SSL-Proxy-List Configuration Mode Commands

The ssl-proxy list configuration mode allows you to configure an SSL proxy configuration list on a CSS containing an SSL Acceleration module. An SSL proxy configuration list is a group of related virtual or back-end SSL servers that are associated with an SSL service. The SSL modules in the CSS use the virtual servers to properly process and terminate SSL communications between the client and the Web server. The SSL module uses the back-end SSL servers to initiate a connection between the module and the back-end SSL server.

To access ssl-proxy-list configuration mode, use the **ssl-proxy-list** command from any configuration mode except from the ACL, boot, group, RMON, or owner configuration modes. The prompt changes to (ssl-proxy-list [*name*]). You can also use this command from this mode to access another SSL proxy list. For information about commands available in this mode, see the commands in this section.

In global configuration mode, use the **no** form of this command to remove an existing SSL-proxy list.

ssl-proxy-list *name*

(config) **no ssl-proxy-list** *name*

Syntax Description

name	Name of a new SSL proxy list you want to create or an existing list you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing names, enter: `(config)# ssl-proxy-list ?`

Usage Guidelines

You add an active SSL proxy list to a service (an **ssl-accel** type for a virtual SSL server and an **ssl-accel-backend** type for a back-end SSL server) to initiate the transfer of SSL configuration data for the SSL Acceleration Module. The SSL services are added to SSL content rules.

You cannot delete an SSL proxy list if an SSL service is in use and contains the active SSL proxy list. You must first suspend the SSL service to delete a specific list.

Each SSL proxy list can have a maximum of 256 virtual or back-end SSL servers.

Each service may have only one SSL proxy list configured on it. You may only have one active SSL service for each slot in the chassis. You can configure more than one on a slot but only one can be activated at a time.

Content rules can have multiple SSL services.

For detailed information on SSL and SSL proxy lists, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl-proxy-list
(config-service) add ssl-proxy-list
(config-service) remove ssl-proxy-list
(config-service) slot

(ssl-proxy-list) active

To activate the specified SSL proxy list, use the **active** command.

active

Usage Guidelines

Before you can activate an SSL proxy list, ensure that you create at least one server in the list. The CSS checks the SSL proxy list servers to verify that all of the necessary components are configured, including verifying the certificate and key pair against each other. If the verification fails, the certificate name is not accepted and the CSS logs the following error message and does not activate the SSL proxy list.

```
Certificate and key pair do not match
```

You must either remove the configured key pair or configure an appropriate certificate.

You cannot modify an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

Related Commands

(ssl-proxy-list) suspend

(ssl-proxy-list) backend-server

To create a back-end SSL server and configure it for an SSL proxy list, use the **backend-server** *number* command. Use the **no** form of the **backend-server** *number* command to delete the back-end server. For information on the other **no** forms of this command, see the commands in the following sections.

backend-server *number* {**cacert**...|**cipher**...|**dhparam**...|**dsacert**...|**dsakey**... |**handshake**...|**ip address**...|**port**...|**rsacert**...|**rsakey**...|**server-ip**... |**server-port**...|**session-cache**...|**tcp**...|**type**...|**version**...}

no backend-server *number* {**cacert**...|**cipher**...|**dhparam**...|**dsacert**... |**dsakey**...|**handshake**...|**ip address**...|**port**...|**rsacert**...|**rsakey**... |**server-ip**...|**server-port**...|**session-cache**...|**tcp**...|**type**...|**version**...}

Syntax Description

number	The index number for the SSL server. This variable without an option creates a back-end server. When you enter this variable with an option, the number identifies the server for configuration. An SSL proxy list can have a maximum of 256 servers. Enter a number from 1 to 256.
cacert...	(Optional) Specifies the certificate authority (CA) certificate of the SSL server. See the **backend-server number cacert** command.
cipher...	(Optional) Specifies the cipher suite for the server. See the **backend-server number cipher** command.
dhparam...	(Optional) Specifies the Diffie-Hellman parameter file for the back-end server. See the **backend-server number dhparam** command.
dsacert...	(Optional) Specifies the back-end server DSA certificate. See the **backend-server number dsacert** command.
dsakey...	(Optional) Specifies the back-end server DSA key name. See the **backend-server number dsakey** command.
handshake...	(Optional) Specifies the handshake negotiation data and timeout value for the server. See the **backend-server number handshake** command.

ip address...	(Optional) Specifies an IP address for the server. This IP address corresponds to the address of the service. See the **backend-server number ip address** command.
port...	(Optional) Specifies a virtual TCP port for the server. See the **backend-server number port** command.
rsacert...	(Optional) Specifies the back-end server RSA certificate. See the **backend-server number rsacert** command.
rsakey...	(Optional) Specifies the back-end server RSA key pair name. See the **backend-server number rsakey** command.
server-ip	(Optional) Specifies the IP address for the back-end SSL server. See the **backend-server number server-ip** command.
server-port	(Optional) Specifies the port for the back-end SSL server. See the **backend-server number server-port** command.
session-cache...	(Optional) Specifies the session cache timeout value for the server. See the **backend-server number session-cache** command.
tcp...	(Optional) Specifies a timeout value to terminate a TCP connection or specifies the Nagle algorithm for a TCP connection. See the **backend-server number tcp** command.
type...	(Optional) Specifies that the back-end server is either a back-end SSL server or an SSL initiation server. See the **backend-server number type** command.
version...	(Optional) Specifies the SSL or Transport Layer Security (TLS) protocol version. See the **backend-server number version** command.

Usage Guidelines

You must create a back-end SSL server before you can configure its parameters.

backend-server *number* cacert

To configure the certificate authority (CA) certificate, use the **backend-server** *number* **cacert** *name* command. Configuring this command in the SSL proxy list allows the CSS to use the public key in the CA certificate to verify the digital signature of the CA in the SSL server certificate. Use the **no** form of this command to remove the configured CA certificate from the SSL proxy list.

backend-server *number* **cacert** *name*

no backend-server *number* **cacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
cacert	Specifies a CA certificate.
name	Name of the CA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The CA certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* cipher

To assign a cipher suite to the back-end SSL server, use the **backend-server** *number* **cipher** command. For each available SSL version, there is a distinct list of supported cipher suites representing a selection of cryptographic algorithms and parameters. Your choice depends on your environment, certificates and keys in use, and security requirements. By default, all supported cipher suites are enabled. Use the **no** form of this command to remove a cipher suite from the server.

backend-server *number* **cipher** *name* {**weight** *number*}

no backend-server *number* **cipher**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
name	The name of a specific cipher suite. See the "Usage Guidelines" section.
weight *number*	(Optional) Assigns a priority to the cipher suite, with 10 being the highest weight. When negotiating which cipher suite to use, the SSL module selects from the client list based on the cipher suite configured with the highest weight. To set the weight for a cipher suite, enter a number from 1 to 10. By default, all configured cipher suites have a weight of 1.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Table 2-5 lists all supported cipher suites and values for the specific SSL server (and corresponding SSL proxy list). The table also lists whether those cipher suites are exportable from the CSS, along with the authentication certificate and encryption key required by the cipher suite.

