crypto a – crypto ir

crypto am-disable

To disable IPsec IKEv1 inbound aggressive mode connections, use the **crypto ikev1 am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

crypto ikev1 am-disable
no crypto ikev1 am-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp am-disable** command was added.
7.2.(1)	The **crypto isakmp am-disable** command replaces the **isakmp am-disable** command**.**
8.4(1)	The command name was changed from crypto isakmp **am-disable to crypto ikev1 am-disable.**

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
ciscoasa(config)# crypto ikev1 am-disable
```

Related Commands

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

crypto ca alerts expiration

Expiration checking for all installed certificates is enabled by default with the **crypto ca alerts expiration** command. To disable expiration checking, use the **no** form of this command:

crypto ca alerts expiration [**begin** < **days before expiration** > [**repeat** < **days** >]
[**no**] **crypto ca alerts expiration** [**begin** < **days before expiration** > [**repeat** < **days** >]

Syntax Description

begin <days before expiration>	Set the interval at which the reminders are sent by configuring the number of days before expiration at which the first alert will go out. The range is from 1 to 90 days.
repeat <*days*>	Configure the alert frequency if the certificate is not renewed. The range is 1 to 14 days.

Command Default

Expiration checking for all installed certificate is enabled by default.

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

Command Modes

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

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Since the reminders are syslog messages, we do not anticipate a need for disabling. This command has little impact on performance because it is only checked once a day. By default we will send the first alert 60 days prior to expiration and once every week after that until the certificate is renewed and removed. In addition, an alert is sent on the day of the expiration and once every day after that. Irrespective of the alerts configuration, a reminder is sent every day during the last week of expiration.

Examples

```
100(config)# crypto ca ?
configure mode commands/options:
  alerts        Configure alerts
100(config)# crypto ca alerts ?
configure mode commands/options:
  expiration  Configure an alert for certificates nearing expiration
100(config)# crypto ca alerts expiration ?
configure mode commands/options:
  begin   Begin alert
  repeat  Repeat alert
  <cr>100(config)# crypto ca alerts expiration begin ?
```

```
configure mode commands/options:
  <1-90>  Days prior to expiration at which the first alert should be sent
100(config)# crypto ca alerts expiration begin 10 ?
configure mode commands/options:
  repeat  Repeat alert
  <cr>
100(config)# crypto ca alerts expiration begin 10 repeat ?
configure mode commands/options:
  <1-14>  Number of days at which the alert should be repeated after the prior
           alert
100(config)# crypto ca alerts expiration begin 10 repeat 1
100(config)# show run crypto ca ?
exec mode commands/options:
  alerts       Show alerts


   server    Show local certificate server configuration
 trustpoint     Show trustpoints
   trustpool    Show trustpool
  |            Output modifiers
  <cr>
100(config)# show run crypto ca alerts
crypto ca alerts expiration begin 10 repeat 1
100(config)# clear conf crypto ca ?
configure mode commands/options:
  alerts       Clear alerts
  certificate  Clear certificate map entries
  server       Clear Local CA server
  trustpoint   Clear trustpoints
  trustpool    Clear trustpool
100(config)# clear conf crypto ca alerts
```

Related Commands

Command	Description
clear conf crypto ca alerts	Clears the configured crypto ca alerts.
show run crypto ca alerts	Shows the configured crypto ca alerts.

crypto ca authenticate

To install and authenticate the CA certificates associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *trustpoint* [**allow-untrusted-connection**] [**fingerprint** *hexvalue*] [**nointeractive**]

Syntax Description

fingerprint	Specifies a hash value consisting of alphanumeric characters that the ASA uses to authenticate the CA certificate. If a fingerprint is provided, the ASA compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the ASA displays the computed fingerprint and asks whether to accept the certificate.
hexvalue	Identifies the hexadecimal value of the fingerprint.
allow-untrusted-connection	Allows the ASA to ignore EST server certificate validation failure. This option is available only for trustpoints that are configured with the EST enrollment protocol.
nointeractive	Obtains the CA certificate for this trustpoint using no interactive mode; intended for use by the device manager only. In this case, if there is no fingerprint, the ASA accepts the certificate without question.
trustpoint	Specifies the trustpoint from which to obtain the CA certificate. The maximum name length is 128 characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.16(1)	The **allow-untrusted-connection** keyword was introduced to ignore EST server certificate validation failure.

Usage Guidelines

Use the **crypto ca authenticate** command to add a CA certificate to a trustpoint in the ASA configuration. When configured, the certificate is considered trusted.

If the trustpoint is configured for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, the ASA prompts you to paste the base-64 formatted CA certificate into the terminal.

The **allow-untrusted-connection** keyword can be used to allow the ASA to ignore server certificate validation failure for EST trustpoints.

The invocations of this command do not become part of the running configuration.

Examples

The following example shows the ASA requesting the certificate of the CA. The CA sends its certificate and the ASA prompts the administrator to verify the certificate of the CA by checking the CA certificate fingerprint. The ASA administrator should verify the fingerprint value displayed with a known, correct value. If the fingerprint displayed by the ASA matches the correct value, you should accept the certificate as valid.

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
ciscoasa(config)#
```

The following example shows the trustpoint tp9 configured for terminal-based (manual) enrollment. The ASA prompts the administrator to paste the CA certificate into the terminal. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained.

