CHAPTER 6

Displaying SSL Information and Statistics

This chapter describes how to use the available **show** commands to display SSL-related information, such as the certificate and key pair files loaded on the ACE. The **show** commands display information associated with the context from which you execute the command. Each command described in this chapter also includes an explanation of the command output.

While the **show** commands are Exec mode commands, you can execute a **show** command from any configuration mode by using the **do** command. The following examples show how to execute the **show running-config** command from either Exec mode or configuration mode.

From Exec mode, enter:

```
host1/Admin# show running-config
```

From configuration mode, enter:

```
host1/Admin(config)# do show running-config
```

This chapter contains the following major sections:

Displaying CSR Parameter Set Configurations

To display the CSR parameter set summary and detailed reports, use the **show crypto csr-params** command in Exec mode.

The syntax of this command is as follows:

show crypto csr-params {*params_set* | **all**}

The arguments and keywords are:

- *params_set*— argument is a specific CSR parameter set. Enter an unquoted alphanumeric string with a maximum of 64 characters. The ACE displays the detailed report for the specified CSR parameter set. The detailed report contains the distinguished name attributes of the CSR parameter set.
- To display the summary report that lists all the CSR parameter sets for the current context, enter the command without specifying a CSR parameter set.

For example, to display the CSR parameter set summary report, enter:

```
host1/Admin# show crypto csr-params all
```

The following example shows how to display the detailed report for the MYCSRCONFIG CSR parameter set:

```
host1/Admin# show crypto csr-params MTCSRCONFIG
```

Table 6-1 describes the fields in the **show crypto csr-params** command output.

Table 6-1 Field Descriptions for the show crypto csr-params config_name Command

Field	Description
Country-name	Country where the certificate owner resides.
State	State where the certificate owner resides.
Locality	Locality where the certificate owner resides.
Org-name	Name of the organization (certificate owner or subject).
Org-unit	Name of unit within the organization.
Common-name	Common-name (domain name or individual hostname of the SSL site).
Serial number	Serial number.
Email	E-mail address.

Displaying the List of Certificate and Key Pair Files

To display a list of all available certificate and key pair files, use the **show crypto files** command in Exec mode.

For example, to display the list of certificate and key pair files, enter:

```
host1/Admin# show crypto files
```

Table 6-2 describes the fields in the **show crypto files** command output.

Table 6-2 Field Descriptions for the show crypto files Command

Field	Description
Filename	Name of the file that contains the certificate or key pair.
Size	Size of the file.
Type	Format of the file: PEM, DER, or PKCS12.

Table 6-2 Field Descriptions for the show crypto files Command (continued)

Field	Description
Exportable	Indicates whether you can export the file from the ACE using the **crypto export** command: • **Yes**—You can export the file to an FTP, SFTP, or TFP server (see the "Exporting Certificate and Key Pair Files" section in Chapter 2, "Managing Certificates and Keys"). • **No**—You cannot export the file as it is protected.
Key/Cert	Indicates whether the file contains a certificate (CERT), a key pair (KEY), or both (BOTH).

Displaying Certificate Information

To display the certificate summary and detailed reports, use the **show crypto certificate** command in Exec mode.

The syntax of this command is as follows:

show crypto certificate {*filename* | **all**}

The keywords and arguments are as follows:

- *filename*—Name of a specific certificate file. Enter an unquoted alphanumeric string with a maximum of 40 characters. The ACE displays the certificate detailed report for the specified file. If the certificate file contains a chain, the ACE displays only the bottom level certificate (the signers are not displayed).
- **all**—Displays the certificate summary report that lists all the certificate files for the current context.

For example, to display the certificate summary report, enter:

```
host1/Admin# show crypto certificate all
```

Table 6-3 describes the fields in the **show crypto certificate all** command output.

Table 6-3 Field Descriptions for the show crypto certificate all Command

Field	Description
Certificate file	Name of the certificate file.
Subject	Distinguished name of the organization that owns the certificate and possesses the private key.
Issuer	Distinguished name of the Certificate Association (CA) that issued the certificate.
Not Before	Starting time period, before which the certificate is not considered valid.
Not After	Ending time period, after which the certificate is not considered valid.
CA Cert	Certificate of the CA that signed the certificate.