If you use the default setting or select the **all-cipher-suite** option, the CSS sends the suites in the same order as they appear in Table 2-5, starting with rsa-with-rc4-128-md5.

Note The **all-cipher-suites** setting works only when no specifically-defined ciphers are configured. To return to using the **all-cipher-suites** setting, you must remove all specifically-defined ciphers.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to man-in-the-middle attacks and is strongly discouraged.

Table 2-5 SSL Cipher Suites Supported by the CSS

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
all-cipher-suites	No	RSA certificate, DSA certificate	RSA key exchange, Diffie-Hellman
rsa-with-rc4-128-md5	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-sha	No	RSA certificate	RSA key exchange
rsa-with-des-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-3des-ede-cbc-sha	No	RSA certificate	RSA key exchange
dhe-dss-with-des-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-dss-with-3des-ede-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-rsa-with-des-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-with-3des-ede-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dh-anon-with-rc4-128-md5	No	Neither party is authenticated	Diffie-Hellman

Table 2-5 SSL Cipher Suites Supported by the CSS (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
dh-anon-with-des-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-3des-ede-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dhe-dss-with-rc4-128-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export-with-rc4-40-md5	Yes	RSA certificate	RSA key exchange
rsa-export-with-des40-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export-with-des40-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-export-with-des40-cbc-sha	Yes	RSA certificate	Ephemeral Diffie-Hellman
dh-anon-export-with-rc4-40-md5	Yes	Neither party is authenticated	Diffie-Hellman
dh-anon-export-with-des40-cbc-sha	Yes	Neither party is authenticated	Diffie-Hellman
rsa-export1024-with-des-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-des-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export1024-with-rc4-56-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-rc4-56-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman

Related Commands **show ssl-proxy-list**

backend-server *number* dhparam

To configure the back-end server Diffie-Hellman (DH) parameter file, use the **backend-server** *number* **dhparam** *name* command. Use the **no** form of this command to remove the configured DH parameter file from the SSL proxy list.

backend-server *number* **dhparam** *name*

no backend-server *number* **dhparam**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dhparam	Specifies a Diffie-Hellman parameter file.
name	Name of the DH parameter file. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The DH parameters file must already be loaded on the SCM. If the parameter file does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* dsacert

To configure the back-end server DSA certificate, use the **backend-server** *number* **dsacert** *name* command. Use the **no** form of this command to remove the configured DSA certificate from the SSL proxy list.

backend-server *number* **dsacert** *name*

no backend-server *number* **dsacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dsacert	Specifies a DSA certificate.
name	Name of the DSA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* dsakey

To configure the back-end server DSA key pair name, use the **backend-server** *number* **dsakey** *name* command. Use the **no** form of this command to remove the configured DSA key pair from the SSL proxy list.

backend-server *number* **dsakey** *name*

no backend-server *number* **dsakey**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dsakey	Specifies a DSA key pair.
name	Name of the DSA key pair. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The key pair must already be loaded on the SCM. If the key pair name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* handshake

To configure SSL session handshake renegotiation to reestablish an SSL session between the SSL module and the back-end SSL server, use the **backend-server** *number* **handshake** command. This command sends the SSL HelloRequest message to a client to restart SSL handshake negotiation. Reestablishing the SSL handshake is useful in instances when a connection has been established for a lengthy period of time and you want to ensure security by reestablishing the SSL session. Use the **no** form of this command to disable handshake data exchange or timeout.

backend-server *number* **handshake** [**data** *kbytes*|**timeout** *seconds*]

no backend-server *number* **handshake data**|**timeout**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
data *kbytes*	Sets the maximum amount of data to be exchanged between the CSS and the back-end SSL server, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *kbytes* variable is the SSL handshake data value in Kbytes. Enter a value from 0 to 512000. The default is 0, disabling the handshake data exchange.
timeout *seconds*	Sets a maximum timeout value, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *seconds* variable is the SSL handshake timeout value in seconds. Enter a value from 0 to 72000 (20 hours). The default is 0, disabling the handshake timeout.

Command Modes

ssl-proxy-list configuration mode

Related Commands **show ssl-proxy-list**

backend-server *number* ip address

To specify an IP address for the back-end SSL server, use the **backend-server** *number* **ip address** command. The IP address corresponds to the address of the service. Use the **no** form of this command to remove the address from the server.

backend-server *number* **ip address** *ip_or_host*

no backend-server *number* **ip address**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
ip address *ip_or_host*	IP address that corresponds to the address of the service. Enter a valid VIP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes ssl-proxy-list configuration mode

Usage Guidelines When you use the mnemonic host-name format for the address, the CSS includes a Domain Name System (DNS) facility that translates host names to IP addresses. If the host name cannot be resolved, the IP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name System, refer to the *Cisco Content Services Switch Administration Guide.*

If the IP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
SSL-server/Backend-server must have valid IP Address
```

Related Commands **show ssl-proxy-list**
(ssl-proxy-list) active

backend-server *number* port

To specify a virtual TCP port number for the back-end SSL server, use the **backend-server** *number* **port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

backend-server *number* **port** *number2*

no backend-server *number* **port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
port *number2*	TCP port number that matches the TCP port number for an SSL content rule. The SSL module uses the port to determine which traffic it should accept. Enter a port number from 1 to 65535. The default port is 80.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines If you configure the **backend-server** *number* **ip address** and **server-ip** commands with the same address, configure the **backend-server** *number* **port** and **server-port** commands with different port numbers.

Related Commands **show ssl-proxy-list**
(config-owner-content) port

backend-server *number* rsacert

To configure the back-end server RSA certificate, use the **backend-server** *number* **rsacert** *name* command. Use the **no** form of this command to remove the configured RSA certificate from the SSL proxy list.

backend-server *number* **rsacert** *name*

no backend-server *number* **rsacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
rsacert	Specifies an RSA certificate.
name	Name of the RSA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines The certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands **show ssl-proxy-list**
(ssl-proxy-list) active

backend-server *number* rsakey

To configure the back-end server RSA key pair name, use the **backend-server** *number* **rsakey** *name* command. Use the **no** form of this command to remove the configured RSA key pair from the SSL proxy list.

backend-server *number* **rsakey** *name*

no backend-server *number* **rsakey**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
rsakey	Specifies an RSA key pair.
name	Name of the RSA key pair. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The key pair must already be loaded on the SCM. If the key pair name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* server-ip

To specify an IP address for the back-end SSL server, use the **backend-server** *number* **server-ip** command. Use the **no** form of this command to remove the address from the server.

backend-server *number* **server-ip** *ip_or_host*

no backend-server *number* **server-ip**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
server-ip *ip_or_host*	IP address for the server. Enter a valid IP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

When you use the mneumonic host-name format for the VIP, the CSS includes a Domain Name Service (DNS) facility that translates host names such as myhost.mydomain.com to IP addresses such as 192.168.11.1. If the host name cannot be resolved, the VIP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name Service, refer to the *Cisco Content Services Switch Administration Guide.*

If the IP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
SSL-server/Backend-server must have valid IP Address
```

