

SSL-Proxy-List Configuration Mode Commands

The `ssl-proxy` list configuration mode allows you to configure an SSL proxy configuration list on an 11500 series CSS containing an SSL module. An SSL proxy configuration list is a group of related virtual SSL servers that are associated with an SSL service. The SSL modules in the CSS use these servers to properly process and terminate SSL communications between the client and the Web server.

To access `ssl-proxy-list` configuration mode, use the **`ssl-proxy-list`** command from any configuration mode except for 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 following commands.

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

<i>name</i>	The 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 an ssl-accel type service 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 up to 256 virtual SSL servers.

Each service may have only one SSL proxy list configured on it. You may only have one active SSL service per 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 Advanced 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 verification of the certificate and key pair against each other. If the verification fails, the certificate name is not accepted and the CSS logs the error message `Certificate and key pair do not match` and does not activate the SSL proxy list. 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) description

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

description "*text*"

Syntax Description

text

The 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 <i>index</i>	Deletes an ACL.
no description	Removes the description for an SSL proxy list.
no ssl-server <i>number</i>	Removes the virtual SSL server from the SSL proxy list.
no ssl-server <i>number association_type</i>	Removes the association from the virtual SSL server. The association type is dhparam , dsacert , dsakey , rsacert , or rsakey .
no ssl-server <i>number</i> cipher	Removes the cipher suite from the virtual SSL server.
no ssl-server <i>number</i> handshake data	Disables the handshake data exchange.
no ssl-server <i>number</i> handshake timeout	Disables the handshake timeout period.
no ssl-server <i>number</i> port	Resets the port number to 443.
no ssl-server <i>number</i> session-cache	Resets the SSL session reuse timeout to 300 seconds
no ssl-server <i>number</i> tcp server inactivity-timeout	Resets the TCP inactivity timer to 240 seconds between the Web server and the CSS.
no ssl-server <i>number</i> tcp server syn-timeout	Resets the TCP SYN timeout to 30 seconds between the Web server and the CSS.
no ssl-server <i>number</i> tcp virtual inactivity-timeout	Resets the TCP inactivity timer to 240 seconds between the client and the CSS.
no ssl-server <i>number</i> tcp virtual syn-timeout	Resets the TCP SYN timeout to 30 seconds between the client and the CSS.
no ssl-server <i>number</i> version	Resets the SSL version to the default of SSL version 3.0 and TLS version 1.0.
no ssl-server <i>number</i> 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 server in the list.

```
show ssl-proxy-list {ssl-server number}
```

Syntax Description

ssl-server <i>number</i>	Optionally displays information for a specified server in a list. To see a list of numbers, enter: # show ssl-proxy-list 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 “[General Commands](#)”.

The **show ssl-proxy-list** command with no 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 Advanced 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 number** 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...|cipher...|handshake...
|port...|session-cache...|tcp...|version...|vip address...}
```

```
no ssl-server number {association_type...|cipher...|handshake...
|port...|session-cache...|tcp...|version...|vip address...}
```

Syntax Description

<i>number</i>	The index number for the virtual SSL server. This variable with no 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 up to 256 virtual servers. Enter a number from 1 to 256.
<i>association_type...</i>	Creates a key pair, certificate, or key parameter association for the server. See the ssl-server number association_type command.
cipher...	Specifies the cipher suite for the server. See the ssl-server number cipher command.
handshake...	Specifies the handshake negotiation data and timeout value for the server. See the ssl-server number handshake command.
port...	Specifies a virtual TCP port for the server. See the ssl-server number port command.
session-cache...	Specifies the session cache timeout value for the server. See the ssl-server number session-cache command.
tcp...	Specifies the TCP timeout value for the server. See the ssl-server number tcp command.
version...	Specifies the SSL or Transport Layer Security (TLS) protocol version. See the ssl-server number version command.
vip address...	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.

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

<i>number</i>	The index number for the server. This variable identifies a server for configuration. To see a list of servers, use the ssl-server ? command.
<i>association_type</i>	Identifies the association type. Enter one of the following: <ul style="list-style-type: none"> • 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.
<i>name</i>	The name of the association. To see a list of existing associations, use the ssl-server <i>number association_type</i> ? 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* 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	<i>number</i>	The index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: (ssl-proxy-list)# ssl-server ?
	<i>name</i>	The name of a specific cipher suite. See “Usage Guidelines” for detailed information.
	<i>ip_or_host</i>	The IP address to assign to the backend 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).

<i>port</i>	The TCP port of the backend content rule/server through which the backend 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 2-1 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.

**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 2-1 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
dhe-dss-export1024-with-rc4-56-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman and DSA key exchange
rsa-export1024-with-rc4-56-sha	Yes	RSA certificate	RSA key exchange

Table 2-1 SSL Cipher Suites Supported by the CSS (continued)

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

Table 2-1 SSL Cipher Suites Supported by the CSS (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
dhe-dss-with-3des-ede-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman and DSA key exchange
dhe-dss-with-des-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman and DSA key exchange
rsa-with-3des-ede-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-des-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-sha	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-md5	No	RSA certificate	RSA key exchange

Related Commands `show ssl-proxy-list`

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 datatimeout
```

SSL-Proxy-List Configuration Mode Commands

Syntax Description	<i>number</i>	<p>The index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter:</p> <pre>(ssl-proxy-list)# ssl-server ?</pre>
data	<i>kbytes</i>	<p>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.</p> <p>The <i>kbytes</i> 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.</p>
timeout	<i>seconds</i>	<p>Sets a maximum timeout value, after which the CSS transmits the SSL handshake message and reestablishes the SSL session.</p> <p>The <i>seconds</i> 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.</p>
Command Modes	ssl-proxy-list configuration mode	
Related Commands	show ssl-proxy-list	

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	<i>number</i>
	The index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: (ssl-proxy-list)# ssl-server ?
Syntax Description	port <i>number2</i>
	The 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 re-use 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	<i>number</i>	The 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 ?
	<i>seconds</i>	The 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* tcp

To specify a timeout value that the CSS uses to terminate a TCP connection for inactivity or an unsuccessful TCP three-way handshake with a client or Web server, use the **ssl-server *number* tcp** command. Use the **no** form of this command to restore the timeout period to 240 seconds for inactivity or 30 seconds for the three-way handshake.

**ssl-server *number* tcp [server|virtual] inactivity-timeout
seconds|syn-timeout seconds2**

**no ssl-server *number* tcp [server|virtual] inactivity-timeout
|syn-timeout**

Syntax Description	<i>number</i>	The 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 ?
	server	Specifies the timeout for the Web server.

virtual	Specifies the timeout for the client.
inactivity-timeout <i>seconds</i>	<p>Specifies the timeout value that the CSS waits to receive inbound flows before terminating the TCP connection.</p> <p>Enter a TCP inactivity timeout value in seconds, from 0 disabling the TCP inactivity timeout to 3600 (1 hour). The default is 240 seconds.</p>
syn-timeout <i>seconds2</i>	<p>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.</p> <p>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.</p> <p>The connection timer should always be shorter than the retransmit termination time for new SSL/TCP connections.</p>

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list

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 *protocol*

Syntax Description	<i>number</i>	The 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 ?
	<i>protocol</i>	The protocol version. Enter one of the following: <ul style="list-style-type: none"> • 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 11500 series 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

<i>number</i>	The 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 <i>ip_or_host</i>	The 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 mnemonic 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*.

**Note**

If the VIP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the error message `VIP address or port/protocol must be specified` and does not activate the SSL proxy list.

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 error message `VIP address must have matching ssl-proxy-list entry` and does not activate the content rule.

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