The following example shows how to display the detailed report for the MYCERT.PEM certificate file:

```
host1/Admin# show crypto certificate MYCERT.PEM
```

Table 6-4 describes the fields in the **show crypto certificate** *filename* command output.

Table 6-4 Field Descriptions for the show crypto certificate filename Command

Field	Description
Certificate	Name of the certificate file.
Data	
Version	Version of the X.509 standard. The certificate complies with this version of the standard.
Serial Number	Serial number associated with the certificate.
Signature Algorithm	Digital signature algorithm used for the encryption of information with a public/private key pair.
Issuer	Distinguished name of the CA that issued the certificate.

Table 6-4 Field Descriptions for the show crypto certificate filename Command (continued)

Field	Description
Validity	
Not Before	Starting time period, before which the certificate is not considered valid.
Not After	Ending time period, after which the certificate is not considered valid.
Subject	Distinguished name of the organization that owns the certificate and possesses the private key.
Subject Public Key Info	
Public Key Algorithm	Name of the key exchange algorithm used to generate the public key (for example, RSA).
RSA Public Key	Number of bits in the key to define the size of the RSA key pair used to secure web transactions.
Modulus	Actual public key on which the certificate was built.
Exponent	One of the base numbers used to generate the key.
X509v3 Extensions	Array of X509v3 extensions added to the certificate.
X509v3 Basic Constraints	Indicates whether the subject may act as a CA, with the certified public key being used to verify certificate signatures. If so, a certification path length constraint may also be specified.
Netscape Comment	Comment that may be displayed when the certificate is viewed.
X509v3 Subject Key Identifier	Public key to be certified. It enables distinct keys used by the same subject to be differentiated (for example, as key updating occurs).
X509v3 Authority Key Identifier	Public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (for example, as key updating occurs).

Table 6-4 Field Descriptions for the show crypto certificate filename Command (continued)

Field	Description
Signature Algorithm	Name of the algorithm used for digital signatures (but not for key exchanges).
Hex Numbers	Actual signature of the certificate. The client can regenerate this signature using the specified algorithm to make sure that the certificate data has not been changed.

Displaying CRL Information

To display a list of certificate revocation lists (CRLs) or definitions for a specified CRL in a context, use the **show crypto crl** command in Exec mode. The syntax of this command is as follows:

show crypto crl {*crl_name* [**detail**] | **all** | **best-effort**}

The keywords and arguments are as follows:

- *crl_name*—Name of a specific CRL configured in the context. Enter an unquoted alphanumeric string. The ACE displays the definitions for the specified CRL.
- **detail**—(Optional) Displays detailed statistics for the downloading of the CRL including failure counters.
- **all**—Displays a lists of all CRLs configured in the context.
- **best-effort**—Displays summarized information for all best-effort CRLs on the ACE (a maximum of 16 CRLs).

For example, to display a list of all CRLs, enter:

```
host1/Admin# show crypto crl all
```

To display the definitions for a specific CRL, for example CRL1, enter:

```
host1/Admin# show crypto crl CRL1
```

Table 6-5 describes the fields in the **show crypto crl** *crl_name* command output.

Table 6-5 Field Descriptions for the show crypto crl Command

Field	Description
URL	URL where the ACE downloads the CRL.
Last Downloaded	Last time the ACE downloaded the CRL. If the CRL is configured on an SSL-proxy service on a policy map that is not active or the service is not associated with a policy map, the field displays the “not downloaded yet” message.
Total Number of Download Attempts	Number of times the ACE attempted to download the CRL.
Failed Download Attempts	Numbers of times the ACE failed to download the CRL.
Total Number of Download Attempts for Real CRL Data	Number of times the ACE attempted to download a specified CRL (not including “best effort” attempts).
Failed Download Attempts for Real CRL Data	Number of times the ACE failed to download a specified CRL (not including “best effort” attempts).

