CHAPTER 12

crypto isakmp disconnect-notify through cxsc auth-proxy port Commands

crypto isakmp disconnect-notify

To enable disconnect notification to peers, use the **crypto isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	The **isakmp disconnect-notify** command was introduced.
7.2.(1)	The **crypto isakmp disconnect-notify** command replaced the **isakmp disconnect-notify** command**.**
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can enable disconnect notifications to peers with the use of the following delete reasons:

- IKE_DELETE_RESERVED = 0
  An invalid code. Do not send.
- IKE_DELETE_BY_ERROR = 1
  A transmission error for a timeout or failure when expecting a response to a keepalive or any other IKE packet ACK. The default text is “Connectivity to client lost.”
- IKE_DELETE_BY_USER_COMMAND = 2
  The SA was actively deleted with manual intervention by the user or administrator. The default text is “Manually Disconnected by Administrator.”
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3
  The SA has expired. The default text is “Maximum Configured Lifetime Exceeded.”
- IKE_DELETE_NO_ERROR = 4
  An unknown error caused the delete.
- IKE_DELETE_SERVER_SHUTDOWN = 5
  The server is being shut down.

- IKE_DELETE_SERVER_IN_FLAMES = 6
  The server has some severe problems. The default text is “Peer is having heat problems.”
- IKE_DELETE_MAX_CONNECT_TIME = 7
  The maximum allowed time of an active tunnel has expired. Unlike EXPIRED_LIFETIME, this reason indicates that the entire IKE-negotiated/controlled tunnel is being disconnected, not just this one SA. The default text is “Maximum Configured Connection Time Exceeded.”
- IKE_DELETE_IDLE_TIMEOUT = 8
  The tunnel has been idle for the maximum allowed time; therefore, the entire IKE-negotiated tunnel has been disconnected, not just this one SA. The default text is “Maximum Idle Time for Session Exceeded.”
- IKE_DELETE_SERVER_REBOOT = 9
  The server is rebooting.
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10
  Phase2 proposal mismatch.
- IKE_DELETE_FIREWALL_MISMATCH = 11
  Firewall parameter mismatch.
- IKE_DELETE_CERT_EXPIRED = 12
  User certification required. The default message is “User or Root Certificate has Expired.”
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13
  Client type or version not allowed.
- IKE_DELETE_FW_SERVER_FAIL = 14
  Failed to contact Zone Integrity Server.
- IKE_DELETE_ACL_ERROR = 15
  ACL downloaded from AAA cannot be inserted. The default message is “ACL parsing error.”

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# crypto isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp identity

To set the Phase 1 ID to be sent to the peer, use the **crypto isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISAKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Defaults

The default ISAKMP identity is **crypto isakmp identity auto**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	The **isakmp identity** command was introduced.
7.2(1)	The **crypto isakmp identity** command replaced the **isakmp identity** command.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPsec peer, depending on connection type:

```
hostname(config)# crypto isakmp identity auto
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you enable it with the **crypto isakmp enable** command) in global configuration mode. To disable the NAT traversal, use the **no** form of this command.

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Defaults

By default, NAT traversal is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	The **isakmp nat-traversal** command was introduced.
7.2.(1)	The **crypto isakmp nat-traversal** command replaced the **isakmp nat-traversal** command**.**
8.0(2)	NAT traversal is enabled by default.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

NAT including PAT is used in many networks where IPsec is also used, but there are a number of incompatibilities that prevent IPsec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The ASA supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html, and supports NAT traversal for both dynamic and static crypto maps.

This command enables NAT-T globally on the ASA. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then sets NAT traversal with a keepalive interval of 30 seconds:

```
hostname(config)# crypto isakmp enable
```

```
hostname(config)# crypto isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. To remove the ISAKMP authentication method, use the related **clear configure** command.

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

Syntax Description

crack	Specifies IKE CRACK as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This basically means you can prove to a third party whether you had an IKE negotiation with the peer.

Defaults

The default ISAKMP policy authentication is **pre-share**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy authentication** command was introduced.
7.2.(1)	The **crypto isakmp policy authentication** command replaced the **isakmp policy authentication** command**.**

Usage Guidelines

IKE policies define a set of parameters for IKE negotiation.

If you specify RSA signatures, you must configure the ASA and its peer to obtain certificates from a CA server. If you specify preshared keys, you must configure these preshared keys separately within the ASA and its peer.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy authentication** command. This example sets the authentication method of RSA signatures to be used for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **crypto isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is **des,** use the **no** form of this command.

crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

no crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

Syntax Description

3des	Specifies that the triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default ISAKMP policy encryption is **3des**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy encryption** command was introduced.
7.2.(1)	The **crypto isakmp policy encryption** command replaced the **isakmp policy encryption** command**.**

Examples

The following example, entered in global configuration mode, shows use of the **crypto isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
hostname(config)# crypto isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 encryption 3des
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **crypto isakmp policy group** command in global configuration mode.To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the IIKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default group policy is group 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy group** command was introduced.
7.2.(1)	The **crypto isakmp policy group** command replaced the **isakmp policy group** command**.**
8.0(4)	The **group 7** command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

IKE policies define a set of parameters to use during IKE negotiation.

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires ISAKMP policy to use DH group 2. (If you configure DH group 1, the Cisco VPN Client cannot connect.)

AES support is available on ASAs licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) group 5 instead of group 1 or group 2. To configures group 5, use the **crypto isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy group** command. This example sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 group 2
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

crypto isakmp policy *priority* hash {**md5** | **sha**}

no crypto isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm for the IKE policy.
priority	Uniquely identifies and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm for the IKE policy.

Defaults

The default hash algorithm is SHA-1 (HMAC variant).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy hash** command was introduced.
7.2.(1)	The **crypto isakmp policy hash** command replaced the **isakmp policy hash** command**.**

Usage Guidelines

IKE policies define a set of parameters to be used during IKE negotiation.

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy hash** command. This example specifies the MD5 hash algorithm for the IKE policy, with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 hash md5
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime.

Defaults

The default value is 86,400 seconds (one day).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy lifetime** command was introduced.
7.2.(1)	The **crypto isakmp policy lifetime** command replaced the **isakmp policy lifetime** command**.**

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. You can specify an infinite lifetime if the peer does not propose a lifetime. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPsec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) for the IKE policy with the priority number of 40:

```
hostname(config)# crypto isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime:

```
hostname(config)# crypto isakmp policy 40 lifetime 0
```

Related Commands

clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the ASA, use the **crypto isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the ASA, use the **no** form of this command.

crypto isakmp reload-wait

no crypto isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	The **isakmp reload-wait** command was introduced.
7.2.(1)	The **crypto isakmp reload-wait** command replaced the **isakmp reload-wait** command**.**
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, tells the ASA to wait until all active sessions have terminated before rebooting:

```
hostname(config)# crypto isakmp reload-wait
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto key generate rsa

To generate RSA key pairs for identity certificates, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**] **dsa** [**label name | elliptic-curve** [**256 | 384 | 521**]

Syntax Description

dsa [**label name**]	Uses the Suite B EDCSA algorithms when generating a keypair.
elliptic-curve [**256	384	521**]	Uses the Suite B EDCSA algorithms when generating a keypair.
general-keys	Generates a single pair of general purpose keys. This is the default key-pair type.
label *key-pair-label*	Specifies the name to be associated with the key pair(s). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the ASA displays a warning message. If no label is provided when the key is generated, the key pair is statically named Default-RSA-Key.
modulus *size*	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.
usage-keys	Generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.

Defaults

The default key-pair type is **general key**. The default modulus size is 1024.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **crypto key generate rsa** command to generate RSA key pairs to support SSL, SSH, and IPsec connections. The generated key pairs are identified by labels that you can provide as part of the command syntax. Trustpoints that do not reference a key pair can use the default one, Default-RSA-Key. SSH connections always use this key. This does not affect SSL, because SSL generates its own certificate or key dynamically, unless a trustpoint has one configured.

