.0), ACE appliance A4(1.0), and later releases of either device type only).

Table 11-4 SSL Key Pair Import Attributes

Field	Description
Protocol	Method to use for accessing the network server: • **FTP**—FTP is to be used to access the network server when importing the SSL key pair file. • **SFTP**—SFTP is to be used to access the network server when importing the SSL key pair file. • **TERMINAL**—You will import the file using cut and paste by pasting the certificate and key pair information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format. • **TFTP**—TFTP is to be used to access the network server when importing the SSL key pair file.
IP Address	Field that appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server on which the SSL key pair file resides.
Remote File Name	Field that appears for single-file SSL key pair importing and FTP, TFTP, and SFTP. Enter the directory and filename of the single key pair file on the network server.
Local File Name	Filename to be used for the single SSL key pair file when it is imported to the ACE.
User Name	This field appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	Field that appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	Field that appears for FTP, SFTP, and TERMINAL. Reenter the password.
Passphrase	Field that 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	Field that appears for FTP and SFTP. Reenter the passphrase.
Non-Exportable	Check box to specify that this key pair file cannot be exported from the ACE. 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 or Web server. Exporting is similar to copying in that the original files are not deleted. Uncheck the check box to indicate that this key pair file can be exported from the ACE.
Import Text	Field that appears for Terminal. Cut the key pair information from the remote server and paste it into this field.

Table 11-5 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	IP address of the remote server on which the SSL key pair files resides.

Table 11-5 SSL Key Pair Bulk Import Attributes (continued)

Field	Description
Remote Path	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 module 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 module 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 module does not import the file and discards it.
User Name	Name of the user account on the network server.
Password	Password for the user account on the network server.
Confirm	Password confirmation.
Passphrase	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	Passphrase confirmation.
Non-Exportable	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 one of the following:

- Click **OK** to accept your entries and to return to the Keys table. ANM 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 11-1
- Importing SSL Certificates, page 11-7
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

Generating SSL Key Pairs

The ACE can generate SSL RSA key pairs if you do not have any matching key pairs.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Keys**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **Keys**.

The Keys table appears.

For the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type, the cisco-sample-key key pair is included in the list. For information about this sample key pair, see the "Using SSL Certificates" section on page 11-5.

Step 2 In the Keys table, click **Add** to add a new key pair.

The Keys configuration window appears.

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

Step 3 In the Keys configuration window, enter the information in Table 11-6.

Table 11-6 Key Attributes

Field	Description
Name	Name of the SSL key pair. Valid entries are alphanumeric strings up to 64 characters.
Size (Bits)	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
Type	RSA is a public-key cryptographic system used for authentication.
Exportable Key	Check box that specifies that the key pair file can be exported. Uncheck the check box to indicate that the key pair file cannot be exported.

Step 4 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 this procedure without saving your entries and to return to the Keys table.

- Click **Next** to deploy your entries and to define another RSA key pair.

After generating an RSA key pair, you can do the following:

- Create a CSR parameter set. The CSR parameter set defines the distinguished name attributes for the ACE to use during the CSR-generating process. For details on defining a CSR parameter set, see the "Configuring SSL CSR Parameters" section on page 11-24.
- 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 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 the "Generating CSRs" section on page 11-26.

Related Topics

- Configuring SSL, page 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

Exporting SSL Certificates

You can export SSL certificates from the ACE to a remote server. 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 or Web server. Exporting certificates is similar to copying in that the original certificates are not deleted.

Assumption

The SSL certificate can be exported (see the "Importing SSL Certificates" section on page 11-7).

Note You can export an SSL certificate in Building Blocks (Config > Global > All Building Blocks); SSL certificate export is available only in virtual context configuration.

Procedure

Step 1 To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Certificates**.

The Certificates table appears, listing any valid SSL certificates.

The cisco-sample-cert certificate is included in the list only for the ACE module A2(3.0), ACE appliance 4(1.0), and later releases of either device type. For information about this sample certificate, see the "Using SSL Certificates" section on page 11-5.