Table 6-5 Field Descriptions for the show crypto crl Command

Field	Description
Successful Loads (**detail** option)	Number of times that the ACE successfully loaded the CRL.
Failed Loads (**detail** option)	Number of times that the ACE could not load the CRL because of a failure.
Hours since Last Load (**detail** option)	Number of hours that elapsed since the ACE last successfully downloaded the CRL. If no successful download has occurred, this field displays NA, not applicable.
No IP Addr Resolutions (**detail** option)	Number of times the DNS resolution for the server host address of CRL the failed.
Host Timeouts (**detail** option)	Number of download retries to the CRL that had timed out.
Next Update Invalid (**detail** option)	Number of times that the next update field of the CRL was invalid.
Next Update Expired (**detail** option)	Number of times that the next update field of the CRL was expired.
Bad Signature (**detail** option)	Number of times that the signature mismatch for the CRL was detected, with respect to the CA certificate configured for signature verification of the CRL.
CRL Found-Failed to load (**detail** option)	Number of times that the ACE could not load the CRL because of the maximum size limitation of 10MB on ACE or the formatting of the CRL was not recognized. The ACE recognizes only DER and PEM encoded CRLs.
File Not Found (**detail** option)	Number of times that the server responded that the CRL file was not found at the server.
Memory Outage failures (**detail** option)	Number of times that the ACE failed to download the CRL because it temporarily could not provide memory to store the CRL data.
Cache Limit failures (**detail** option)	Number of times that the ACE could not load the CRL because the CRL cache was exhausted.

Table 6-5 Field Descriptions for the show crypto crl Command

Field	Description
Conn Failures (**detail** option)	Number of times that the ACE failed to download the CRL because it could not establish a connection with the server or no server entity was listening on the destination system.
Internal Failures (**detail** option)	Number of internal failures in the ACE that hampered downloading the CRL, for example, internal communication failures between components responsible for the downloading the CRL.
Not Eligible for download (**detail** option)	Number of times that the CRL was found ineligible for downloading because the following conditions: • The downloading of the same CRL is in progress. • The CRL has already been loaded successfully earlier and has not expired yet.
HTTP Read Failures (**detail** option)	Number of times that the ACE encountered an error when downloading the CRL because it could not read data on the connection established with server.
HTTP Write failures (**detail** option)	Number of times that the ACE encountered an error when downloading the CRL because it could not write the CRL download request from the connection established with the server.

For example, to display summarized information for all best-effort CRLs, enter:

```
host1/Admin# show crypto crl best-effort
```

Table 6-6 describes the fields in the **show crypto crl best-effort** command output.

Table 6-6 Field Descriptions for the show crypto crl best-effort Command

Field	Description
Best Effort CRL	Identifier to distinguish each best-effort CRL present at this time. At another time, the identifier can vary for the same CRL.
CRL Distribution Point	URL of the CDP. The ACE displays the first 255 characters of the URL.
CRL Downloaded	Whether the CRL is downloaded on the ACE module, Yes or No.
CRL Issuer Name	Name of the CRL issuer. The ACE displays the first 255 characters of the name.
Last Update	Contents of the Last Update field extracted from the CRL. The ACE displays the first 64 characters in the field
Next Update	Contents of the Next Update field extracted from the CRL. The ACE displays the first 64 characters in the field.

If no best-effort CRL exists on the ACE module, the ACE module displays the following message:

```
No best effort crl present in the system
```

Note To view whether the ACE rejects client certificates when the CRL in use is expired, use the **show parameter-map** command.

Displaying CDP Error Statistics

CRL Distribution Points (CDPs) indicate the location of the CRL in the form of a URL. CDP parsing in the certificate occurs only when best effort CRL is in use. To display statistics for discrepancies in CDPs for the certificates, use the **show crypto cdp-errors** command.

For example, to display the CDP statistics, enter:

```
host1/Admin# show crypto cdp-errors
```

Table 6-7 describes the fields in the **show crypto cdp-errors** command output.

