

SSL Management Service Configuration Mode Commands

SSL management services lets you configure SSL parameters used for secure communications between the Central Manager and the WAE devices. To configure secure socket layer (SSL) encryption management service parameters on a WAAS device, use the **crypto ssl management-service** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl management-service

no crypto ssl management-service

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes global configuration

Device Modes application-accelerator
central-manager

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

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

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

Examples The following example shows how to enter SSL management service configuration mode:

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)# exit
WAE(config)#
```

Related Commands [\(config-ssl-mgmt\) cipher-list](#)
[\(config-ssl-mgmt\) peer-cert-verify](#)

(config-ssl-mgmt) version

(config-ssl-mgmt) 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	<i>cipher-list-name</i>	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 management 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 management 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: <pre>WAE(config)# crypto ssl services management-service WAE(config-ssl-mgmt)# cipher-list myciphers</pre>	
Related Commands	(config) crypto ssl	

(config-ssl-mgmt) peer-cert-verify

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

peer-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 management service configuration
----------------------	--------------------------------------

Device Modes	application-accelerator central-manager
---------------------	--

Usage Guidelines	<p>SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections.</p> <p>If peer certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and not be able to accelerate SSL traffic.</p> <p>To disable OCSP certificate revocation checking, set the revocation check value to none.</p>
-------------------------	--

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

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)# peer-cert-verify revocation-check none
```

Related Commands	(config) crypto ssl
-------------------------	-------------------------------------

(config-ssl-mgmt) version

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

```
version {all | ssl3 | tls1}
```

Syntax Description		
	version tls1	Specifies TLS1 for the SSL version 3 protocol.
	version ssl3	Specifies SSL3 for the Transport Layer Security version 1 protocol.
	version all	Specifies ALL to use both SSL3 and TLS1 SSL protocols.

Defaults No default behavior or values.

Command Modes SSL management service configuration

Device Modes application-accelerator
central-manager

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

```
WAE(config)# crypto ssl management-service  
WAE(config-ssl-mgmt)# version SSL3
```

Related Commands [\(config\) crypto ssl](#)

■ (config-ssl-mgmt) version