Note The amount of NVRAM space for storing key pairs varies depending on the ASA platform. You may reach a limit if you generate more than 30 key pairs.

Note The 4096-bit RSA keys are only supported on the ASA5580, 5585, or later platforms.

Caution Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the ASA and rejected clientless logins.

Examples

The following example, entered in global configuration mode, generates an RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

The following example, entered in global configuration mode, inadvertently attempts to generate a duplicate RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

The following example, entered in global configuration mode, generates an RSA key pair with the default label:

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

The following example, entered in global configuration mode, generates a warning message because there is not enough space to save the RSA keypair:

```
hostname(config)# crypto key generate rsa label mypubkey mod 2048
INFO: The name for the keys will be: mypubkey
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair mypubkey. Remove any unnecessary
keypairs and save the running config before using this keypair.
hostname(config)#
```

Related Commands

Command	Description
crypto key zeroize	Removes RSA key pairs.
show crypto key	Displays the RSA key pairs.

crypto key zeroize

To remove the key pairs of the indicated type (rsa or dsa), use the **crypto key zeroize** command in global configuration mode.

crypto key zeroize {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

Syntax Description

default	Removes RSA key pairs with no labels. This keyword is legal only with RSA key pairs.
dsa	Specifies DSA as the key type.
label *key-pair-label*	Removes the key pairs of the indicated type (**rsa** or **dsa**). If you do not provide a label, the ASA removes all key pairs of the indicated type.
noconfirm	Suppresses all interactive prompting.
rsa	Specifies RSA as the key type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, removes all RSA key pairs:

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

Related Commands

Command	Description
crypto key generate dsa	Generates DSA key pairs for identity certificates.
crypto key generate rsa	Generates RSA key pairs for identity certificates.

crypto large-cert-acceleration enable

To enable the ASA to perform 2048-bit RSA key operations in hardware, use the **crypto large-cert-acceleration enable** command in global configuration mode. To perform 2048-bit RSA key operations in software, use the **no crypto large-cert-acceleration enable** command.

crypto large-cert-acceleration enable

no crypto large-cert-acceleration enable

Syntax Description

This command has no keywords or arguments.

Defaults

By default, 2048-bit RSA key operations are performed in software.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.2(3)	This command was introduced.

Usage Guidelines

This command is only available on the ASA 5510, ASA 5520, ASA 5540, and 5550. The command is not available on the ASA 5580.

Examples

The following example shows that 2048-bit RSA key operations have been enabled in hardware:

```
hostname (config)# show running-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
hostname (config)#
```

Related Commands

Command	Description
clear configure crypto	Clears the 2048-bit RSA key configuration with the rest of the crypto configuration.
show running-config crypto	Shows the 2048-bit RSA key configuration with the rest of the crypto configuration.

crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command in global configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

Syntax Description

interface-name	Specifies the interface for the ASA to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a CA to obtain certificates, this should be the interface with the address specified in the CA certificates.
map-name	Specifies the name of the crypto map set.
ipv6-local-address *ipv6-address*	Specifies an IPv6 address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.3(1)	The **ipv6-local-address** keyword was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use this command to assign a crypto map set to any active ASA interface. The ASA supports IPsec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPsec services.

You can assign only one crypto map set to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are part of the same set and are all applied to the interface. The ASA evaluates the crypto map entry with the lowest sequence number first.

Use the **ipv6-local-address** keyword when you have multiple IPv6 addresses configured on an interface and are configuring the ASA to support LAN-to-LAN VPN tunnels in an IPv6 environment.

Note The ASA lets you change crypto map, dynamic map, and IPsec settings on the fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the accesslist, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

Every static crypto map must define three parts: an access list, a transform set, and an IPsec peer. If one of these is missing, the crypto map is incomplete and the ASA moves on to the next entry. However, if the crypto map matches the access list but not either or both of the other two requirements, this ASA drops the traffic.

Use the **show running-config crypto map** command to ensure that every crypto map is complete. To fix an incomplete crypto map, remove the crypto map, add the missing entries, and reapply it.

Examples

The following example, entered in global configuration mode, assigns the crypto map set named mymap to the outside interface. When traffic passes through the outside interface, the ASA evaluates it using all the crypto map entries in the mymap set. When outbound traffic matches an access list in one of the mymap crypto map entries, the ASA forms a security association using that crypto map entry's configuration.

```
hostname(config)# crypto map mymap interface outside
```

The following example shows the minimum required crypto map configuration:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map ipsec-isakmp dynamic

To require a given crypto map entry to refer to a preexisting dynamic crypto map, use the **crypto map ipsec-isakmp dynamic** command in global configuration mode. To remove the cross-reference, use the **no** form of this command.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Syntax Description

dynamic-map-name	Specifies the name of the crypto map entry that refers to a preexisting dynamic crypto map.
ipsec-isakmp	Indicates that IKE establishes the IPsec security associations for this crypto map entry.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to remove the **ipsec-manual** keyword.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the dynamic crypto map set to interfaces.

Dynamic crypto maps provide two functions: filtering/classifying traffic to protect, and defining the policy to apply to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPsec dynamic crypto maps identify the following:

- The traffic to protect
- IPsec peer(s) with which to establish a security association

- Transform sets to use with the protected traffic
- How to use or manage keys and security associations

A crypto map set is a collection of crypto map entries, each with a different sequence number (*seq-num*) but the same map name. Therefore, for a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPsec security applied. To accomplish this, you create two crypto map entries, each with the same map name, but each with a different sequence number.

The number you assign as the *seq-num* argument should not be arbitrary. This number ranks multiple crypto map entries within a crypto map set. A crypto map entry with a lower sequence number is evaluated before a map entry with a higher sequence number; that is, the map entry with the lower number has a higher priority.

Note When you link the crypto map to a dynamic crypto map, you must specify the dynamic crypto map. This links the crypto map to an existing dynamic crypto map that was previously defined using the **crypto dynamic-map** command. Now any changes you make to the crypto map entry after it has been converted will not take affect. For example, a change to the set peer setting does not take effect. However, the ASA stores the change while it is up. When the dynamic crypto map is converted back to the crypto map, the change is effective and appears in the output of the **show running-config crypto map** command. The ASA maintains these settings until it reboots.

Examples

The following command, entered in global configuration mode, configures the crypto map mymap to refer to a dynamic crypto map named test:

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map match address

To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode. To remove the access list from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

Syntax Description

acl_name	Specifies the name of the encryption access list. This name should match the name argument of the named encryption access list being matched.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list** command to define the access lists. The access list hit counts only increase when the tunnel initiates. After the tunnel is up, the hit counts do not increase on a per-packet flow. If the tunnel drops and then reinitiates, the hit count will be increased.

The ASA uses the access lists to differentiate the traffic to protect with IPsec crypto from the traffic that does not need protection. It protects outbound packets that match a permit ACE, and ensures that inbound packets that match a permit ACE have protection.

When the ASA matches a packet to a deny statement, it skips the evaluation of the packet using the remaining ACEs in the crypto map, and resumes evaluation of the packet using the ACEs in the next crypto map in sequence. *Cascading ACLs* involves the use of deny ACEs to bypass evaluation of the remaining ACEs in an ACL, and the resumption of evaluation of traffic using the ACL assigned to the next crypto map in the crypto map set. Because you can associate each crypto map with different IPsec

settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security.

Note The crypto access list does not determine whether to permit or deny traffic through the interface. An access list applied directly to the interface with the **access-group** command makes that determination.

In transparent mode, the destination address should be the IP address of the ASA, the management address. Only tunnels to the ASA are allowed in transparent mode.

