SSL Cipher List Configuration Mode Commands

A cipher list is customer list of cipher suites that you assign to an SSL connection. To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **crypto ssl cipher-list** global configuration command. To delete a cipher list use the **no** form of the command.

crypto ssl cipher-list *cipher-list-name*

no crypto ssl 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

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **crypto ssl cipher-list** command to add and configure a cipher list. The **crypto ssl cipher-list** command initiates cipher list configuration mode, as indicated by the following prompt:

```
WAE(config-cipher-list)#
```

Within cipher list configuration mode, you can use the **cipher** cipher list configuration command to define list of cipher suites. To return to global configuration mode, enter **exit** at the cipher list configuration mode prompt.

Examples

The following example shows how to create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **crypto ssl cipher-list** command edits it. If the cipher list does not exist, the **crypto ssl cipher-list** command creates it:

```
WAE(config)# crypto ssl cipher-list myciphers
WAE(config-ca)# cipher rsa-with-rc4-128-sha
WAE(config-ca)# exit
WAE(config)#
```

Related Commands

(config-cipher-list) cipher

(config-cipher-list) cipher

To add a cipher suite to a cipher list, or to change the priority of a cipher suite on the list, use the **cipher** command.

cipher *cipher-suite-name* [**priority** *value*]

Syntax Description

cipher-suite-name	Name of the cipher suite you want to add or reprioritize. Type any of the following strings: **dhe-rsa-with-3des-ede-cbc-sha** **dhe-rsa-with-aes-128-cbc-sha** **dhe-rsa-with-aes-256-cbc-sha** **dhe-rsa-with-des-cbc-sha** **rsa-with-3des-ede-cbc-sha** **rsa-with-aes-128-cbc-sha** **rsa-with-aes-256-cbc-sha** **rsa-with-des-cbc-sha** **rsa-with-rc4-128-md5** **rsa-with-rc4-128-sha** If you are establishing an SSL connection to a Microsoft IIS server, do not select a DHE-based cipher suite.
priority *value*	(Optional specifies)The priority of the cipher suite in relation to other suites in the list. The priority value is from 1 to 15 (15 is the highest).

Defaults

No default behavior or values.

Command Modes

cipher list configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The SSL protocol supports a variety of different cryptographic algorithms, or ciphers, for use in operations such as authenticating the server and client to each other, transmitting certificates, and establishing session keys. Clients and servers may support different cipher suites, or sets of ciphers, depending on various factors such as the version of SSL they support, company policies regarding acceptable encryption strength, and government restrictions on export of SSL-enabled software. Among its other functions, the SSL handshake protocol determines how the server and client negotiate which cipher suites they will use to authenticate each other to transmit certificates and to establish session keys.

Note Note *Exportable* cipher suites are those cipher suites that are considered not to be as strong as some of the other cipher suites (for example, 3DES or RC4 with 128-bit encryption) as defined by U.S. export restrictions on software products. Exportable cipher suites may be exported to most countries from the United States, and provide the strongest encryption available for exportable products.

Each cipher suite specifies a set of key exchange algorithms. For example, Figure 3-1 summarizes the algorithms associated with the rsa-export-with-rc4-40-md5 cipher suite.

Figure 3-1 Cipher Suite Algorithms

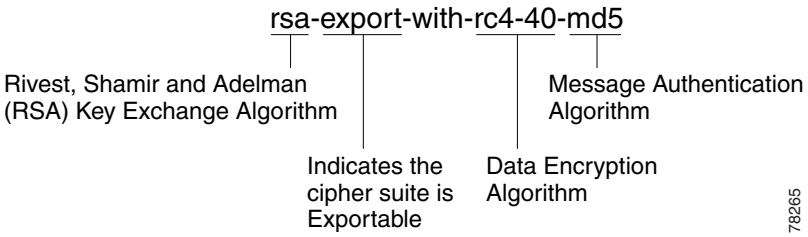

Table 3-1 lists the supported cipher suites and indicates whether those cipher suites are exportable, the authentication certificate, and the encryption key required by the cipher suite.

Table 3-1 SSL Cipher Suites

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
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-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

Note The client-specified order for ciphers overrides the cipher list priority assigned here if the cipher list is applied to an accelerated service. The priorities assigned in this cipher list are only applicable if the cipher list is applied to SSL peering and management services.

Examples

The following example shows how to enter cipher list configuration mode for the cipher list named myciphers, and then add the cipher suite rsa-with-3des-ede-cbc-sha with a priority of 1:

```
WAE(config)# crypto ssl cipher-list myciphers
```

```
WAE(config-cipher-list)# cipher rsa-with-3des-ede-cbc-sha priority 1
```

Related Commands

(config) crypto ssl