Related Commands **show ssl-proxy-list**
(ssl-proxy-list) active
(config-owner-content) vip address

backend-server *number* server-port

To specify a port number for the back-end SSL server, use the **backend-server** *number* **server-port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

backend-server *number* **server-port** *number2*

no backend-server *number* **server-port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
server-port *number2*	The port number for the back-end SSL server. Enter a port number from 1 to 65535. The default port is 443.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines If you configure the **backend-server** *number* **ip address** and **server-ip** commands with the same address, configure the **backend-server** *number* **port** and **server-port** commands with different port numbers.

Related Commands **show ssl-proxy-list**
(config-owner-content) port

backend-server *number* session-cache

To set the SSL cache timeout value, use the **backend-server** *number* **session-cache** command. In SSL, a new session ID is created every time the SSL module and back-end SSL server go through a full key exchange and establish a new master secret key. Specifying an SSL session cache timeout allows the reuse of the master key on subsequent connections between the client and the CSS SSL module, which can speed up the SSL negotiation process. Use the **no** form of this command to reset the SSL session reuse timeout back to 300 seconds.

backend-server *number* **session-cache** *seconds*

no backend-server *number* **session-cache**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
seconds	SSL session cache timeout in seconds. Enter a value from 0 to 72000 (20 hours). The default is 300 seconds (5 minutes). To disable the timeout, set the value to 0. The full SSL handshake occurs for each new connection between the client and the SSL module.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list

backend-server *number* tcp

To configure TCP connections with a back-end server, use the **backend-server** *number* **tcp** command. You can specify:

- A timeout value that the CSS uses to terminate a TCP connection for inactivity or for an unsuccessful TCP three-way handshake with a back-end SSL server
- The Nagle algorithm for the TCP connection

Use the **no** form of this command to reset the buffer size to 32768, restore the timeout period to 240 seconds for inactivity or 30 seconds for the three-way handshake.

backend-server *number* **tcp** [**buffer-share** [**rx**|**tx**] *number2*|[**server**|**virtual**] **inactivity-timeout** *seconds*|**nagle** [**enable**|**disable**]|**syn-timeout** *seconds2*]

no backend-server *number* **tcp** [**buffer-share** [**rx**|**tx**]| [**server**|**virtual**] **inactivity-timeout** |**syn-timeout**]

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
buffer-share [**rx**|**tx**] *number2*	Sets the TCP buffering from the client or server on a given connection. • To set the amount of data in bytes that a given connection can buffer from the client traffic, use the **rx** *number2* keyword and variable. • To set the amount of data in bytes that a given connection can buffer from the server to the client, use the **tx** *number2* keyword and variable. By default, the buffer size is 32768. The buffer size can range from 16400 to 262144.
server	Specifies the TCP connection for the back-end SSL server.

virtual	Specifies the TCP connection for the client.
inactivity-timeout *seconds*	Specifies the timeout value that the CSS waits to receive inbound flows before terminating the TCP connection. Enter a TCP inactivity timeout value in seconds, from 0 (disabling the TCP inactivity timeout) to 3600 (1 hour). The default is 240 seconds.
nagle enable|**disable**	Specifies the Nagle algorithm for the TCP connection. By default, the Nagle algorithm is enabled for each TCP connection. Use the **disable** keyword to disable the Nagle algorithm when you observe an unacceptable delay in the TCP connection. Use the **enable** keyword to reenable the Nagle algorithm.
syn-timeout *seconds2*	Specifies a timeout value that the CSS uses to terminate a TCP connection with client or a server that has not successfully completed the TCP three-way handshake prior to transferring data. Enter a TCP SYN timeout value in seconds, from 0 to 3600 (1 hour). The default is 30 seconds. To disable the TCP SYN timeout period, set the value to 0. The timer becomes inactive and the retransmit timer eventually terminates a broken TCP connection. The connection timer should always be shorter than the retransmit termination time for new SSL/TCP connections.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The TCP Nagle algorithm automatically concatenates a number of small buffer messages transmitted over the TCP connection between a client and the SSL module or between a back-end server and the SSL module. This process increases the throughput of your CSS by decreasing the number of packets sent over each TCP connection. However, the interaction between the Nagle algorithm and the TCP delay acknowledgment may increase latency in your TCP connection. Disable the Nagle algorithm when you observe an unacceptable delay in a TCP connection (clear-text or SSL).

Related Commands **show ssl-proxy-list**

backend-server *number* type

To configure a back-end SSL server as an SSL initiation server or to reconfigure an SSL initiation server as a back-end SSL server (the default), use the **backend-server** *number* **type** command. An SSL initiation server allows a CSS to accept clear text from a client and to initiate an SSL session with an SSL server. Use the **no** form of this command to reset the back-end server type to the default of **backend-ssl**.

backend-server *number* **type** [**backend-ssl**|**initiation**]

no backend-server *number* **type**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
type	Keyword that specifies the type of back-end server on the CSS.
backend-ssl	(Default) Specifies a back-end SSL server that allows a CSS to: • Receive encrypted data from a client • Decrypt the data for load balancing • Re-encrypt the data and send it to an SSL server over an SSL connection **Note** Use back-end SSL with SSL termination. For information about SSL termination, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
initiation	Specifies an SSL initiation server that allows a CSS to: • Receive clear text from a client • Encrypt the data and send it to an SSL server over an SSL connection

Command Modes ssl-proxy-list configuration mode

Usage Guidelines By default, a back-end server is a server of type **backend-ssl** for use with services of type **ssl-accel-backend**. To use the back-end server for SSL initiation, you must configure it as an initiation server for use with services of type **ssl-accel**. If you have configured an SSL initiation server and want to reconfigure it as a back-end SSL server, enter the **backend-server** *number* **type backend-ssl** command.

