SSL Accelerated Service Configuration Mode Commands

SSL accelerated services lets you enable and configure SSL acceleration on your WAAS system, and define services to be accelerated on the SSL path. To configure secure socket layer (SSL) encryption accelerated services on a WAAS device, use the **crypto ssl services accelerated-service** global configuration command. To delete a parameter use the **no** form of the command.

> **crypto ssl service accelerated-service** *<service-name>* match sni

> **no crypto ssl service accelerated-service** *<service-name>* match sni

Syntax Description	*service-name*	Name of the accelerated service that you want to create or edit. The service list name may contain up to 128 characters.
	match sni	Matches SSL Server Name Indication(SNI) with Subject Alternate Names(SAN) in the configured SSL certificate.

Defaults   No default behavior or values.

Command Modes   global configuration

Device Modes   application-accelerator

central-manager

Usage Guidelines   Use the **crypto ssl services accelerated-service** command to add and configure an accelerated service. The **crypto ssl services accelerated-service** command initiates accelerated service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-accelerated)#
```

Within SSL accelerated service configuration mode, you can use SSL accelerated service configuration commands. To return to global configuration mode, enter **exit** at the accelerated service configuration mode prompt.

Examples   The following example shows how to create or edit an accelerated service called myservice. If the service is already established on the WAAS device, the **crypto ssl services accelerated-service** command edits it. If the service does not exist, the **crypto ssl services accelerated-service** command creates it:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# exit
WAE(config)#
```

Related Commands   **(config-ssl-accelerated) cipher-list**

(config-ssl-accelerated) client-cert-key

(config-ssl-accelerated) client-cert-verify

(config-ssl-accelerated) client-version-rollback-check

(config-ssl-accelerated) description

(config-ssl-accelerated) inservice

(config-ssl-accelerated) server-cert-key

(config-ssl-accelerated) server-cert-verify

(config-ssl-accelerated) server-domain

(config-ssl-accelerated) server-ip

(config-ssl-accelerated) server-name

(config-ssl-accelerated) version

(config-ssl-accelerated) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description	*cipher-list-name*	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Usage Guidelines A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# cipher-list myciphers
```

Related Commands **(config) crypto ssl**

(config-ssl-accelerated) client-cert-key

To configure a certificate and private key, use the **client-cert-key** command.

client-cert-key *filename*

Syntax Description

filename	Filename of the certificate and key. Must be in PKCS#12 and have a ".p12" extension.

Defaults　　　No default behavior or values.

Command Modes　　　SSL accelerated service configuration

Device Modes　　　application-accelerator

central-manager

Examples　　　The following example shows how to enter SSL accelerated service configuration mode, and then import a certificate and key:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-cert-key cert.p12
```

Related Commands　　　**(config) crypto ssl**

(config-ssl-accelerated) client-cert-verify

To enable verification of client certificates, use the **client-cert-verify** command.

client-cert-verify [**revocation-check none**]

Syntax Description	**revocation-check none**	(Optional) Specifies a revocation check null method that returns revocation success.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

                      central-manager

Usage Guidelines If the server and client devices are using self-signed certificates and certificate verification is enabled, WAAS devices will not be able to accelerate SSL traffic.

                      To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-cert-verify revocation-check none
```

Related Commands **(config) crypto ssl**

(config-ssl-accelerated) client-version-rollback-check

To disable the client SSL version rollback check, use the **client-version-rollback-check** command.

client-version-rollback-check disable

Syntax Description	**disable** Disables the client SSL version rollback check.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Usage Guidelines   If a non-RFC 2246 compliant client passes the incorrect client version in the SSL message, a bad record MAC SSL handshake failure may occur. The SSL accelerator terminates such connections. In this case, you can disable the client version rollback check which allows these connections to be optimized.

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then disable the client SSL version rollback check:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-version-rollback-check disable
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) description

To add a description of the SSL accelerated service, use the **description** command.

description *description*

Syntax Description	*description*	String that is the description of the SSL accelerated service.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then a description of the accelerated service:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# description SSL accelerated service
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) inservice

To enable the accelerated service, use the **inservice** command.

inservice

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then enable the accelerated service:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# inservice
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) protocol-chaining enable

To enable the accelerated service, use the **protocol-chaining enable** command. To disable this accelerated service, use the **no** form of this command.

protocol-chaining enable

Syntax Description   This command has no arguments or keywords.

Defaults   By default, protocol chaining is enabled.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then enable the protocol chaining:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# protocol-chaining enable
```

(config-ssl-accelerated) server-cert-key

To configure a certificate and private key, use the **server-cert-key** command.

server-cert-key *filename*

Syntax Description

filename	Filename of the certificate and key. Must be in PKCS#12 and have a ".p12" extension.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then import a certificate and key:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-cert-key cert.p12
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) server-cert-verify

To enable verification of server certificates, use the **server-cert-verify** command.

server-cert-verify [**revocation-check none**]

Syntax Description	**revocation-check none**	(Optional) Specifies a revocation check null method that returns revocation success.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Usage Guidelines If the server and client devices are using self-signed certificates and certificate verification is enabled, WAAS devices will not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-cert-verify revocation-check none
```

Related Commands **(config) crypto ssl**

(config-ssl-accelerated) server-domain

To configure the accelerated server domain and TCP port, use the **server-domain** command.

server-domain *srv-domain* {**port** *port-no*}

Syntax Description

server-domain *srv-domain*	Specifies the domain name of the accelerated server starting with the characters "*.". 255 alphanumeric characters maximum, 63 characters per label/segment.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server domain name and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-domain 2.2.2.2 port 1
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) server-ip

To configure the accelerated server IP address and TCP port, use the **server-ip** command.

server-ip *ip-address* {**port** *port-no*}

Syntax Description

server-ip *ip-address*	Specifies the IP address of the accelerated server.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults   No default behavior or values.

Command Modes   SSL accelerated service configuration

Device Modes   application-accelerator

central-manager

Examples   The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server IP address and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-ip 2.2.2.2 port 1
```

Related Commands   **(config) crypto ssl**

(config-ssl-accelerated) server-name

To configure the accelerated server hostname and TCP port, use the **server-name** command.

server-name *hostname* {**port** *port-no*}

Syntax Description

server-name *hostname*	Specifies the hostname of the accelerated server. 255 alphanumeric characters max, 63 characters per label/segment.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults No default behavior or values.

Command Modes SSL accelerated service configuration

Device Modes application-accelerator

central-manager

Examples The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server name and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-name acc_server port 1
```

Related Commands **(config) crypto ssl**

(config-ssl-accelerated) version

To specify the type of SSL protocol to use for accelerated services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version {**all**	**ssl3**	**tls1**}	Specifies SSL3 for the SSL version 3 protocol, TLS1 for the Transport Layer Security version 1 protocol, or All to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# version SSL3
```

Related Commands   **(config) crypto ssl**

■ **(config-ssl-accelerated) version**