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set connection-type

To specify the connection type for the backup Site-to-Site feature for this crypto map entry, use the **crypto map set connection-type** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

no crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

Syntax Description

answer-only	Specifies that this peer only responds to inbound IKE connections first during the initial proprietary exchange to determine the appropriate peer to connect to.
bidirectional	Specifies that this peer can accept and originate connections based on this crypto map entry. This is the default connection type for all Site-to-Site connections.
map-name	Specifies the name of the crypto map set.
originate-only	Specifies that this peer initiates the first proprietary exchange to determine the appropriate peer to connect to.
seq-num	Specifies the number you assign to the crypto map entry.
set connection-type	Specifies the connection type for the backup Site-to-Site feature for this crypto map entry. There are three types of connections: answer-only, originate-only, and bidirectional.

Defaults

The default setting is bidirectional.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0	This command was introduced.
9.0	Support for multiple context mode was added.

Usage Guidelines

The **crypto map set connection-type** command specifies the connection types for the backup LAN-to-LAN feature. It allows multiple backup peers to be specified at one end of the connection.

This feature works only between the following platforms:

- Two Cisco ASA 5500 series
- A Cisco ASA 5500 series and a Cisco VPN 3000 concentrator
- A Cisco ASA 5500 series and a security appliance running Cisco PIX security appliance software Version 7.0, or higher

To configure a backup LAN-to-LAN connection, we recommend that you configure one end of the connection as originate-only using the **originate-only** keyword, and the end with multiple backup peers as answer-only using the **answer-only** keyword. On the originate-only end, use the **crypto map set peer** command to order the priority of the peers. The originate-only ASA attempts to negotiate with the first peer in the list. If that peer does not respond, the ASA works its way down the list until either a peer responds or there are no more peers in the list.

When configured in this way, the originate-only peer initially attempts to establish a proprietary tunnel and negotiate with a peer. Thereafter, either peer can establish a normal LAN-to-LAN connection and data from either end can initiate the tunnel connection.

In transparent firewall mode, you can see this command but the connection-type value cannot be set to anything other than answer-only for crypto map entries that are part of a crypto map that has been attached to the interface.

Table 12-1 lists all supported configurations. Other combinations may result in unpredictable routing issues.

Table 12-1 Supported Backup LAN-to-LAN Connection Types

Remote Side	Central Side
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the connection-type to originate-only.

```
hostname(config)# crypto map mymap 10 set connection-type originate-only
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set df-bit

To set the per-signature algorithm (SA) do-not-fragment (DF) policy, use the **crypto map set df-bit** command in global configuration mode. To disable the DF policy, use the **no** form of this command.

crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Defaults

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The original DF policy command is retained and acts as a global policy setting on an interface, but it is superseded for an SA by the **crypto map** command.

crypto map set ikev2 pre-shared-key

To specify a preshared key for AnyConnect IKEv2 connections, the **crypto map set ikev2 pre-shared-key** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

Syntax Description

key	Alphanumeric string from 1 to 128 characters.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
8.4(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Examples

The following example configures the preshared key SKTIWHT:

```
hostname(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set inheritance

To set the granularity (single or multiple) of security associations generated for this crypto map entry, use the **set inheritance** command in global configuration mode. To remove the inheritance setting for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

no crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

Syntax Description

data	Specifies one tunnel for every address pair within the address ranges specified in the rule.
map-name	Specifies the name of the crypto map set.
rule	Specifies one tunnel for each ACL entry associated with this crypto map. This is the default.
seq-num	Specifies the number that you assign to the crypto map entry.
set inheritance	Specifies the type of inheritance: **data or rule**. Inheritance allows a single security association (SA) to be generated for each security policy database (SPD) rule or multiple security SAs for each address pair in the range.

Defaults

The default value is **rule**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command works only when the ASA is initiating the tunnel, not when responding to a tunnel. Using the data setting may create a large number of IPsec SAs. This consumes memory and results in fewer overall tunnels. You should use the data setting only for extremely security-sensitive applications.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the inheritance type to data:

```
hostname(config)# crypto map mymap 10 set inheritance data
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default setting for this command is not on (therefore NAT-T is enabled by default).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command, entered in global configuration mode, disables NAT-T for the crypto map entry named mymap:

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
isakmp nat-traversal	Enables NAT-T for all connections.
show running-config crypto map	Displays the crypto map configuration.

crypto map set peer

To specify an IPsec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode. Use the **no** form of this command to remove an IPsec peer from a crypto map entry.

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

Syntax Description

hostname	Specifies a peer by its hostname as defined by the ASA **name** command.
ip_address	Specifies a peer by its IP address (IPv4 or IPv6).
map-name	Specifies the name of the crypto map set.
peer	Specifies an IPsec peer in a crypto map entry either by hostname or IP address (IPv4 or IPv6). Multiple peers are not supported for IKEv2.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to allow up to 10 peer addresses.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used because the peer is usually unknown.

Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the ASA attempts to negotiate with the first peer in the list. If that peer does not respond, the ASA works its way down the list until either a peer responds or there are no more peers in the list. You can set up multiple peers only when using the backup LAN-to-LAN feature (that is, when the crypto map connection type is originate-only). For more information, see the **crypto map set connection-type** command.

Note Multiple peers are not supported for IKEv2.

Examples

The following example, entered in global configuration mode, shows a crypto map configuration using IKE to establish the security associations. In this example, you can set up a security association to either the peer at 10.0.0.1 or the peer at 10.0.0.2:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set pfs

Use the **crypto map set pfs** command in global configuration mode to set IPsec to ask for PFS when requesting new security associations for this crypto map entry or that IPsec requires PFS when receiving requests for new security associations. To specify that IPsec should not request PFS, use the **no** form of this command.

crypto map *map-name seq-num* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

no crypto map *map-name seq-num* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

Syntax Description

group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

By default PFS is not set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to add Diffie-Hellman group 7.
8.0(4)	The **group 7** command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

With PFS, each time a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. If the **set pfs** statement does not specify a group, the ASA sends the default (group2).

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the ASA assumes a default of group2. If the local configuration specifies group2 or group5, that group must be part of the peer's offer or the negotiation fails.

For a negotiation to succeed, PFS has to be set on both ends of the LAN to LAN tunnel (with or without the Diffie-Hellman group). If set, the groups have to be an exact match. The ASA does not accept just any offer of PFS from the peer.

The 1536-bit Diffie-Hellman prime modulus group, group5, provides more security than group1 or group2, but requires more processing time than the other groups.

When interacting with the Cisco VPN Client, the ASA does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example, entered in global configuration mode, specifies that PFS should be used whenever a new security association is negotiated for the crypto map mymap 10:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

Related Commands

Command	Description
clear isakmp sa	Deletes the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups and their parameters.

crypto map set ikev1 phase1-mode

To specify the IKEv1 mode for phase 1 when initiating a connection to either main or aggressive, use the **crypto map set ikev1 phase1-mode** command in global configuration mode. To remove the setting for phase 1 IKEv1 negotiations, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

Syntax Description

aggressive	Specifies aggressive mode for Phase 1 IKEv1 negotiations.
group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
main	Specifies main mode for Phase 1 IKEv1 negotiations.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

The default Phase 1 mode is **main**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	The **group 7** command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
8.4(1)	The **ikev1** keyword was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command works only in initiator mode; not in responder mode. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the ASA uses group 2.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the phase one mode to aggressive using group 2:

```
hostname(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
hostname(config)#
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev2 phase1-mode

To specify the IKEv2 mode for Phase 1 when initiating a connection to either main or aggressive, use the **crypto map set ikev2 phase1-mode** command in global configuration mode. To remove the setting for Phase 1 IKEv2 negotiations, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

Syntax Description

aggressive	Specifies aggressive mode for Phase 1 IKEv2 negotiations.
group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
main	Specifies main mode for Phase 1 IKEv2 negotiations.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