Step 2 In the Certificates table, choose the certificate you want to export, and click **Export**.

The Export dialog box appears.

Step 3 In the Export dialog box, enter the information in Table 11-7.

Table 11-7 SSL Certificate Export Attributes

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

Step 4 Do one of 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 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Generating SSL Key Pairs, page 11-14
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

Exporting SSL Key Pairs

You can export SSL key pairs from the ACE to a remote server. 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 or Web server. Exporting key pair files is similar to copying in that the original key pairs are not deleted.

Assumption

The SSL key pair can be exported (see the "Generating SSL Key Pairs" section on page 11-14).

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Keys**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **Keys**.

The Keys table appears. For the ACE module A2(3.0) and later releases only, the cisco-sample-key key pair is included in the list. For information about this sample key pair, see the "Using SSL Certificates" section on page 11-5.

Step 2 In the Keys table, choose the key entry you want to export, and click **Export**.

The Export dialog box appears.

Step 3 In the Export dialog box, enter the information in Table 11-8.

Table 11-8 SSL Key Export Attributes

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

Step 4 Do one of 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 11-1
- Importing SSL Certificates, page 11-7

Configuring SSL Parameter Maps

You can create SSL parameter maps., which defines the SSL session parameters that the ACE applies to an SSL proxy service. SSL parameter maps let you apply the same SSL session parameters to different proxy services.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **Parameter Map**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **Parameter Map**.

The Parameter Map table appears.

Step 2 In the Parameter Map table, click **Add** to add a new SSL parameter map, or choose an existing entry to modify and click **Edit**.

The Parameter Map configuration window appears.

Step 3 In the Parameter Map configuration window, enter the information in Table 11-9.

Table 11-9 SSL Parameter Map Attributes

Field	Description
Name	Unique name for the parameter map. Valid entries are alphanumeric strings with a maximum of 64 characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. 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. Double quotes must be entered as matching pairs.
Queue Delay Timeout (Milliseconds)	Time (in milliseconds) to wait before emptying the queued data for encryption. Valid entries are 0 to 10000 milliseconds. 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.

Table 11-9 SSL Parameter Map Attributes (continued)

Field	Description
Session Cache Timeout (Milliseconds)	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 feature allows the ACE to reuse the master key on subsequent connections with the client, which can speed up the SSL negotiation process. Valid entries are 0 to 72000 milliseconds. Specifying a value of 0 causes the ACE to implement a least recently used (LRU) timeout policy. By disabling this option (with the **no** command), the full SSL handshake occurs for each new connection with the ACE module.
Reject Expired CRL Certificates	Check box that instructs the ACE to reject any certificates listed on an expired CRL. Uncheck the check box to instruct the ACE to accept certificates listed on an expired CRL, which is the default setting.
Close Protocol Behavior	Method that the ACE uses to close the SSL connection: • **Disabled**—The ACE sends 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**—The ACE does not send a close-notify alert message to the SSL peer, nor does the ACE expect a close-notify alert message from the peer. The ACE preserves the session information so that SSL resumption can be used for future SSL connections. This is the default. **Note** Where ACE 1.0 is already configured with the Strict option, ANM interprets it as the option None. This is due to the change in ACE 1.0 configuration (which no longer allows the Strict option).
SSL Version	Version of SSL to be used during SSL communications: • **All**—The ACE uses both SSL v3 and TLS v1 in its communications with its SSL peer. • **SSL3**—The ACE uses only SSL v3 in its communications with its SSL peer. • **TLS1**—The ACE uses only TLS v1 in its communications with its SSL peer. • **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

Table 11-9 SSL Parameter Map Attributes (continued)

Field	Description
Ignore Authentication Failure	Option that enables the ACE to ignore expired or invalid SSL certificates and continue setting up the connection as follows: • ACE module versions 3.0(0)A2(1.1) forward and ACE appliance version A3(1.0) only—If checked, this feature enables the ACE to ignore expired or invalid server certificates and to continue setting up the back-end connection in an SSL initiation configuration. This option allows the ACE to ignore the following nonfatal errors with respect to server certificates: – Certificate not yet valid – Certificate has expired – Certificate revoked – Unknown issuer • ACE module version A2(3.0) and later only—If checked, this feature enables the ACE to ignore expired or invalid client or server certificates and to continue setting up the SSL connection. This options allows the ACE 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 4 Click the **Parameter Map Cipher** tab and click **Add** to add a cipher, or choose an existing cipher and click **Edit**.