Related Commands **show ssl-proxy-list**
(ssl-proxy-list) active

backend-server *number* version

To specify the SSL or Transport Layer Security (TLS) protocol version, use the **backend-server** *number* **version** command. Use the **no** form of the command to reset the default SSL version setting to SSL version 3.0 and TLS version 1.0. The SSL module sends a ClientHello that has an SSL version 3 header with the ClientHello message set to TLS version 1.0.

backend-server *number* **version** *protocol*

no backend-server *number* **version**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
protocol	Protocol version. Enter one of the following keywords: • **ssl-tls** - SSL protocol version 3.0 and TLS protocol version 1.0 (default). • **ssl** - SSL protocol version 3.0 • **tls** - TLS protocol version 1.0

Command Modes ssl-proxy-list configuration mode

Usage Guidelines The CSS supports SSL version 3.0 and TLS version 1.0. The CSS understands and accepts an SSL version 2.0 ClientHello message to allow dual version clients to communicate with the CSS through the SSL module. In this case, the client indicates an SSL version of 3.0 in the version 2.0 ClientHello. This indicates to the SSL module that the client can support SSL version 3.0, and the SSL module returns a version 3.0 ServerHello message.

If the client only supports SSL version 2.0 (SSL version 2.0 compliant), the CSS cannot to pass network traffic.

Related Commands **show ssl-proxy-list**

(ssl-proxy-list) description

To provide a description for the SSL proxy list, use the **description** command.

description "*text***"**

Syntax Description

"*text***"**	Description for the SSL proxy list. Enter a quoted text string with a maximum length of 64 characters including spaces.

(ssl-proxy-list) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in this mode.

Syntax Description

no acl *index*	Deletes an ACL.
no backend-server *number*	Removes the back-end SSL server from the SSL proxy list.

no backend-server *number* **cacert**	Removes the CA certificate from the SSL proxy list.
no backend-server *number* **cipher**	Removes the cipher suite from the back-end SSL server.
no backend-server *number* **dhparam**	Removes the DH parameter file from the SSL proxy list.
no backend-server *number* **dsacert**	Removes the DSA certificate from the SSL proxy list.
no backend-server *number* **dsakey**	Removes the DSA key pair name from the SSL proxy list.
no backend-server *number* **handshake data**	Disables the handshake data exchange.
no backend-server *number* **handshake timeout**	Disables the handshake timeout period.
no backend-server *number* **ip address**	Removes the IP address from the back-end SSL server. The IP address corresponds to address of the service.
no backend-server *number* **port**	Resets the port number to 80.
no backend-server *number* **rsacert**	Removes the RSA certificate from the SSL proxy list.
no backend-server *number* **rsakey**	Removes the RSA key pair name from the SSL proxy list.
no backend-server *number* **server-ip**	Removes the IP address from the back-end SSL server.
no backend-server *number* **server-port**	Resets the port number to 443.
no backend-server *number* **session-cache**	Resets the SSL session reuse timeout to 300 seconds.
no backend-server *number* **tcp server inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the back-end SSL server and the CSS.
no backend-server *number* **tcp server syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the back-end SSL server and the CSS.

no backend-server *number* **tcp virtual inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the server and the CSS.
no backend-server *number* **tcp virtual syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the server and the CSS.
no backend-server *number* **version**	Resets the SSL version to the default of SSL version 3.0 and TLS version 1.0.
no description	Removes the description for an SSL proxy list.
no ssl-server *number*	Removes the virtual SSL server from the SSL proxy list.
no ssl-server *number association_type*	Removes the association from the virtual SSL server. The association type is **dhparam**, **dsacert**, **dsakey**, **rsacert**, or **rsakey**.
no ssl-server *number* **cacert** *name*	Removes a CA certificate association from the virtual SSL server.
no ssl-server *number* **cipher**	Removes the cipher suite from the virtual SSL server.
no ssl-server *number* **crl** *crl_record_name*	Removes the CRL from the virtual SSL server.
no ssl-server *number* **failure-url**	Removes the redirect URL used by the **ssl-server** *number* **failure redirect** command.
no ssl-server *number* **handshake data**	Disables the handshake data exchange.
no ssl-server *number* **handshake timeout**	Disables the handshake timeout period.
no ssl-server *number* **http-header client-cert**	Disables the insertion of client certificate fields and information in the HTTP request header.
no ssl-server *number* **http-header prefix**	Deletes the configured prefix for client certificate fields, server certificate fields, or session fields inserted in the HTTP request header.
no ssl-server *number* **http-header server-cert**	Disables the insertion of server certificate fields and information in the HTTP request header.
no ssl-server *number* **http-header session**	Disables the insertion of SSL session fields and information in the HTTP request header.

no ssl-server *number* **http-header static**	Disables the insertion of the static string in the HTTP request header and deletes the string.
no ssl-server *number* **port**	Resets the port number to 443.
no ssl-server *number* **session-cache**	Resets the SSL session reuse timeout to 300 seconds.
no ssl-server *number* **tcp server inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the web server and the CSS.
no ssl-server *number* **tcp server syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the web server and the CSS.
no ssl-server *number* **tcp virtual inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the client and the CSS.
no ssl-server *number* **tcp virtual syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the client and the CSS.
no ssl-server *number* **unclean-shutdown**	Resets the CSS default behavior of sending both a Close-Notify alert and a TCP FIN message to close the client connection.
no ssl-server *number* **urlrewrite**	Removes a URL rewrite rule from the virtual SSL server.
no ssl-server *number* **version**	Resets the SSL version to the default of SSL version 3.0 and TLS version 1.0.
no ssl-server *number* **vip address**	Removes the VIP address from the virtual SSL server.

(ssl-proxy-list) show ssl-proxy-list

To display information about the current SSL proxy configuration list, use the **show ssl-proxy-list** command. You can display detailed information about the list, or a virtual or back-end server in the list.

show ssl-proxy-list {**ssl-server**|**backend-server** {*number*}}

Syntax Description

ssl-server	(Optional) Displays information for all virtual SSL servers in the list.
backend-server	(Optional) Displays information for the back-end SSL servers in the list.
number	(Optional) Displays information for a specific virtual or back-end SSL server.

Usage Guidelines

For information on using the **show ssl-proxy-list** command to display information about other SSL proxy lists, see the **show ssl-proxy-list** command in the "General Commands" section.

The **show ssl-proxy-list** command without an option displays detailed configuration information about the current SSL proxy list.