The default Phase 1 mode is **main**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	The **group 7** command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command works only in initiator mode; not in responder mode. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the ASA uses group 2.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the Phase 1 mode to aggressive, using group 2.

```
hostname(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
hostname(config)#
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set reverse-route

To enable reverse route injection for any connection based on this crypto map entry, use the **crypto map set reverse-route** command in global configuration mode. To disable reverse route injection for any connection based this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set reverse-route**

no crypto map *map-name seq-num s***et reverse-route**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

The default setting for this command is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ASA can automatically add static routes to the routing table and announce these routes to its private network or border routers using OSPF.

Examples

The following example, entered in global configuration mode, enables reverse route injection for the crypto map named mymap.

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations, use the **crypto map set security-association lifetime** command in global configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

Syntax Description

kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.
map-name	Specifies the name of the crypto map set.
seconds	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).
seq-num	Specifies the number that you assign to the crypto map entry.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the ASA requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations.

When the ASA receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

There are two lifetimes: a timed lifetime and a traffic-volume lifetime. The session keys and security association expire after the first of these lifetimes is reached. You can specify both with one command.

Note The ASA lets you change crypto map, dynamic map, and IPsec settings on-the-fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the access list, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

To change the timed lifetime, use the **crypto map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for the crypto map mymap:

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev1 transform-set

To specify the IKEv1 transform sets to use in a crypto map entry, use the **crypto map set transform-set** command in global configuration mode. To remove the names of the transform sets from a crypto map entry, use the **no** form of this command with the specified transform set name. To specify all or none of the transform sets and remove the crypto map entry, use the **no** form of the command.

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
transform-set-name1 *transform-set-name11*	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec transform-set** command. Each crypto map entry supports up to 11 transform sets.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The maximum number of transform sets in a crypto map entry was modified.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is required for all crypto map entries.

The peer at the opposite end of the IPsec initiation uses the first matching transform set for the security association. If the local ASA initiates the negotiation, the order specified in the **crypto map** command determines the order in which the ASA presents the contents of the transform sets to the peer. If the peer initiates the negotiation, the local ASA uses the first transform set in the crypto map entry that matches the IPsec parameters sent by the peer.

If the peer at the opposite end of the IPsec initiation fails to match the values of the transform sets, IPsec does not establish a security association. The initiator drops the traffic because there is no security association to protect it.

To change the list of transform sets, specify a new list to replace the old one.

If you use this command to modify a crypto map, the ASA modifies only the crypto map entry with the same sequence number you specify. For example, the ASA inserts the transform set named 56des-sha in the last position if you enter the following commands:

```
hostname(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
hostname(config)# crypto map map1 1 transform-set 56des-sha
hostname(config)#
```

The response to the following command shows the cumulative effect of the previous two commands:

```
hostname(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

To reconfigure the sequence of transform sets in a crypto map entry, delete the entry, specifying both the map name and sequence number; then recreate it. For example, the following commands reconfigure the crypto map entry named map2, sequence 3:

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

Examples

The **crypto ipsec transform-set** (create or remove transform set) section shows ten transform set commands. The following example creates a crypto map entry named map2 consisting of the same ten transform sets:

```
hostname(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

The following example, entered in global configuration mode, shows the minimum required crypto map configuration when the ASA uses IKE to establish the security associations:

```
hostname(config)# crypto map map2 10 ipsec-isakmp
hostname(config)# crypto map map2 10 match address 101
hostname(config)# crypto map map2 set transform-set 3des-md5
hostname(config)# crypto map map2 set peer 10.0.0.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
clear configure crypto map	Clears all crypto maps from the configuration.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
crypto ipsec transform-set	Configures a transform set.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev2 ipsec-proposal

To specify the IKEv2 proposal to use in a crypto map entry, use the **crypto map set ikev2 ipsec-proposal** command in global configuration mode. To remove the names of the proposals from a crypto map entry, use the **no** form of this command with the specified proposal name. To specify all or none of the proposal and remove the crypto map entry, use the **no** form of the command.

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1* [*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1* [*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
propsal-name1 *proposal-name11*	Specifies one or more names of the IPsec proposals for IKEv2. Any proposal named in this command must be defined in the **crypto ipsec ikev2 ipsec-proposal** command. Each crypto map entry supports up to 11 proposals.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.4(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

For all crypto map entries, an IKEv1 transform set or an IKEv2 proposal is required.

The peer at the opposite end of the IPsec IKEv2 initiation uses the first matching proposal for the security association. If the local ASA initiates the negotiation, the order specified in the **crypto map** command determines the order in which theASA presents the contents of the proposals to the peer. If the peer initiates the negotiation, the local ASA uses the first proposal in the crypto map entry that matches the IPsec parameters sent by the peer.

If the peer at the opposite end of the IPsec initiation fails to match the values of the proposals, IPsec does not establish a security association. The initiator drops the traffic because there is no security association to protect it.

To change the list of proposals, create a new list and specify it to replace the old one.

If you use this command to modify a crypto map, the ASA modifies only the crypto map entry with the same sequence number you specify. For example, the ASA inserts the proposal named 56des-sha in the last position if you enter the following commands:

```
hostname(config)# crypto map map1 1 set ikev2 ipsec-proposal 128aes-md5 128aes-sha
192aes-md5
hostname(config)# crypto map map1 1 set ikev2 ipsec-proposal 56des-sha
hostname(config)#
```

The response to the following command shows the cumulative effect of the previous two commands:

```
hostname(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

To reconfigure the sequence of proposals in a crypto map entry, delete the entry, specifying both the map name and sequence number; then recreate it. For example, the following commands reconfigure the crypto map entry named *map2*, sequence 3:

```
asa2(config)# no crypto map map2 3 set ikev2 ipsec-proposal
asa2(config)# crypto map map2 3 set ikev2 ipsec-proposal 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