Table 6-7 Field Descriptions for the show crypto cdp-errors Command

Field	Description
Incomplete	Number of times that the CDPs are missing information required to download the CRLs, for example, host, file name or base information.
Unrecognized Transports	Number of times that the ACE does not recognize or support the transport mechanism in the CDP for the CRL.
Malformed	Number of times that the CDPs are malformed with erroneous information, for example, specifying an incorrect attribute or base information. This counter also includes CDPs with URL lengths exceeding the ACE limit of 255 characters; a truncated URL could point to the wrong CRL.
Missing from cert	Number of times that the CDPs are missing from the certificate.
Best Effort CDP Errors Ignored	Number of times that the ACE ignored CDP errors in the presented certificates, and thereby allowed the SSL connection. This field is related to the **cdp-errors ignore** command in parameter map SSL configuration mode.

Displaying RSA Key Pair Information

To display the key pair file summary and detailed reports, use the **show crypto key** command in Exec mode.

The syntax of this command is as follows:

show crypto key {*filename* | **all**}

The keywords and arguments are as follows:

- *filename*—Name of a specific key pair file. Enter an unquoted alphanumeric string with a maximum of 40 characters. The ACE displays the key pair detailed report for the specified file.
- **all**—Displays the key pair summary report that lists all of the available key pair files.

For example, to display the key pair summary report, enter:

```
host1/Admin# show crypto all
```

Table 6-8 describes the fields in the **show crypto key** command output.

Table 6-8 Field Descriptions for the show crypto key Command

Field	Description
Filename	Name of the key pair file that contains the RSA key pair.
Bit Size	Size of the file.
Type	Type of key exchange algorithm, such as RSA.

The following example shows how to display the detailed report for the public and private keys contained in the MYKEYS.PEM key pair file:

```
host1/Admin# show crypto key MYKEYS.PEM
1024-bit RSA keypair
```

Table 6-9 describes the fields in the **show crypto key** *filename* command output.

Table 6-9 Field Descriptions for the show crypto key filename Command

Field	Description
Key Size	Size (in bits) of the RSA key pair.
Modulus	Hex value of the public key. The private key modulus is not shown for security purposes.

Displaying Certificate Chain Group Information

To display the chain group file summary and detailed reports, use the **show crypto chaingroup** command in Exec mode.

The syntax of this command is as follows:

show crypto chaingroup {*filename* | **all**}

The keywords and arguments are as follows:

- *filename*—Name of a specific chain group file. Enter an unquoted alphanumeric string with a maximum of 64 characters. The ACE displays the chain group detailed report for the specified file. The detailed report contains a list of the certificates configured for the chain group.
- **all**—Displays the chain group summary report that lists each of the available chain group files. The summary report also lists the certificates configured for each chain group.

For example, to display the chain group summary report, enter:

```
host1/Admin# show crypto chaingroup all
```

The following example shows how to display the detailed report of the certificates configured for the MYCERTGROUP chain group:

```
host1/Admin# show crypto chaingroup MYCERTGROUP
```

Table 6-10 describes the fields in the **show crypto chaingroup** command output.

Table 6-10 Field Descriptions for the show crypto chaingroup Command

Field	Description
Certificate	Certificate filename.
Subject	Distinguished name of the organization that owns the certificate and possesses the private key.
Issuer	Distinguished name of the CA that issued the certificate.

Displaying Client Authentication Group Information

To display a list of certificates for each authentication group or the certificates in a specified client authentication group including the Subject and Issuer information for each certificate, use the **show crypto authgroup** command in Exec mode.

The syntax of this command is as follows:

show crypto authgroup {*group_name* | **all**}

The keywords and arguments are as follows:

- *group_name*—Name of a specific authentication group file. Enter an unquoted alphanumeric string with a maximum of 64 characters.
- **all**—Displays the list of certificates for each authentication groups.

For example, to display the list of certificates for each authentication group, enter:

```
host1/Admin# show crypto authgroup all
```

To display each certificate for the AUTH-CERT1 group including the Subject and Issuer information for each certificate, enter:

```
host1/Admin# show crypto authgroup AUTH-CERT1
```

Table 6-11 describes the fields in the **show crypto authgroup** *group_name* command output.