For information about the fields in the **show ssl-proxy-list** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) ssl-proxy-list
(ssl-proxy-list) description
(ssl-proxy-list) ssl-server

(ssl-proxy-list) ssl-server

To create a virtual SSL server and configure it for an SSL proxy list, use the **ssl-server** command. Use the **no** form of the **ssl-server** command to delete the SSL server. For information on the other **no** forms of this command, see the commands in the following section.

ssl-server *number* {*association_type*...|**authentication**|**cacert**...
|**cipher**...|**crl**...|**failure**...|**failure-url**...|**handshake**...|**http-header**...
|**port**...|**session-cache**...|**ssl-queue-delay**...|**tcp**...|**unclean-shutdown**
|**urlrewrite**...|**version**...|**vip address**...}

no ssl-server *number*{*association_type*...|**authentication**|**cacert**...
|**cipher**...|**crl**...|**failure-url**|**handshake**....|**http-header**...|**port**...
|**session-cache**...|**ssl-queue-delay**|**tcp**...|**unclean-shutdown**
|**urlrewrite**...|**version**...|**vip address**...}

Syntax Description

number	The index number for the virtual SSL server. This variable without an option creates a server. When you enter this variable with an option, the number identifies the server for configuration. An SSL proxy list can have a maximum of 256 virtual servers. Enter a number from 1 to 256.
association_type...	(Optional) Creates a key pair, certificate, or key parameter association for the server. See the **ssl-server number association_type** command.
authentication	(Optional) Specifies whether to enable or disable client authentication. See the **ssl-server number authentication** command.
cacert	(Optional) Assigns the certificate association to the virtual SSL server. See the **ssl-server number cacert** command.
cipher...	(Optional) Specifies the cipher suite for the server. See the **ssl-server number cipher** command.
crl...	(Optional) Assigns the CRL record to the server. See the **ssl-server number crl** command.
failure...	(Optional) Specifies how the CSS handles a client authentication failure. See the **ssl-server number failure** command.
failure-url...	(Optional) Specifies the URL to redirect a client connection when a failure occurs and the CSS is configured to redirect the connection. See the **ssl-server number failure-url** command.
handshake...	(Optional) Specifies the handshake negotiation data and timeout value for the server. See the **ssl-server number handshake** command.

http-header...	(Optional) Specifies the information to insert in the HTTP request header to a back-end server. See the **ssl-server number http-header** command.
port...	(Optional) Specifies a virtual TCP port for the server. See the **ssl-server number port** command.
session-cache...	(Optional) Specifies the session cache timeout value for the server. See the **ssl-server number session-cache** command.
ssl-queue-delay...	(Optional) Specifies the time to wait before sending queued data for encryption. See the **ssl-server number ssl-queue-delay** command.
tcp...	(Optional) Specifies a timeout value to terminate a TCP connection, the Nagle algorithm for a TCP connection, or buffer size for the TCP connection. See the **ssl-server number tcp** command.
unclean-shutdown	(Optional) Instruct the CSS to send only a TCP FIN message to terminate a client connection (the CSS does not send a Close Notify alert). See the **ssl-server number unclean-shutdown** command.
urlrewrite...	(Optional) Adds a URL rewrite rule to the virtual SSL server to avoid nonsecure HTTP 300-series redirects by the server. See the **ssl-server number urlrewite** command.
version...	(Optional) Specifies the SSL or Transport Layer Security (TLS) protocol version. See the **ssl-server number version** command.
vip address...	(Optional) Specifies a VIP address for the server. See the **ssl-server number vip address** command.

Usage Guidelines

You must create a virtual SSL server before you can configure its parameters.

You cannot modify a server in an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

ssl-server *number association_type*

To specify the certificate, key pair, or Diffie-Hellman key exchange parameter file association for the virtual SSL server, use the **ssl-server** *number association_type* command. Use the **no** form of this command to remove the association.

ssl-server *number association_type name*

no ssl-server *number association_type*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
association_type	Identifies the association type. Enter one of the following options: • **dhparam** - A Diffie-Hellman key exchange parameter file association. The Diffie-Hellman key exchange parameter file ensures that the two sides in a data exchange cooperate to generate a symmetric (shared) key for packet encryption and authentication. • **dsacert** - A DSA certificate association to be used in the exchange of digital signatures. • **dsakey** - A DSA key pair association. DSA key pairs are used to sign packet data, and they are a requirement before another device (client or web server) can exchange an SSL certificate with the CSS. • **rsacert** - An RSA certificate association to be used in the exchange of a public and private key pair for authentication and packet encryption. • **rsakey** - An RSA key pair association. RSA key pairs are a requirement before another device (client or web server) can exchange an SSL certificate with the CSS.
name	The name of the association. To see a list of existing associations, use the **ssl-server** *number association_type* **?** command.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines The certificate, key pair, or Diffie-Hellman parameter file must already be loaded on the CSS and an association made. If there is not a proper association upon activation of the SSL proxy list, the CSS logs an error message and does not activate the list.

Related Commands
copy ssl
show ssl-proxy-list
(config) ssl associate

ssl-server *number* authentication

To enable or disable client authentication on a virtual SSL server, use the **ssl-server** *number* **authentication** command. By default, client authentication is disabled. Use the **no** form of this command or the **disable** keyword to disable client authentication on the virtual SSL server.

ssl-server *number* **authentication** [**enable**|**disable**]

no ssl-server *number* **authentication**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
enable	Enables client authentication on the virtual SSL server.
disable	Disables client authentication on the virtual SSL server (default).

Command Modes ssl-proxy-list configuration mode

Usage Guidelines After you enable client authentication on the CSS, you must specify a CA certificate that the CSS uses to verify client certificates.

Related Commands
show ssl statistics
show ssl-proxy-list ssl-server
(config) ssl associate
(config-ssl-proxy-list) ssl-server number cacert

ssl-server *number* cacert

To assign a Certificate Authority (CA) certificate association to a virtual SSL server, use the **ssl-server** *number* **cacert** command. Use the **no** form of this command to remove a CA certificate association from the virtual SSL server.

ssl-server *number* **cacert** *association_name*

no ssl-server *number* **cacert** *association_name*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
association_name	Name of the CA certificate association. To see a list of existing associations, use the **ssl-server** *number* **cacert ?** command.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines If you configure a virtual SSL server for client authentication, you must configure the server with a CA certificate. The CSS uses the public key in the certificate to verify the digital signature in the client certificate.

Before you configure the CA certificate on a virtual SSL server, you must import the CA certificate on the CSS and then associate it to a filename.

You must configure at least one certificate; however, you can configure a maximum of four. If you try to configure more than four certificates, the CSS displays an error message.

You must configure a CA certificate before you activate the SSL proxy list.