Examples

The following example creates a crypto map entry named map2, consisting of ten proposals.

```
hostname(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
clear configure crypto map	Clears all crypto maps from the configuration.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
crypto ipsec transform-set	Configures a transform set.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto map set tfc-packets

To enable dummy Traffic Flow Confidentiality (TFC) packets on an IPsec SA, use the **crypto map set tfc-packets** command in global configuration mode. To disable TFC packets on an IPsec SA, use the **no** form of this command.

crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

no crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

This command configures the existing DF policy (at an SA level) for the crypto map.

crypto map set trustpoint

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

Syntax Description

chain	(Optional) Sends a certificate chain. A CA certificate chain includes all CA certificates in a hierarchy of certificates from the root certificate to the identity certificate. The default value is disable (no chain).
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.
trustpoint-name	Identifies the certificate to be sent during Phase 1 negotiations. The default is none.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This crypto map command is valid only for initiating a connection. For information on the responder side, see the **tunnel-group** commands.

Examples

The following example, entered in global configuration mode, specifies a trustpoint named tpoint1 for crypto map mymap and includes the chain of certificates:

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups.

crypto map set validate-icmp-errors

To specify whether or not to validate incoming ICMP error messages received through an IPsec tunnel that are destined for an interior host on the private network, use the **crypto map set validate-icmp-errors** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

crypto map *name priority* **set validate-icmp-errors**

no crypto map *name priority* **set validate-icmp-errors**

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

This crypto map command is valid only for validating incoming ICMP error messages.

csc

To enable the ASA to send network traffic to the CSC SSM, use the **csc** command in class configuration mode. To remove the configuration, use the **no** form of this command.

csc {**fail-open** | **fail-close**}

no csc

Syntax Description

fail-close	Specifies that the adaptive ASA should block traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.
fail-open	Specifies that the adaptive ASA should allow traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Class configuration mode is accessible from policy map configuration mode.

The **csc** command configures a security policy to send to the CSC SSM all traffic that is matched by the applicable class map. This occurs before the ASA allows the traffic to continue to its destination.

You can specify how the ASA treats matching traffic when the CSC SSM is not available to scan the traffic. The **fail-open** keyword specifies that the ASA permits the traffic to continue to its destination even though the CSC SSM is not available. The **fail-close** keyword specifies that the ASA never lets matching traffic continue to its destination when the CSC SSM is not available.

The CSC SSM can scan HTTP, SMTP, POP3, and FTP traffic. It supports these protocols only when the destination port of the packet requesting the connection is the well-known port for the protocol, that is, CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21
- HTTP connections opened to TCP port 80

- POP3 connections opened to TCP port 110
- SMTP connections opened to TCP port 25

If policies using the **csc** command select connections that misuse these ports for other protocols, the ASA passes the packets to the CSC SSM; however, the CSC SSM passes the packets without scanning them.

To maximize the efficiency of the CSC SSM, configure class maps used by policies implementing the **csc** command as follows:

- Select only the supported protocols that you that want the CSC SSM to scan. For example, if you do not want to scan HTTP traffic, be sure that service policies do not divert HTTP traffic to the CSC SSM.
- Select only those connections that risk trusted hosts protected by the ASA. These are connections from outside or untrusted networks to inside networks. We recommend scanning the following connections:
  - Outbound HTTP connections
  - FTP connections from clients inside the ASA to servers outside the ASA
  - POP3 connections from clients inside the ASA to servers outside the ASA
  - Incoming SMTP connections destined to inside mail servers

FTP Scanning

The CSC SSM supports scanning of FTP file transfers only if the primary channel for the FTP session uses the standard port, which is TCP port 21.

FTP inspection must be enabled for the FTP traffic that you want scanned by the CSC SSM. This is because FTP uses a dynamically assigned secondary channel for data transfer. The ASA determines the port assigned for the secondary channel and opens a pinhole to allow the data transfer to occur. If the CSC SSM is configured to scan FTP data, the ASA diverts the data traffic to the CSC SSM.

You can apply FTP inspection either globally or to the same interface that the **csc** command is applied to. By default, FTP inspection is enabled globally. If you have not changed the default inspection configuration, no further FTP inspection configuration is required to enable FTP scanning by the CSC SSM.

For more information about FTP inspection or the default inspection configuration, see the CLI configuration guide.

Examples

The ASA should be configured to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. HTTP requests from the inside network to the web server on the DMZ network should not be scanned.

The following configuration creates two service policies. The first policy, csc_out_policy, is applied to the inside interface and uses the csc_out access list to ensure that all outbound requests for FTP and POP3 are scanned. The csc_out access list also ensures that HTTP connections from inside to networks on the outside interface are scanned, but the access list includes a deny ACE to exclude HTTP connections from inside to servers on the DMZ network.

The second policy, csc_in_policy, is applied to the outside interface and uses the csc_in access list to ensure that requests for SMTP and HTTP originating on the outside interface and destined for the DMZ network are scanned by the CSC SSM. Scanning HTTP requests protects the web server from HTTP file uploads.

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
```

```
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

Note FTP inspection must be enabled for the CSC SSM to scan files transferred by FTP. FTP inspection is enabled by default.

Related Commands

Commands	Description
class (policy-map)	Specifies a class map for traffic classification.
class-map	Creates a traffic classification map, for use with a policy map.
match port	Matches traffic using a destination port.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.

csd enable

To enable Cisco Secure Desktop (CSD) for clientless SSL VPN remote access or remote access using the AnyConnect client, use the **csd enable** command in webvpn configuration mode. To disable CSD, use the **no** form of this command.

csd enable

no csd enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

CSD is enabled or disabled globally for all remote access connection attempts made to the ASA with one exception.

The **csd enable** command does the following:

1. Provides a validity check that supplements the check performed by the previous **csd image** *path* command.
2. Creates an sdesktop folder on disk0: if one is not already present.
3. Inserts a data.xml (Cisco Secure Desktop configuration) file in the sdesktop folder if one is not already present.
4. Loads the data.xml from the flash device to the running configuration.
5. Enables CSD.

Note

- You can enter the **show webvpn csd** command to determine whether or not Cisco Secure Desktop is enabled.
- The **csd image** *path* command must be in the running configuration before you enter the **csd enable** command.

- The **no csd enable** command disables CSD in the running configuration. If CSD is disabled, you cannot access CSD Manager and remote users cannot use CSD.
- If you transfer or replace the data.xml file, disable and then enable CSD to load the file into the running configuration.
- CSD is enabled or disabled globally for all remote access connection attempts made to the ASA. You cannot enable or disable CSD for an individual connection profile or group policy.

  Exception: Connection profiles for clientless SSL VPN connections can be configured so that CSD will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and CSD is enabled globally. For example:

```
hostname(config)# tunnel-group group-name webvpn-attributes
hostname(config-tunnel-webvpn)# group-url https://www.url-string.com
hostname(config-tunnel-webvpn)# without-csd
```

Examples

The following commands shows how to view the status of the CSD image and enable it:

```
hostname(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)#
```

Related Commands

Command	Description
csd image	Copies the CSD image named in the command from the flash drive specified in the path to the running configuration.
show webvpn csd	Identifies the version of CSD if it is enabled. Otherwise, the CLI indicates "Secure Desktop is not enabled."
without-csd	Configures connection profiles for clientless SSL VPN sessions so that CSD will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and CSD is enabled globally.

csd hostscan image

To install or upgrade the Cisco Host Scan distribution package and add it to the running configuration, use the **csd hostscan image** command in webvpn configuration mode. To remove the Host Scan distribution package from the running configuration, use the **no** form of this command:

csd hostscan image *path*

no csd hostscan image *path*

Syntax Description

path	Specifies the path and filename of the Cisco Host Scan package, up to 255 characters. The Host Scan package can be a standalone Host Scan package that has the file name convention, hostscan-*version*.pkg, or it can be the full AnyConnect Secure Mobility Client package that can be downloaded from Cisco.com and has the file name convention, anyconnect-win-*version*-k9.pkg. When customers specify the AnyConnect Secure Mobility Client, the ASA extracts the Host Scan package from the AnyConnect package and installs it. The Host Scan package contains the Host Scan software as well as the Host Scan library and support charts. This command cannot upload a CSD image. Use the **csd image** command for that operation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Enter the **show webvpn csd hostscan** command to determine the version of the Host Scan image that is currently installed and enabled.

After installing Host Scan with the **csd hostscan image** command, enable the image using the **csd enable** command.

Enter the **write memory** command to save the running configuration to ensure that the Host Scan image is available the next time that the ASA reboots.

Examples

The following commands show how to install a Cisco Host Scan package, enable it, view it, and save the configuration on the flash drive:

```
hostname> en
Password: ******
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
hostname(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
hostname(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd hostscan	Identifies the version of Cisco Host Scan if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd enable	Enables CSD for management and remote user access.

csd image

To validate the Cisco Secure Desktop (CSD) distribution package and add it to the running configuration, effectively installing CSD, use the **csd image** command in webvpn configuration mode. To remove the CSD distribution package from the running configuration, use the **no** form of the command:

csd image *path*

no csd image *path*

Syntax Description

path	Specifies the path and filename of the CSD package, up to 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Enter the **show webvpn csd** command to determine whetheror not the CSD image is enabled before entering this command. The CLI indicates the version of the CSD image that is currently installed if it is enabled.

Use the **csd image** command to install a new Cisco Secure Desktop image, or upgrade an existing image, after you download it to your computer, and transfer it to the flash drive. When downloading it, be sure to get the correct file for the ASA; it is in the form securedesktop_asa_<n>_<n>*.pkg.

Entering the **no csd image** command removes both management access to CSD Manager and remote user access to CSD. The ASA does not make any changes to the CSD software and the CSD configuration on the flash drive when you enter this command.

Note Enter the **write memory** command to save the running configuration to ensure CSD is available the next time that the ASA reboots.

