Cipher Suite Configuration Mode Commands

Command Modes

The Cipher Suite Configuration Mode is used to configure the building blocks for SSL cipher suites, including the encryption algorithm, hash function, and key exchange.

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

encryption

Specifies the encryption algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
encryption { 3des | aes-128 | null | rc4 }
default encryption
```

default

Sets the encryption option to its default value of RC4.

encryption 3des | aes-128 | null | rc4

Specifies the encryption algorithm.

3des: Encryption algorithm 3DES (Triple Encryption Algorithm). 3DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

aes-128: Encryption algorithm AES-128 (Advanced Encryption Standard-128). AES-128 is a symmetric-key encryption standard which has a 128-bit block size, with key size of 128.

null: Encryption algorithm Null.

rc4: Encryption algorithm RC4 (Rivest Cipher 4). RC4 is a stream cipher used with SSL protocol.

Usage Guidelines Use this command to specify encryption for the SSL cipher suite.

Example

The following command sets the encryption option to its default value, which is RC4:

```
encryption rc4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines Use this command to return to the parent configuration mode.

hmac

Specifies the HMAC (keyed-Hash Message Authentication Code) for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
hmac { sha1 }
default hmac
```

default

Sets the HMAC option to its default value of SHA-1.

hmac sha1

Specifies the SHA-1 (Secure Hash Algorithm-1) HMAC for the SSL cipher suite.SHA-1 uses a 160-bit secret key and produces a 160-bit digest.

Usage Guidelines

Use this command to specify the SHA-1 HMAC for the SSL cipher suite. The default and only currently available option is SHA-1.

A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity.

Example

The following command sets the HMAC option to its default value, which is SHA-1:

```
hmac sha1
```

key-exchange

Specifies the key exchange algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > **context** *context_name* > **cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
key-exchange { rsa }
default key-exchange
```

default

Sets the key exchange option to its default value of RSA.

key-exchange rsa

Specifies the RSA (Rivest, Shamir, and Adleman) key exchange algorithm for the SSL cipher suite. With RSA, the secret key is encrypted with the receiver's public key, and a public-key certificate from the receiver's key must be made available.

Usage Guidelines

Use this command to specify the RSA key exchange for the SSL cipher suite. The default and only currently available option is RSA.

The key exchange algorithm provides the means by which the cryptographic keys for conventional encryption and MAC calculations are exchanged.

Example

The following command sets the key exchange option to its default value, which is RSA:

```
key-exchange rsa
```