Related Commands

copy ssl
show ssl-proxy-list ssl-server
(config) ssl associate
(config-ssl-proxy-list) ssl-server number authentication

ssl-server *number* cipher

To assign a cipher suite to the virtual SSL server, use the **ssl-server** *number* **cipher** command. For each available SSL version, there is a distinct list of supported cipher suites representing a selection of cryptographic algorithms and parameters. Your choice depends on your environment, certificates and keys in use, and security requirements. By default, no supported cipher suites are enabled. Use the **no** form of this command to remove a cipher suite from the server.

ssl-server *number* **cipher** *name ip_or_host port* {**weight** *number*}

no ssl-server *number* **cipher**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
name	The name of a specific cipher suite. See the "Usage Guidelines" section for detailed information.
ip_or_host	IP address to assign to the back-end content rule/server used with the cipher suite. Specify the IP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

port	TCP port of the back-end content rule/server through which the back-end HTTP connections are sent.
weight *number*	(Optional) Assigns a priority to the cipher suite, with 10 being the highest weight. When negotiating which cipher suite to use, the SSL module selects from the client list based on the cipher suite configured with the highest weight. To set the weight for a cipher suite, enter a number from 1 to 10. By default, all configured cipher suites have a weight of 1.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Table 2-6 lists all supported cipher suites and values for the specific SSL server (and corresponding SSL proxy list). The table also lists whether those cipher suites are exportable from the CSS, along with the authentication certificate and encryption key required by the cipher suite.

If you use the default setting or select the **all-cipher-suite** option, the CSS sends the suites in the same order as they appear in Table 2-6, starting with rsa-with-rc4-128-md5.

Note The **all-cipher-suites** setting works only when no specifically-defined ciphers are configured. To return to using the **all-cipher-suites** setting, you must remove all specifically-defined ciphers.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to man-in-the-middle attacks and is strongly discouraged.

Table 2-6 SSL Cipher Suites Supported by the CSS

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
all-cipher-suites	No	RSA certificate, DSA certificate	RSA key exchange, Diffie-Hellman
rsa-with-rc4-128-md5	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-sha	No	RSA certificate	RSA key exchange
rsa-with-des-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-3des-ede-cbc-sha	No	RSA certificate	RSA key exchange
dhe-dss-with-des-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-dss-with-3des-ede-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-rsa-with-des-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-with-3des-ede-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dh-anon-with-rc4-128-md5	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-des-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-3des-ede-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dhe-dss-with-rc4-128-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export-with-rc4-40-md5	Yes	RSA certificate	RSA key exchange
rsa-export-with-des40-cbc-sha	Yes	RSA certificate	RSA key exchange

Table 2-6 SSL Cipher Suites Supported by the CSS (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
dhe-dss-export-with-des40-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-export-with-des40-cbc-sha	Yes	RSA certificate	Ephemeral Diffie-Hellman
dh-anon-export-with-rc4-40-md5	Yes	Neither party is authenticated	Diffie-Hellman
dh-anon-export-with-des40-cbc-sha	Yes	Neither party is authenticated	Diffie-Hellman
rsa-export1024-with-des-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-des-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export1024-with-rc4-56-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-rc4-56-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman

Related Commands **show ssl-proxy-list**

ssl-server *number* crl

To assign a certificate revocation list (CRL) record to a virtual SSL server, use the **ssl-server** *number* **crl** command. Use the **no** form of this command to remove the CRL from the virtual SSL server.

ssl-server *number* **crl** *crl_record_name*

no ssl-server *number* **crl** *crl_record_name*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
crl_record_name	Name of the configured CRL record. To see a list of existing associations, use the **ssl-server** *number* **crl ?** command.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Before you configure the CRL record on a virtual SSL server, you must configure the CRL record by using the global configuration **ssl crl-record** command.

You can configure only one CRL record for each SSL server.

Related Commands

show ssl crl-record
(config) ssl crl-record

ssl-server *number* failure

To configure how the CSS handles client authentication failures, use the **ssl-server** *number* **failure** command. A client certificate can fail if it is invalid, expired, or revoked by a CA. By default, the CSS rejects the client connection when client authentication fails.

ssl-server *number* **failure** [**ignore**|**redirect**|**reject**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
ignore	Ignores client authentication failures and allows both invalid and valid certificates to connect.
redirect	Sends client connections of a failed authentication to a configured URL. To configure the URL where the CSS redirects the client connection, use the **ssl-server number failure-url** command.
reject	Resets the CSS default behavior of rejecting the client connection when client authentication fails.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list ssl-server

ssl-server *number* failure-url

To configure the URL where the CSS redirects the client connection when authentication fails, use the **ssl-server** *number* **failure-url** command. Use this command when you configure the CSS to redirect connections through the **ssl-server** *number* **failure redirect** command. Use the **no** form of this command to remove the URL.

ssl-server *number* **failure-url** *url*

no ssl-server *number* **failure-url**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
url	URL to redirect the client connection when authentication fails. Enter a URL with a maximum of 168 characters and no spaces.

Usage Guidelines

To change an existing redirect URL, you must first remove the existing URL by using the **no ssl-server** *number* **failure-url** command. Then you can reissue the **ssl-server** *number* **failure-url** command to configure the new URL.

You must suspend an activated virtual SSL server before modifying it.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list ssl-server
ssl-server number failure redirect

ssl-server *number* handshake

To configure SSL session handshake renegotiation to reestablish an SSL session between the SSL module and a client, use the **ssl-server** *number* **handshake** command. This command send the SSL HelloRequest message to a client to restart SSL handshake negotiation. Reestablishing the SSL handshake is useful in instances when a connection has been established for a lengthy period of time and you want to ensure security by reestablishing the SSL session. Use the **no** form of this command to disable handshake data exchange or timeout.

ssl-server *number* **handshake** [**data** *kbytes*|**timeout** *seconds*]

no ssl-server *number* **handshake data**|**timeout**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
data *kbytes*	Sets the maximum amount of data to be exchanged between the CSS and the client, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *kbytes* variable is the SSL handshake data value in Kbytes. Enter a value from 0 to 512000. The default is 0, disabling the handshake data exchange.
timeout *seconds*	Sets a maximum timeout value, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *seconds* variable is the SSL handshake timeout value in seconds. Enter a value from 0 to 72000 (20 hours). The default is 0, disabling the handshake timeout.