Examples

The following commands show how to view the current CSD distribution package, view the contents of the flash file system, and upgrade to a new version:

```
hostname# show webvpn csd
```

```
Secure Desktop version 3.1.0.24 is currently installed and enabled.
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
hostname(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
hostname(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd	Identifies the version of CSD if it is enabled. Otherwise, the CLI indicates "Secure Desktop is not enabled."
csd enable	Enables CSD for management and remote user access.

ctl

To enable the Certificate Trust List (CTL) provider to parse the CTL file from the CTL client and install trustpoints, use the **ctl** command in ctl provider configuration mode. To remove the configuration, use the **no** form of this command.

ctl install

no ctl install

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ctl provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **ctl** command in ctl provider configuration mode to enable the CTL provider to parse the CTL file from the CTL client and install trustpoints for entries from the CTL file. Ttrustpoints installed by this command have names prefixed with "_internal_CTL_<ctl_name>."

If this command is disabled, each CallManager server and CAPFs certificate must be manually imported and installed via the **crypto ca trustpoint** and **crypto ca certificate chain** commands.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

ctl-file (global)

To specify the CTL instance to create for a phone proxy or to parse the CTL file stored in flash memory, use the **ctl-file** command in global configuration mode. To remove the CTL instance, use the **no** form of this command.

ctl-file *ctl_name* **noconfirm**

no ctl-file *ctl_name* **noconfirm**

Syntax Description

ctl_name	Specifies the name of the CTL instance.
noconfirm	(Optional) Used with the **no** command, stops warnings about deleting trustpoints when the CTL file is removed from being printed to the ASA console.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

If users have phones that require LSC provisioning, you must also import the CAPF certificate into the ASA from the CUMC when configuring the CTL file instance with the **ctl-file** command. For more information,see the CLI configuration guide.

Note To create the CTL file, use the **no shutdown** command in the ctl file configuration mode. To modify or add entries to a CTL file or to delete a CTL file, use the **shutdown** command.

Using the **no** form of the command removes the CTL file and all enrolled trustpoints internally created by a phone proxy. Additionally, removing the CTL file deletes all certificates received from the related certificate authority.

Examples

The following example shows how to configure the CTL file for the phone proxy feature:

```
hostname(config)# ctl-file myctl
```

Related Commands

Command	Description
ctl-file (phone-proxy)	Specifies the CTL file to use when configuring the phone proxy instance.
cluster-ctl-file	Parses the CTL file stored in flash memory to install the trustpoints from that file.
phone-proxy	Configures the phone proxy instance.
record-entry	Specifies the trustpoints to be used for the creation of the CTL file.
sast	Specifies the number of SAST certificates to create in the CTL record.

ctl-file (phone-proxy)

To specify the CTL instance to use when configuring the Phone Proxy, use the **ctl-file** command in phone-proxy configuration mode. To remove the CTL instance, use the **no** form of this command.

ctl-file *ctl_name*

no ctl-file *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **ctl-file** command to configure the CTL file for the Phone Proxy feature:

```
hostname(config-phone-proxy)# ctl-file myctl
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from flash memory.
phone-proxy	Configures the Phone Proxy Instance.

ctl-provider

To configure a CTL provider instance in CTL provider mode, use the **ctl-provider** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL provider instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **ctl-provider** command to enter CTL provider configuration mode to create a CTL provider instance.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and the username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.
export	Specifies the certificate to be exported to the client.

Commands	Description
service	Specify the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

cts import-pac

To import a Protected Access Credential (PAC) file from the Cisco ISE, use the **cts import-pac** command in global configuration mode:

cts import-pac *filepath* **password** *value*

Syntax Description

filepath	Specifies one of the following **exec** mode commands and options:. **Single Mode** • **disk0**: Path and filename on disk0 • **disk1**: Path and filename on disk1 • **flash**: Path and filename on flash • **ftp**: Path and filename on FTP • **http**: Path and filename on HTTP • **https**: Path and filename on HTTPS • **smb**: Path and filename on SMB • **tftp**: Path and filename on TFTP **Multi-mode** • **http**: Path and filename on HTTP • **https**: Path and filename on HTTPS • **smb**: Path and filename on SMB • **tftp**: Path and filename on TFTP
password *value*	Specifies the password used to encrypt the PAC file. The password is independent of the password that was configured on the ISE as part of the device credentials. The password must match the one provided when the PAC file was requested, and is necessary to decrypt the PAC data. This password is not related to the one that is configured on the ISE as part of the device credentials.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Importing the PAC file to the ASA establishes the connection with the ISE. After the channel is established, the ASA initiates a secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data; specifically, the ASA downloads the security group table. The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups. No channel is established prior to the RADIUS transaction. The ASA initiates a RADIUS transaction with the ISE using the PAC for authentication.

Tip The PAC file contains a shared key that allows the ASA and ISE to secure the RADIUS transactions that occur between them. Given the sensitive nature of this key, it must be stored securely on the ASA.

After successfully importing the file, the ASA download Cisco TrustSec environment data from the ISE without requiring the device password configured in the ISE.

The ASA stores the PAC file in an area of NVRAM that is not accessible through the user interface.

Prerequisites

- The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can generate a PAC file. The ASA can import any PAC file but it will only work on the ASA when the file was generated by a properly configured ISE.
- Obtain the password used to encrypt the PAC file when generating it on the ISE.

  The ASA requires this password to import and decrypt the PAC file.
- Access to the PAC file generated by the ISE. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not have to reside on the ASA flash before you can import it.)
- The server group has been configured for the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must import the PAC file to the primary ASA device.
- When the ASA is part of a clustering configuration, you must import the PAC file to the master device.

Examples

The following example imports a PAC from the ISE:

```
hostname(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

Related Commands

Command	Description
cts refresh environment-data	Refreshes the Cisco TrustSec environment data from the ISE when the ASA is integrated with Cisco TrustSec
cts sxp enable	Enables the SXP protocol on the ASA.

cts refresh environment-data

To refresh the Cisco TrustSec environment data from the ISE and reset the reconcile timer to the configured default value, use the **cts refresh environment-data** command in global configuration mode:

cts refresh environment-data

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

When the ASA is integrated with Cisco TrustSec, the ASA downloads environment data from the ISE, which includes the Security Group Tag (SGT) name table. The ASA automatically refreshes its environment data obtained from the ISE when you complete the following tasks on the ASA:

- Configure a AAA server to communicate with the ISE.
- Import a PAC file from the ISE.
- Identify the AAA server group that the ASA will use for retrieval of Cisco TrustSec environment data.

Normally, you will not need to manually refresh the environment data from the ISE; however, security groups can change on the ISE. These changes are not reflected on the ASA until you refresh the data in the ASA security group table. Refresh the data on the ASA to make sure any security group made on the ISE are reflected on the ASA.

Tip We recommend that you schedule policy configuration changes on the ISE and the manual data refresh on the ASA during a maintenance window. Handling policy configuration changes in this way maximizes the chances of security group names getting resolved and security policies becoming active immediately on the ASA.

Prerequisites

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE and the ASA must have successfully imported a PAC file, so that the changes made for Cisco TrustSec are applied to the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must refresh the environment data on the primary ASA device.
- When the ASA is part of a clustering configuration, you must refresh the environment data on the master device.

Examples

The following example downloads the Cisco TrustSec environment data from the ISE:

```
hostname(config)# cts refresh environment-data
```

Related Commands

Command	Description
cts import-pac	Imports a Protected Access Credential (PAC) file from the Cisco ISE when the ASA is integrated with Cisco TrustSec.
cts sxp enable	Enables the SXP protocol on the ASA.

cts server-group

To identify the AAA server group that the ASA uses to integrate with Cisco TrustSec for environment data retrieval, use the **cts server-group** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts server-group *aaa-server-group-name*

no cts server-group [*aaa-server-group-name*]

Syntax Description

aaa-server-group-name	Specifies the name of an existing, locally configured AAA server group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

As part of configuring the ASA to integrate with Cisco TrustSec, you must configure the ASA so that it can communicate with the ISE. Only one instance of the server group can be configured on the ASA for Cisco TrustSec.

Prerequisites

- The referenced server group must exist. If specify a undefined server group name in the *aaa-server-group-name* argument, the ASA will display an error message.
- The referenced server group must be configured to use the RADIUS protocol. If you add a non-RADIUS server group to the ASA, the feature configuration will fail.
- If the ISE is also used for user authentication, obtain the shared secret that was entered on the ISE when you registered the ASA with the ISE. Contact your ISE administrator if you do not have this information.

Examples

The following example locally configures on the ASA the AAA server group for the ISE and configures the ASA to use that AAA server group for the ASA integration with Cisco TrustSec:

```
hostname(config)# aaa-server ISEserver protocol radius
```

```
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server ISEserver (inside) host 192.0.2.1
hostname(config-aaa-server-host)# key myexclusivemumblekey
hostname(config-aaa-server-host)# exit
hostname(config)# cts server-group ISEserver
```

Related Commands

Command	Description
aaa-server *server-tag* **protocol radius**	Creates the AAA server group and configures the AAA server parameters for the ASA to communicate with the ISE server; where *server-tag* specifies the server group name.
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	Configures a AAA server as part of a AAA server group and sets host-specific connection data; where (*interface-name*) specifies the network interface where the ISE server resides, and *server-tag* is the name of the AAA server group for the Cisco TrustSec integration, and e *server-ip* specifies the IP address of the ISE server.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp connection peer

To set up an SXP connection to an SXP peer, use the **cts sxp connection peer** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **mode**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

no cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] [**password** {**default** | **none**}] [**mode** {**local** | **peer**}] [**speaker** | **listener**]

Syntax Description

default	Used with the **password** keyword. Specifies to use the default password configured for SXP connections.
listener	Specifies that the ASA functions as a listener for the SXP connection; meaning that the ASA can receive IP-SGT mappings from downstream devices. Specifying a speaker or listener role for the ASA for the SPX connection is required.
local	Used with the **mode** keyword. Species to use the local SXP device.
mode	(Optional) Specifies the mode of the SXP connection.
none	Used with the **password** keyword. Specifies not to use a password for the SXP connection.
password	(Optional) Specifies whether to use the authentication key for the SXP connection.
peer	Used with the **mode** keyword. Species to use the peer SXP device.
peer_ip_address	Specifies the IPv4 or IPv6 address of the SXP peer. The peer IP address must be reachable from the ASA outgoing interface.
source *source_ip_address*	(Optional) Specifies the local IPv4 or IPv6 address of the SXP connection.
speaker	Specifies that the ASA functions as a speaker for the SXP connection; meaning that the ASA can forward IP-SGT mappings to upstream devices. Specifying a speaker or listener role for the ASA for the SPX connection is required.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

SXP connections between peers are point-to-point and use TCP as the underlying transport protocol. SXP connections are set per IP address; a single device pair can service multiple SXP connections.

Restrictions

- The ASA does not support per-connection passwords for SXP connection.
- When you use the **cts sxp default password** to configure a default SXP password, you should configure the SXP connection to use the default password; conversely, when you do not configure a default password, you should not configure a default password for the SXP connection. If you do not follow these two guidelines, SXP connections can fail.
- When you configure an SXP connection with a default password, but the ASA does not have default password configured, the SXP connection will fail.
- When you configure a source IP address for an SXP connection, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, the SXP connection will fail.

  When the source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection. We recommend that you do not configure a source IP address for SXP connection and allow the ASA to perform a route/ARP lookup to determine the source IP address for the SXP connection.
- Configuring an IPv6 local link address for an SXP peer or source is not supported.
- Configuring multiple IPv6 addresses on the same interface for SXP connections is not supported.

Examples

The following example creates an SXP connection on the ASA:

```
hostname(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
```

Related Commands

Command	Description
cts sxp default password	Specifies the default password for SXP connectios.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp default password

To configure a default password for TCP MD5 authentication with SXP peers, use the **cts sxp default password** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp default password [**0** | **8**] *password*

no cts sxp default password [**0** | **8**] [*password*]

Syntax Description

0	(Optional) Specifies that the default password use unencrypted cleartext for the encryption level. You can only set one encryption level for the default password.
8	(Optional) Specifies that the default password use encrypted text for the encryption level.
password	Specifies an encrypted string up to 162 characters or an ASCII key string up to 80 characters.

Defaults

By default, SXP connections do not have a password set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

When you configure an SXP connection with a default password, but the ASA does not have default password configured, the SXP connection will fail.

Restrictions

- The ASA does not support per-connection passwords for SXP connection.
- When you use the **cts sxp default password** to configure a default SXP password, you should configure the SXP connection to use the default password; conversely, when you do not configure a default password, you should not configure a default password for the SXP connection. If you do not follow these two guidelines, SXP connections can fail.

Examples

The following example shows how to set default values for all SXP connections, including a default password for SXP connections:

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp default source-ip 192.168.1.100
hostname(config)# cts sxp default password 8 ********
hostname(config)# cts sxp retry period 60
hostname(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer. Specifying the **password default** keywords with this command, enables the use of the default password for that SXP connection.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp default source-ip

To configure a default local IP address for SXP connections, use the **cts sxp default source-ip** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp default source-ip *ipaddress*

no cts sxp default source-ip [*ipaddress*]

Syntax Description

ipaddress	Specifies an IPv4 or IPv6 address for the source IP address.

Defaults

By default, SXP connections do not have a default source IP address set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

When you configure a default source IP address for SXP connections, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, SXP connections will fail.

When a source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection. We recommend that you do not configure a default source IP address for SXP connections and allow the ASA to perform a route/ARP lookup to determine the source IP address for an SXP connection.

Examples

The following example shows how to set default values for all SXP connections, including a default source IP address for SXP connections:

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp default source-ip 192.168.1.100
hostname(config)# cts sxp default password 8 ********
hostname(config)# cts sxp retry period 60
hostname(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA. Specifying the **source** *source_ip_address* keyword and argument with this command, enables the use of the default source IP address for that SXP connection.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp enable

To enable the SXP protocol on the ASA, use the **cts sxp enable** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp enable

no cts sxp enable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the SXP protocol is disabled on the ASA.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Examples

The following example enables the SXP protocol on the ASA:

```
hostname(config)# cts sxp enable
```

Related Commands

Command	Description
clear cts	Clears data used by the ASA when integrated with Cisco TrustSec.
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.

cts sxp reconciliation period

To ..., use the **cts sxp reconciliation period** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp reconciliation period *timervalue*

no cts sxp reconciliation period [*timervalue*]

Syntax Description

timervalue	Specifies the default value for the reconciliation timer. Enter the number of seconds in the range of 1 to 64000 seconds.

Defaults

By default, the *timervalue* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

After an SXP peer terminates its SXP connection, the ASAstarts a hold down timer. If an SXP peer connects while the hold down timer is running, the ASA starts the reconciliation timer; then, the ASA updates the SXP mapping database to learn the latest mappings.

When the reconciliation timer expires, the ASA scans the SXP mapping database to identify stale mapping entries (entries that were learned in a previous connection session). The ASA marks these connections as obsolete. When the reconciliation timer expires, the ASA removes the obsolete entries from the SXP mapping database.

You cannot specify 0 for the timer because specifying 0 would prevent the reconciliation timer from starting. Not allowing the reconciliation timer to run would keep stale entries for an undefined time and cause unexpected results from the policy enforcement.

Examples

The following example shows how to set default values for all SXP connections, including a default reconciliation timer:

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp default source-ip 192.168.1.100
hostname(config)# cts sxp default password 8 ********
hostname(config)# cts sxp retry period 60
```

```
hostname(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp retry period

To specify the default time interval between ASA attempts to set up new SXP connections between SXP peers., use the **cts sxp retry period** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp retry period *timervalue*

no cts sxp retry period [*timervalue*]

Syntax Description

timervalue	Specifies the default value for the retry timer. Enter the number of seconds in the range of 0 to 64000 seconds.

Defaults

By default, the *timervalue* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Specifies the default time interval between ASA attempts to set up new SXP connections between SXP peers. The ASA continues to make connection attempts until a successful connection is made.

The retry timer is triggered as long as there is one SXP connection on the ASA that is not up.

If you specify 0 seconds, the timer never expires and the ASA will not attempt to connect to SXP peers.

When the retry timer expires, the ASA goes through the connection database and if the database contains any connections that are off or in a “pending on” state, the ASA restarts the retry timer.

We recommend you configure the retry timer to a different value from its SXP peer devices.

Examples

The following example shows how to set default values for all SXP connections, including a default retry period:

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp default source-ip 192.168.1.100
hostname(config)# cts sxp default password 8 ********
hostname(config)# cts sxp retry period 60
hostname(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.
cts sxp enable	Enables the SXP protocol on the ASA.

customization

To specify the customization to use for a tunnel group, group, or user, use the **customization** command in tunnel-group webvpn-attributes configuration mode or webvpn configuration mode. To not specify a customization, use the **no** form of this command.

customization ***name***

no customization *name*

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

Syntax Description

name	Specifies the name of the WebVPN customization to apply to a group or user.
none	Disables customization for the group or user, and prevents the customization from being inherited.
value *name*	Specifies the name of a customization to apply to the group policy or user.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn-attributes configuration	•	—	•	—	—
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Before entering the **customization** command in tunnel-group webvpn-attributes configuration mode, you must name and configure the customization using the **customization** command in webvpn configuration mode.

Mode-Dependent Command Options

The keywords available with the **customization** command differ depending on the mode you are in. In group-policy attributes configuration mode and username attributes configuration mode, the additional keywords **none** and **value** appear.

For example, if you enter the **customization none** command from username attributes configuration mode, the ASA will not look for the value in the group policy or tunnel group.

Examples

The following example shows a command sequence that first establishes a WebVPN customization named “123” that defines a password prompt. The example then defines a WebVPN tunnel group named “test” and uses the **customization** command to specifies the use of the WebVPN customization named “123”:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization 123
hostname(config-tunnel-webvpn)#
```