Enter the information in Table 11-10.

Table 11-10 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 the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* or the *Cisco Application Control Engine Module SSL Configuration Guide*.
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.

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 11-11 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 11-12 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 }
RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x3C }

Step 5 In the Parameter Map Cipher table, do one of the following:

- Click **Deploy Now** to deploy the Parameter Map Cipher 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 Cipher table.
- Click **Next** to deploy your entries and to add another entry to the Parameter Map Cipher table.

Step 6 Click the **Redirect Authentication Failure** tab and click **Add** to add a redirect or choose an existing redirect, and click **Edit**.

Note This option is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type.

Enter the information in Table 11-13.

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 11-13 SSL Parameter Map Redirect Configuration Attributes

Field	Description
Client Certificate Validation	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	Redirect type to use: • **Server Farm**—Specifies a redirect server farm for the redirect. • **URL**—Specifies a static URL path for the redirect.
Server Farm Name	Field that appears when the Redirect Type is set to Server Farm. ANM displays the available server farms as follows: • ACE software Version A4(1.0) or later—ANM displays all configured host and redirect server farms. • All earlier ACE software versions—ANM displays only those server farms configured as 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 8-31).
Redirect URL	Field that appears when the Redirect Type is set to URL. Specifies the static URL path for the redirect. Enter a string with a maximum of 255 characters and no spaces.
Redirect Code	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 7 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 8 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 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Generating SSL Key Pairs, page 11-14
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

Configuring SSL Chain Group Parameters

You can configure certificate chain groups for a virtual context. A chain group specifies the *certificate chains* that the ACE sends to its peer during the handshake process. A certificate chain is a hierarchal list of certificates that includes the ACE'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.

Assumption

At least one SSL certificate is available.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **SSL** > **Chain Group Parameters**.

The Chain Group Parameters table appears.

Step 2 In the Chain Group Parameters table, click **Add** to add a new chain group, or choose an existing chain group, and click **Edit** to modify it.

The Chain Group Parameters configuration window appears.

Step 3 In the Name field of the Chain Group Parameters configuration window, enter a unique name for the chain group.

Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 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. The updated Chain Group Parameters window 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 deploy 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 window appears.

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

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

Step 7 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 Chain Group Certificates table.
- Click **Next** to deploy your entries and to add another certificate to this chain group table.

Related Topics

- Configuring SSL, page 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Generating SSL Key Pairs, page 11-14
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL CSR Parameters, page 11-24
- Configuring SSL Proxy Service, page 11-27

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 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 the ACE can contain up to eight CSR parameter sets.

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

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **SSL** > **CSR Parameters**.
- To configure a building block, choose **Config** > **Global** > *building_block* > **SSL** > **CSR Parameters**.

The CSR Parameters table appears.

Step 2 In the CSR Parameters table, click **Add** to add new set of CSR attributes, or choose an existing entry to modify and click **Edit**.

The CSR Parameters configuration window appears.

Step 3 In the CSR Parameters configuration window, enter the information in Table 11-14.

Table 11-14 SSL CSR Parameter Attributes

Field	Description
Name	Unique name for this parameter set. Valid entries are alphanumeric strings with a maximum of 64 characters.
Country	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).
State	Name of the state or province where the SSL site resides.
Locality	Name of the city where the SSL site resides.
Common Name	Name of the domain or host of the SSL site. Valid entries are strings with a maximum of 64 characters. Special characters are allowed.
Serial Number	Serial number to assign to the certificate. Valid entries are alphanumeric strings with a maximum of 16 characters.
Organization Name	Name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.
Email	Site email address. Valid entries are text strings, including alphanumeric and special characters (for example, @ symbol in email address) with a maximum of 40 characters.
Organization Unit	Name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 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 this procedure without saving your entries and to return to the CSR Parameters table.
- Click **Next** to deploy your entries and to define another set of CSR attributes.