Table 6-11 Field Descriptions for the show crypto authgroup group_name Command

Field	Description
Certificate	Certificate filename.
Subject	Distinguished name of the organization that owns the certificate and possesses the private key.
Issuer	Distinguished name of the CA that issued the certificate.

Displaying Cached TLS and SSL Session Entries

To display the number of cached TLS and SSL client and server session entries in the current context, use the **show crypto session** command in Exec mode.

The syntax of this command is as follows:

show crypto session

For example, enter:

```
host1/Admin# show crypto session
```

Displaying TLS and SSL Statistics

To display TLS and SSL client or server statistics for the current context, use the **show stats crypto** command in Exec mode.

The syntax of this command is as follows:

show stats crypto {**client** | **server**}

The keywords are as follows:

- **client**—Displays the TLS and SSL client statistics.
- **server**—Displays TLS and SSL server statistics.

For example, to display the client statistics, enter:

```
host1/Admin# show stats crypto client
```

To display the server statistics, enter:

```
host1/Admin# show stats crypto server
```

Table 6-12 describes the fields in the **show stats crypto** command output. For an explanation of how the HTTP header insertion counters work, see the "Information about SSL HTTP Header Insertion and Truncated Counters" section.

Table 6-12 Field Descriptions for the show stats crypto Command

Field	Description
SSL alert... rcvd/sent	Number of times that the standard SSL alert messages are received or sent.
SSLv2/v3 client hello received	Number of ClientHello message received.
SSLv3/TLSv1 negotiated protocol	Number of the times that the version is used in the connection.
SSLv3 full handshakes	Number of handshakes completed without errors.
SSLv3 resumed handshakes	Number of handshakes resumed by using a session ID.

Table 6-12 Field Descriptions for the show stats crypto Command (continued)

Field	Description
Cipher sslv3...	Number of times that the cipher suite is used in the connection.
TLSv1 full handshakes	Number of handshakes completed without errors.
TLSv1 resumed handshakes	Number of handshakes resumed by using a session ID.
Cipher tlsv1...	Number of times that the cipher suite is used in the connection.
Total SSL client authentications	Number of authenticated client connections. This field increments only when displaying server statistics.
Failed SSL client authentications	Number of client connections that failed authentication. This field increments only when displaying server statistics.
SSL client authentication cache hits	Number of times that an authenticated client reconnects and a cache entry is found. This field increments only when displaying server statistics.
SSL static CRL lookups	Number of lookups against a statically defined CRL.
SSL best effort CRL lookups	Number of lookups using the best effort.
SSL CRL lookup cache hits	Number of CRL lookups where the cache result was used.
SSL revoked certificates	Number of revoked certificates encountered.
Total SSL server authentications	Number of server certificate authentications that the ACE attempted to perform. This field increments only when displaying client statistics.
Failed SSL server authentications	Number of server certificate authentications that failed. This field increments only when displaying client statistics.

Table 6-12 Field Descriptions for the show stats crypto Command (continued)

Field	Description
Session headers extracted	Number of HTTP headers that contain SSL-negotiated session parameter information that the ACE successfully added to the HTTP header information build[1].
Session headers failed	Number of HTTP headers that contain SSL-negotiated session parameter information that the ACE could not add to the HTTP header information build[1].
Server cert headers extracted	Number of HTTP headers that contain SSL server certificate information that the ACE successfully added to the HTTP header information build[1].
Server cert headers failed	Number of HTTP headers that contain SSL server certificate information that the ACE could not add to the HTTP header information build[1].
Client cert headers extracted	Number of HTTP headers that contain SSL client certificate information that the ACE successfully added to the HTTP header information build[1].
Client cert headers failed	Number of HTTP headers that contain SSL client certificate information that the ACE could not add to the HTTP header information build[1].
Headers truncated	Number of HTTP headers that contain the SSL negotiated session parameter, server certificate, or client certificate information that the ACE truncated because the combined header information exceeded 512 bytes[1].
Redirect due to cert not yet valid	Number of redirects because the certificate is not valid yet.
Redirect due to cert expired	Number of redirects because the certificate has expired.
Redirect due to unable to get issuer cert	Number of redirects because the ACE is unable to retrieve issuer certificate.
Redirect due to cert revoked	Number of redirects because the certificate is revoked.