The folowing example shows the customization named “cisco” applied to the group policy named “cisco_sales.” Note that the additional command option **value** is required with the **customization** command entered in group-policy attributes configuration mode via webvpn configuration mode:

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)#  webvpn
hostname(config-group-webvpn)# customization value cisco
```

Related Commands

Command	Description
clear configure tunnel-group	Removes all tunnel group configuration.
show running-config tunnel-group	Displays the current tunnel group configuration.
tunnel-group webvpn-attributes	Enters the webvpn configuration mode for configuring WebVPN tunnel group attributes.

cxsc

To redirect traffic to the ASA CX module, use the **cxsc** command in class configuration mode. To remove the ASA CX action, use the **no** form of this command.

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

no cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

Syntax Description

auth-proxy	(Optional) Enables the authentication proxy, which is required for active authentication.
fail-close	Sets the ASA to block all traffic if the ASA CX module is unavailable.
fail-open	Sets the ASA to allow all traffic through, uninspected, if the ASA CX module is unavailable.
monitor-only	For demonstration purposes only, specify **monitor-only** to send a read-only copy of traffic to the ASA CX module. When you configure this option, you see a warning message similar to the following: `WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.`

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.4(4.1)	We introduced this command.
9.1(2)	We added the **monitor-only** keyword to support demonstration functionality.
9.1(3)	You can now configure ASA CX policies per context.

Usage Guidelines

You can access the class configuration mode by first entering the policy-map command.

Before or after you configure the **cxsc** command on the ASA, configure the security policy on the ASA CX module using Cisco Prime Security Manager (PRSM).

To configure the **cxsc** command, you must first configure the **class-map** command, **policy-map** command, and the **class** command.

Traffic Flow

The ASA CX module runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. When you apply the **cxsc** command for a class of traffic on the ASA, traffic flows through the ASA and the ASA CX module in the following way:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA CX module over the backplane.
5. The ASA CX module applies its security policy to the traffic and takes appropriate actions.
6. Valid traffic is sent back to the ASA over the backplane; the ASA CX module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

Information About Authentication Proxy

When the ASA CX needs to authenticate an HTTP user (to take advantage of identity policies), you must configure the ASA to act as an authentication proxy: the ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. By default, the port is 885 (user configurable with the **cxsc auth-proxy port** command). Configure this feature as part of the service policy to divert traffic from the ASA to the ASA CX module. If you do not enable the authentication proxy, only passive authentication is available.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA CX module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

To take full advantage of the ASA CX module features, see the following guidelines for traffic that you send to the ASA CX module:

- Do not configure ASA inspection on HTTP traffic.
- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both the ASA CX action and Cloud Web Security inspection for the same traffic, the ASA only performs the ASA CX action.
- Other application inspections on the ASA are compatible with the ASA CX module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA CX module.
- Do not enable ASA clustering; it is not compatible with the ASA CX module.
- If you enable failover, when the ASA fails over, any existing ASA CX flows are transferred to the new ASA, but the traffic is allowed through the ASA without being acted upon by the ASA CX module. Only new flows recieved by the new ASA are acted upon by the ASA CX module.

Monitor-Only Mode

For testing and demonstration purposes, you can configure the ASA to send a duplicate stream of read-only traffic to the ASA CX module using the **monitor-only** keyword, so you can see how the module inspects the traffic without affecting the ASA traffic flow. In this mode, the ASA CX module

inspects the traffic as usual, makes policy decisions, and generates events. However, because the packets are read-only copies, the module actions do not affect the actual traffic. Instead, the module drops the copies after inspection.

See the following guidelines:

- You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed.
- The following features are not supported in monitor-only mode:
  - Deny policies
  - Active authentication
  - Decryption policies
- The ASA CX does not perform packet buffering in monitor-only mode, and events will be generated on a best effort basis. For example, some events, such as ones with long URLs spanning packet boundaries, may be impacted by the lack of buffering.
- Be sure to configure both the ASA policy and the ASA CX to have matching modes: both in monitor-only, or both in normal inline mode.

Examples

The following example diverts all HTTP traffic to the ASA CX module and blocks all HTTP traffic if the ASA CX module card fails for any reason:

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the ASA CX module and allows all traffic through if the ASA CX module fails for any reason:

```
hostname(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list my-cx-acl
hostname(config)# class-map my-cx-class2
hostname(config-cmap)# match access-list my-cx-acl2
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap)# class my-cx-class2
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy interface outside
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
cxsc auth-proxy port	Sets the authentication proxy port.
debug cxsc	Enables ASA CX debugging messages.
hw-module module password-reset	Resets the module password to the default.

Command	Description
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
session do get-config	Gets the module configuration.
session do password-reset	Resets the module password to the default.
session do setup host ip	Configures the module management address.
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show module	Shows the module status.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.

cxsc auth-proxy port

To set the authentication proxy port for ASA CX module traffic, use the **cxsc auth-proxy port** command in global configuration mode. To set the port to the default, use the **no** form of this command.

cxsc auth-proxy port *port*

no cxsc auth-proxy port [*port*]

Syntax Description

port *port*	Sets the authentication proxy port to a value higher than 1024. The default is 885.

Command Default

The default port is 885.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.4(4.1)	We introduced this command.
9.1(3)	You can now configure ASA CX policies per context.

Usage Guidelines

If you enable the authentication proxy when you configure the **cxsc** command, you can change the port using this command.

When the ASA CX needs to authenticate an HTTP user (to take advantage of identity policies), you must configure the ASA to act as an authentication proxy: the ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. By default, the port is 885. Configure this feature as part of the service policy to divert traffic from the ASA to the ASA CX module. If you do not enable the authentication proxy, only passive authentication is available.

Examples

The following example enables the authentication proxy for ASA CX traffic, then changes the port to 5000:

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

```
hostname(config)# cxsc auth-port 5000
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
cxsc	Redirects traffic to the ASA CX module.
debug cxsc	Enables ASA CX debug messages.
hw-module module password-reset	Resets the module password to the default.
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset, and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
session do get-config	Gets the module configuration.
session do password-reset	Resets the module password to the default.
session do setup host ip	Configures the module management address.
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show module	Shows the module status.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.