Related Topics

- Configuring SSL, page 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL Proxy Service, page 11-27

Generating CSRs

You can generate an SSL *certificate signing request* (CSR), which is a message that 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 the "Importing SSL Certificates" section on page 11-7 and the "Importing SSL Key Pairs" section on page 11-11).

Note You cannot generate a CSR in Building Blocks (Config > Global > All Building Blocks); SSL CSR generation is available only in virtual context configuration.

Assumption

You have configured SSL CSR parameters (see the "Configuring SSL CSR Parameters" section on page 11-24).

Procedure

Step 1 Choose **Config > Devices >** *context* **> SSL > Keys**.

The Keys table appears.

Step 2 In the Keys table, choose a key and click **Generate CSR**.

The Generate a Certificate Signing Request dialog box appears.

Step 3 In the CSR Parameter field of the Generate a Certificate Signing Request dialog box, choose the CSR parameter to be used.

Step 4 Do one of 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 email 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 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Parameter Maps, page 11-18
- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL Proxy Service, page 11-27

Configuring SSL Proxy Service

You can configure an SSL proxy service that defines the SSL parameter map, key pair, certificate, and chain group the ACE uses during SSL handshakes. By configuring an SSL proxy *server* service on the ACE, the ACE 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** > **Devices** > *context* > **SSL** > **Proxy Service**.

The Proxy Service table appears.

Step 2 In the Proxy Service table, click **Add** to add a new proxy service, or choose an existing service and click **Edit** to modify it.

The Proxy Service configuration window appears.

Step 3 In the Proxy Service configuration window, enter the information in Table 11-15.

Table 11-15 SSL Proxy Service Attributes

Field	Description
Proxy Service Name	Unique name for this proxy service. Valid entries are alphanumeric strings with a maximum of 40 to 65 characters, depending on your ACE and hardware version.
Keys	Key pair that the ACE 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, ANM selects the keys that correspond to the certificate that you choose. If ANM cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ANM verify that the keys correspond to the selected certificate. ANM 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 11-4. The **cisco-sample-key** option is available for the ACE module A2(3.0) and later releases only. For information about this sample key pair, see the "Using SSL Certificates" section on page 11-5.
Certificates	Certificate that the ACE 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, ANM selects the keys that correspond to the certificate that you choose. If ANM cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ANM verify that the keys correspond to the selected certificate. ANM 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 11-4. The **cisco-sample-cert** option is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type. For information about this sample certificate, see the "Using SSL Certificates" section on page 11-5.
Chain Groups	Chain group that the ACE is to use during the SSL handshake. To create a chain group, see the "Configuring SSL Chain Group Parameters" section on page 11-23.
Auth Groups	Authorization group name that the ACE is to use during the SSL handshake. To create an authorization group, see the "Configuring SSL Authentication Groups" section on page 11-31.
CRL Best-Effort	Field that displays only when Auth Groups is selected. Allows ANM to search client certificates for the service to determine if it contains a CRL in the extension. ANM then retrieves the value, if it exists.

Table 11-15 SSL Proxy Service Attributes (continued)

Field	Description
CRL Name	Field that displays only when Auth Groups is selected. Do one of the following: • Choose **N/A** when the CRL name is not applicable. • Choose the CRL name that the ACE used for authentication.
OCSP Best-Effort	Field that displays for ACE module or appliance software Version A5(1.0) or later, and when Auth Groups is selected. Check the OCSP Best-Effort checkbox 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. Uncheck the checkbox to display the OCSP server field to choose the available OCSP server.
OCSP Servers	Field that displays for ACE module or appliance software Version A5(1.0) or later, and when the OCSP Best-Effort check box is unchecked. Choose the available OCSP server.
Parameter Maps	SSL parameter map to associate with this SSL proxy server service.
Revocation Check Priority Order	Field that displays for ACE module or appliance software Version A5(1.0) or later. Priority setting for the revocation check. Choose one of the following: • **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 4 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 this procedure without saving your entries and to return to the Proxy Service table.
- Click **Next** to deploy your entries and to add another proxy service.
- Click **Delete** to remove this configuration on the ACE.