Table 6-12 Field Descriptions for the show stats crypto Command (continued)

Field	Description
Redirect due to no client cert sent	Number of redirects because the client did not send a client certificate.
Redirect due to no CRL available	Number of redirects because a CRL was not available.
Redirect due to CRL expired	Number of redirects because the CRL has expired.
Redirect due to bad cert signature	Number of redirects because the certificate has a bad signature.
Redirect due to other cert error	Number of redirects caused by certificate errors that do not apply to the other redirect fields.
Handshake FlushRX/TX operations	Number of times that the SSL handshake finished.
Xscale messages rcvd/sent for ME	Number of messages passed between the SSL processors during the SSL handshake.
Xscale rcvd abort msg before hdshk	Number of times that the SSL handshake was aborted.
Finish msg split across ssl recs	Number of times that the SSL Finished message was split by the client into multiple SSL records.
Fasttx msg ring full	Debug tools for use by Cisco personnel only.
SSL_ME tx msg	
N2 . . .	

1. For more information, see the "Information about SSL HTTP Header Insertion and Truncated Counters" section.

Information about SSL HTTP Header Insertion and Truncated Counters

When you configure the ACE for SSL HTTP header insertion, the ACE creates a build of the HTTP header information during the SSL handshake with the client. This information is based on the SSL negotiated session parameters, client certificate parameters, or server certificate parameters that you specify in the action list. When the ACE receives the session's first HTTP request, it performs the HTTP header insert operation and inserts the HTTP header build.

While the ACE is creating the HTTP header build, it uses the following counters to track the success rate of the information being inserted:

- "(header type) headers extracted" counters—The ACE increments the corresponding header type counter (session, server certificate, or client certificate) by the number of headers that it can successfully add to the information being built for the HTTP header insertion operation.
- "(header type) headers failed" counters—The ACE increments the corresponding header type counter (session, server certificate, or client certificate) by the number of headers that it is unable to add to the information being built for the HTTP header insertion operation. The ACE is unable to insert a header because it encounters either an internal error (such as not being able to allocate memory) or an error when parsing a certificate field (for example, the certificate has an invalid date specified date field).
- Headers truncated—The ACE increments this counter every time it truncates a header because the combined header information exceeds 512 bytes.

The ACE creates only one build of the header information per session, which means that it inserts the same build even when you configure the ACE to insert the information into all the HTTP requests that it receives during the session. Because the same build is used for all session HTTP requests, the counters increment during the build process only and not every time the ACE performs the HTTP header insertion operation. For information about the counters that track the success rate of the HTTP header insertion operation, see the "Displaying HTTP Header Insertion Statistics" section.

Note It is possible for the ACE to extract the header information during the SSL handshake but not insert the information into the HTTP request. This situation can occur if the SSL handshake fails after the ACE extracts the header information but before it receives the first GET. When this situation occurs, the SSL counters increment but the HTTP counters do not increment.

Displaying HTTP Header Insertion Statistics

You can display HTTP statistics, including information relating to the HTTP headers that contain SSL session information, by using the **show stats http** command in Exec mode. The syntax of this command is as follows:

show stats http

Table 6-13 describes the fields in the **show stats http** command output relating to the HTTP headers that provide the server with SSL session information. For information about the other fields that display with this command, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*.

Table 6-13 Field Descriptions for the show stats http Command

Field	Description
SSL headers inserted	Number of times that the ACE successfully performed the HTTP header insert operation by inserting all of the HTTP headers that contain SSL session information defined in the corresponding action list into the HTTP request.

Table 6-13 Field Descriptions for the show stats http Command

Field	Description
SSL header insert errors	Number of times that the ACE failed to perform the HTTP header insert operation completely because it could not insert the HTTP headers that contain the SSL session information defined in the corresponding action list.
SSL spoof headers deleted	Number of times that the ACE deleted an HTTP header from the HTTP request that it received over the client connection. To prevent HTTP header spoofing, the ACE deletes any incoming HTTP headers that contain SSL session information that matches any of the headers that it has to insert.