Command Modes

ssl-proxy-list configuration mode

Related Commands **show ssl-proxy-list**

ssl-server *number* http-header

To insert client certificate, server certificate, SSL session, or static text information in the HTTP request header during a client connection, use the **ssl-server** *number* **http-header** command. You can also insert a prefix in SSL fields when you configure the insertion of client certificate, server certificate, or session information. Use the **no** form of this command to disable the insertion of information into the HTTP request header.

ssl-server *number* **http-header** [**client-cert**|**server-cert**|**session** |**prefix "***text_string***"**|**static "***text_string***"**]

no ssl-server *number* **http-header** [**client-cert**|**server-cert**|**session**|**prefix**|**static**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
client-cert	Inserts SSL client certificate fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
server-cert	Inserts SSL server certificate fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
session	Inserts SSL session fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

prefix "*text_string***"**	Changes the prefix on each HTTP inserted field when you configure the insertion of client certificate, server certificate, or SSL session information. By default, no prefix is added to each HTTP inserted field. Enter a quoted text string with a maximum of 16 characters.
static "*text_string***"**	Inserts a static text string in the HTTP request header to the back-end server. Enter a quoted text string with a maximum of 199 characters including spaces. For Microsoft Outlook Web Access (OWA) application support, enter the text string "FRONT-END-HTTPS: on". You can also insert multiple strings on different lines by using the \r\n characters in between each line. Note that these characters use 4 out of the 199 characters

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

During an SSL session, a client may need to pass specific information to a back-end server. HTTP request header insertion allows the embedding of information into an HTTP request header during a client connection. For example, when a client connects to the HTTP request head virtual SSL server and the CSS decrypts the data, the CSS can insert information about the SSL session and the client and server certificates into the HTTP request header, and then the CSS passes the header to the back-end server.

Note HTTP header insertion only occurs on the first HTTP request for a persistent HTTP 1.1 connection. Subsequent requests within the same TCP connection are sent unmodified. For HTTP 1.0, in which persistence is not implemented, all HTTP requests contain the inserted header.

The CSS can insert one or more of the following into the HTTP request header after it decrypts the client data:

- Client certificate fields and associated information

- Server certificate fields and associated information
- SSL session fields and associated information
- Static text string

You can also configure the CSS to place a prefix in the client certificate, server certificate, or SSL session fields inserted in the HTTP request header. The prefix has no effect on the insertion of a static text string.

The primary purpose of text string insertion through the **static** keyword is to support Microsoft OWA applications, however, you may have other reasons to insert static text.

Related Commands **show ssl-proxy-list ssl-server**

ssl-server *number* port

To specify a virtual TCP port number for the virtual SSL server, use the **ssl-server** *number* **port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

ssl-server *number* **port** *number2*

no ssl-server *number* **port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
port *number2*	TCP port number that matches the TCP port number for an SSL content rule. The SSL module uses the port to determine which traffic it should accept. Enter a port number from 1 to 65535. The default port is 443.

Command Modes ssl-proxy-list configuration mode

Related Commands **show ssl-proxy-list**
(config-owner-content) port

ssl-server *number* session-cache

To set the SSL cache timeout value, use the **ssl-server** *number* **session-cache** command. In SSL, a new session ID is created every time the client and CSS SSL module go through a full key exchange and establish a new master secret key. Specifying an SSL session cache timeout allows the reuse of the master key on subsequent connections between the client and the CSS SSL module, which can speed up the SSL negotiation process. Use the **no** form of this command to reset the SSL session reuse timeout back to 300 seconds.

ssl-server *number* **session-cache** *seconds*

no ssl-server *number* **session-cache**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
seconds	SSL session cache timeout in seconds. Enter a value from 0 to 72000 (20 hours). The default is 300 seconds (5 minutes). To disable the timeout, set the value to 0. The full SSL handshake occurs for each new connection between the client and the SSL module.

Command Modes ssl-proxy-list configuration mode

Related Commands **show ssl-proxy-list**

ssl-server *number* ssl-queue-delay

To set the amount of time for the CSS virtual SSL server to wait for packets before emptying the queued data for encryption, use the **ssl-server** *number* **ssl-queue-delay** command. Use the **no** form of this command to reset the delay to 200 milliseconds.

ssl-server *number* **ssl-queue-delay** *number2*

no ssl-server *number* **ssl-queue-delay**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
ssl-queue-delay *number2*	The time in milliseconds to wait for packets before emptying the queued data for encryption. Enter a value from 0 to 10000. The default delay is 200. Setting the value to 0 disables the queuing of data.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The virtual SSL server on the CSS empties the data from the queue and encrypts it for transmission to the client when:

- The queue fills to 16,400 bytes (the maximum SSL record size)
- The server sends a TCP FIN packet
- When the delay time on the CSS has passed, even though the queue has less than 16,400 bytes

When you set the value to 0 to disable the queuing of data, the virtual SSL server on the CSS encrypts the data as soon as it arrives from the server and then sends the data to the client.

ssl-server *number* tcp

To configure TCP connections with a virtual SSL server, use the **ssl-server** *number* **tcp** command. You can specify:

- A timeout value that the CSS uses to terminate a TCP connection for inactivity or an unsuccessful TCP three-way handshake with a back-end SSL server
- The Nagle algorithm for the TCP connection
- The buffer size for the TCP connection

Use the **no** form of this command to reset the buffer size to 32768, restore the timeout period to 240 seconds for inactivity or 30 seconds for the three-way handshake.

ssl-server *number* **tcp** [**buffer-share** [**rx**|**tx**] *number2*|[**server**|**virtual**] **inactivity-timeout** *seconds*|**nagle** [**enable**|**disable**]|**syn-timeout** *seconds2*]

no ssl-server *number* **tcp** [**buffer-share** [**rx**|**tx**]| [**server**|**virtual**] **inactivity-timeout** |**syn-timeout**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
buffer-share [**rx**|**tx**] *number2*	Sets the TCP buffering from the client or server on a given connection. • To set the amount of data in bytes that a given connection can buffer from the client traffic, use the **rx** *number2* keyword and variable. • To set the amount of data in bytes that a given connection can buffer from the server to the client, use the **tx** *number2* keyword and variable. By default, the buffer size is 32768. The buffer size can range from 16400 to 262144.
server	Specifies the TCP connection for the web server.

virtual	Specifies the TCP connection for the client.
inactivity-timeout *seconds*	Specifies the timeout value that the CSS waits to receive inbound flows before terminating the TCP connection. Enter a TCP inactivity timeout value in seconds, from 0 disabling the TCP inactivity timeout to 3600 (1 hour). The default is 240 seconds.
nagle enable|disable	Specifies the Nagle algorithm for the TCP connection. By default, the Nagle algorithm is enabled for each TCP connection. Use the **disable** keyword to disable the Nagle algorithm when you observe a delay on the TCP connection. Use the **enable** keyword to reenable the Nagle algorithm.
syn-timeout *seconds2*	Specifies a timeout value that the CSS uses to terminate a TCP connection with a web server or client that has not successfully completed the TCP three-way handshake prior to transferring data. Enter a TCP SYN timeout value in seconds, from 0 to 3600 (1 hour). The default is 30 seconds. To disable the TCP SYN timeout period, set the value to 0. The timer becomes inactive and the retransmit timer will eventually terminate a broken TCP connection. The connection timer should always be shorter than the retransmit termination time for new SSL/TCP connections.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The TCP Nagle algorithm automatically concatenates a number of small buffer messages transmitted over the TCP connection between a client and the SSL module or between a server and the SSL module. This process increases the throughput of your CSS by decreasing the number of packets sent over each TCP connection. However, the interaction between the Nagle algorithm and the TCP delay acknowledgment may increase latency in your TCP connection. Disable the Nagle algorithm when you observe an unacceptable delay in a TCP connection (clear-text or SSL).