Note When an authorization group is deleted, the CRL Name object (if it exists) is deleted automatically.

Related Topics

- Configuring SSL, page 11-1
- Importing SSL Certificates, page 11-7
- Importing SSL Key Pairs, page 11-11
- Configuring SSL Parameter Maps, page 11-18

- Configuring SSL Chain Group Parameters, page 11-23
- Configuring SSL CSR Parameters, page 11-24

Configuring SSL OCSP Service

Note The SSL Online Certificate Status Protocol feature requires ACE module and ACE appliance software Version A5(1.0) or later.

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** > **Devices** > *context* > **SSL** > **OCSP Service**. The OCSP Service table appears.

Step 2 Click **Add** to add a new OCSP service, or select an existing service, 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 filename 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 filename 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.

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 one of 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 11-1
- Configuring SSL Proxy Service, page 11-27

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 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 11-27
- Configuring SSL Authentication Groups, page 11-31
- Configuring CRLs for Client Authentication, page 11-33

Configuring SSL Authentication Groups

You can 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.

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 the "Enabling Client Authentication" section on page 11-31.

For information on server authentication and assigning an authentication group, see the "Configuring SSL Proxy Service" section on page 11-27.

Note You cannot create an authorization group in Building Blocks (Config > Global > All Building Blocks); You can only create SSL authentication groups while configuring virtual contexts in specific modules.

Assumptions

- At least one SSL certificate is available.
- Your ACE supports authentication groups. See the *Supported Devices Table for Cisco Application Networking Manager* for details.

Procedure

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

The Auth Group Parameters table appears.

Step 2 In the Auth Group Parameters table, click **Add** to add an authentication group, or choose an existing authorization group and click **Edit** to modify it.

The Auth Group Parameters configuration window appears.

Step 3 In the Name field of the Auth Group Parameters configuration window, enter a unique name for the authorization group.

Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 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. The updated Auth Group Parameters window 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 window appears.

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

Step 6 In the Certificate Name field, choose the certificate to add to this authorization group.

Step 7 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 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 authorization group or click **Deploy Now**.

Step 9 After you configure authorization group parameters, you can configure the SSL proxy service to use a CRL. See the "Configuring CRLs for Client Authentication" section on page 11-33.

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 11-23
- Configuring CRLs for Client Authentication, page 11-33

Configuring CRLs for Client Authentication

You can configure the ACE to scan for CRLs and retrieve them. 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 either the *Cisco Application Control Engine Module SSL Configuration Guide* or the *Cisco ACE 4700 Series Appliance SSL Configuration Guide*.

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.

Assumption

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

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **SSL** > **Certificate Revocation Lists (CRLs)**.

The Certificate Revocation Lists (CRLs) table appears.

Step 2 In the Certificate Revocation Lists (CRLs) table, click **Add** to add a CRL, or choose an existing CRL and click **Edit** to modify it.

The Certificate Revocation Lists (CRLs) window appears.

Step 3 In the Certificate Revocation Lists (CRLs) window, enter the information in Table 11-16.

Table 11-16 SSL Certificate Revocation List

Field	Description
Name	CRL name. Valid entries are unquoted alphanumeric strings with a maximum of 64 characters.
URL	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 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. The updated Certificate Revocation Lists (CRLs) table appears.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Certificate Revocation Lists (CRLs) table.
- Click **Next** to deploy your entries and to add another entry to the Certificate Revocation Lists (CRLs) table.

Related Topics

- Configuring SSL Proxy Service, page 11-27
- Configuring SSL Authentication Groups, page 11-31