Related Commands **show ssl-proxy-list**

ssl-server *number* unclean-shutdown

To instruct the CSS to send only a TCP FIN message to terminate a client connection, use the **ssl-server** *number* **unclean-shutdown** command. The CSS does not send a Close-Notify alert to close a client connection. The **no** version of this command resets the CSS default behavior of sending both a Close-Notify alert and a TCP FIN message to close the client connection.

ssl-server *number* **unclean-shutdown**

no ssl-server *number* **unclean-shutdown**

Usage Guidelines Normally, the SSL Close-Notify alert terminates a connection without an error. However, some versions of MSIE browsers do not close the connection upon receiving the Close-Notify alert. The browser may attempt to reuse the connection even though it appears to be closed to the CSS. Because the CSS cannot reply to a new request on this connection, the browser may display an error.

ssl-server *number* urlrewite

To add a URL rewrite rule to the virtual SSL server and avoid nonsecure HTTP 300-series redirects by the server, use the **ssl-server** *number* **urlrewrite** command. This command instructs the CSS, through the SSL Acceleration module, to examine every HTTP header field received from the server for a 300-series redirection response (such as 302 Found or 304 Not Modified). If the CSS finds a 300-series return code, it searches the Location response-header field in the HTTP header to determine if the field matches the hostname defined in a URL rewrite rule. If there is a match, the CSS rewrites the Location field to contain an HTTPS location and the SSL port for the response. Use the **no** form of this command to remove a URL rewrite rule.

ssl-server *number* **urlrewrite** *number hostname* [**sslport** *port* {**clearport** *port*}]

no ssl-server *number* **urlrewrite** *number*

Syntax Description

number	The number used to identify the virtual SSL server in the SSL proxy list. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
urlrewrite *number*	The number of the URL rewrite rule to be added to the virtual SSL server. Enter a value between 1 and 32 corresponding to the URL rewrite rule. You can add a maximum of 32 URL rewrite rules to each SSL server for handling HTTP to HTTPS redirects.
hostname	The domain name of the URL to be redirected (for example, www.mydomain.com). Enter an unquoted text string with a maximum length of 240 characters that corresponds to the domain name of the URL rewrite host. Do not include the directory path as part of the hostname. You can use wildcards in domain names as part of the matching criteria for a URL redirect rule. An asterisk (*) wild card character may be used in the domain name to identify more than one host in a single domain. You can specify a wildcard-only hostname (for example, *), a prefix wildcard (for example, *.mydomain.com), or a suffix wildcard (for example, www.mydomain.*). name is the * character and all HTTP redirects that come through this VIP from the server are rewritten to HTTPS. In this case, there is no need to have additional URL rewrite rules for this SSL server.
sslport *port*	(Optional) Specifies the port used for SSL network traffic. Enter a TCP port number that corresponds with an SSL content rule, which uses the specified TCP port number. The SSL module rewrites an HTTP redirect matching the URL redirect rule with the specified SSL port (or default port 443 if no port number is specified). Enter a port value from 1 to 65535. The default value is 443.
clearport *port*	(Optional) Specifies the port used for clear text network traffic. The SSL module matches redirects in the Location Response-Header field with the specified clear text port (or default port 80 if no port number is specified). Enter a port value from 1 to 65535. The default value is 80.

Command Modes ssl-proxy-list configuration mode

Usage Guidelines Use care when specifying wildcards in domain names to avoid the unwanted rewriting of all URL references by the SSL Acceleration module. Review your redirects and ensure that every URL that matches a specified wildcard rule needs to be rewritten.

Related Commands **show ssl**

ssl-server *number* version

To specify the SSL or Transport Layer Security (TLS) protocol version, use the **ssl-server** *number* **version** command. Use the **no** form of this command to reset the SSL version to the default of SSL version 3.0 and TLS version 1.0.

ssl-server *number* **version** *protocol*

no ssl-server *number* **version**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
protocol	Protocol version. Enter one of the following keywords: • **ssl-tls -** SSL protocol version 3.0 and TLS protocol version 1.0 (default) • **ssl -** SSL protocol version 3.0 • **tls** - TLS protocol version 1.0

Command Modes ssl-proxy-list configuration mode

Usage Guidelines

The CSS supports SSL version 3.0 and TLS version 1.0. The CSS understands and accepts an SSL version 2.0 ClientHello message to allow dual version clients to communicate with the CSS through the SSL module. In this case, the client indicates an SSL version of 3.0 in the version 2.0 ClientHello. This indicates to the SSL module that the client can support SSL version 3.0, and the SSL module returns a version 3.0 ServerHello message.

If the client only supports SSL version 2.0 (SSL version 2.0 compliant), the CSS will be unable to pass network traffic.

Related Commands

show ssl-proxy-list

ssl-server *number* vip address

To specify a VIP address for the virtual SSL server that corresponds to a VIP address configured in a content rule, use the **ssl-server** *number* **vip address** command. Use the **no** form of this command to remove the address from the server.

ssl-server *number* **vip address** *ip_or_host*

no ssl-server *number* **vip address**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
vip address *ip_or_host*	VIP address for the server that matches the address for an SSL content rule. The SSL module uses the address to determine which traffic it should accept. Enter a valid VIP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

When you use the mneumonic host-name format for the VIP, the CSS includes a Domain Name Service (DNS) facility that translates host names such as to IP addresses. If the host name cannot be resolved, the VIP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name Service, refer to the *Cisco Content Services Switch Administration Guide.*

If the VIP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
VIP address or port/protocol must be specified
```

When the **active** command is entered for a content rule with a configured SSL service, the CSS verifies that each VIP address configured in the content rule matches at least one VIP address configured in the SSL proxy list in each of the added services. If a match is not found, the CSS logs the following error message and does not activate the content rule.

```
VIP address must have matching ssl-proxy-list entry
```

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active
(config-owner-content) vip address

(ssl-proxy-list) suspend

To suspend an active SSL proxy list, use the **suspend** command.

suspend

Usage Guidelines

You cannot modify a server in an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

Related Commands

(ssl-proxy-list) active