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=
Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]:
yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

The following example shows successful certification validation when an EST trustpoint is configured without using **allow-untrusted-connection** and **nointeractive** keywords. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **nointeractive** keyword. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
   asa(config-ca-trustpoint)# crypto ca authenticate EST_TP nointeractive

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **allow-untrusted-connection**. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **allow-untrusted-connection** and **nointeractive** keywords. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection
nointeractive

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured without using **allow-untrusted-connection** and **nointeractive** keywords. ASA prompts the administrator to confirm if the TLS server certificate validation should be bypassed. If it is bypassed, the fingerprint of the certificate is displayed and the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
Bypass TLS server certificate validation: [yes/no]: yes

INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured with **nointeractive** keyword.

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP nointeractive

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
 ERROR: receiving Certificate Authority certificate: status = FAIL, cert length = 0
asa(config-ca-trustpoint)#
```

The following example shows failed certification validation when an EST trustpoint is configured with **allow-untrusted-connection** keyword. ASA bypasses the TLS server certificate validation. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured with **allow-untrusted-connection** and **nointeractive** keywords. ASA bypasses the TLS server certificate validation. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection
nointeractive

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when there is a fingerprint mismatch:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP fingerprint 87654321 1212121212
11111111 12345678

INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d
Fingerprint mismatch

Trustpoint CA certificate NOT accepted.
```

Related Commands

Command	Description
crypto ca enroll	Starts enrollment with a CA.
crypto ca import certificate	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca certificate chain

To enter certificate chain configuration mode for the indicated trustpoint, use the **crypto ca certificate chain** command in global configuration mode.

crypto ca certificate chain *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint for configuring the certificate chain.

Command Default

No default values or behaviors.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters certificate chain configuration mode for the trustpoint, central:

```
ciscoasa
(config)#
crypto ca certificate chain central
ciscoasa
(config-cert-chain)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.

crypto ca certificate map

To maintain a prioritized list of certificate mapping rules, use the **crypto ca certificate map** command in global configuration mode. To remove a crypto CA configuration map rule, use the **no** form of the command.

crypto ca certificate map { *sequence-number* | *map-name sequence-number* }
no crypto ca certificate map { *sequence-number* | *map-name sequence-number* }

Syntax Description

map-name	Specifies a name for a certificate-to-group map.
sequence-number	Specifies a number for the certificate map rule that you are creating. The range is 1 through 65535. You can use this number when creating a tunnel group map, which maps a tunnel group to a certificate map rule.

Command Default

The default value for *map-name* is DefaultCertificateMap.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The *map-name* option was added.

Usage Guidelines

Entering this command places the ASA in ca certificate map configuration mode, where you can configure rules based on the issuer and subject distinguished names (DNs) of the certificate. The sequence number orders the mapping rules. The general form of these rules is as follows:

- *DN match-criteria match-value*
- *DN* is either *subject-name* or *issuer-name*. DNs are defined in the ITU-T X.509 standard.
- *match-criteria* comprise the following expressions or operators:

attr *tag*	Limits the comparison to a specific DN attribute, such as common name (CN).
co	Contains
eq	Equal

nc	Does not contain
ne	Not equal

The DN matching expressions are case insensitive.

Examples

The following example enters ca certificate map mode with a map named example-map and a sequence number of 1 (rule # 1), and specifies that the common name (CN) attribute of the subject-name must match Example1:

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

The following example enters ca certificate map mode with a map named example-map and a sequence number of 1, and specifies that the subject-name contain the value cisco anywhere within it:

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

Related Commands

Command	Description
issuer-name	Indicates that rule entry is applied to the issuer DN of the IPsec peer certificate.
subject-name (crypto ca certificate map)	Indicates that rule entry is applied to the subject DN of the IPsec peer certificate.
tunnel-group-map enable	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

crypto ca crl request

To request a CRL based on the configuration parameters of the specified trustpoint, use the **crypto ca crl request** command in crypto ca trustpoint configuration mode.

crypto ca crl request *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint. The maximum number of characters allowed is 128.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the running configuration.

Examples

The following example requests a CRL based on the trustpoint named central:

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.

crypto ca enroll

To start the certificate enrollment process with the CA, use the **crypto ca enroll** command in global configuration mode.

crypto ca enroll *trustpoint* [**est-username** *name* **est-password** *password*] [**regenerate**] [**shared-secret** < **value** > | **signing-certificate** < **value** >] [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses all prompts. Enrollment options that might have been prompted for must be preconfigured in the trustpoint. This option is for use in scripts, ASDM, or other noninteractive needs.
regenerate	Indicates whether or not a new key pair should be generated prior to building the enrollment request.
shared-secret	A value provided out-of-band by the CA that is used to confirm the authenticity and integrity of the messages exchanged with ASA..
signing-certificate	The name of the trustpoint with a previously-issued device certificate used for signing the cmp enrollment request.
trustpoint	Specifies the name of the trustpoint to enroll with. The maximum number of characters allowed is 128.
est-username *user*	The EST username used for initial enrollment. This keyword is available only for trustpoints that are configured with the EST enrollment protocol.
est-password *password*	The EST password used for initial enrollment. This keyword is available only for trustpoints that are configured with the EST enrollment protocol.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The option to regenerate was added, and the shared-secret and signing-certificate keywords were added.

Release	Modification
9.16(1)	The provision to enroll an EST certificate was added.

Usage Guidelines

Use **crypto ca enroll** command to initiate a certificate enrollment or re-enrollment with a CA.

When the trustpoint is configured for SCEP enrollment, the ASA displays a CLI prompt immediately and status messages appear on the console asynchronously. When the trustpoint is configured for manual enrollment, the ASA writes a base-64-encoded PKCS10 certificate request to the console and then the CLI prompt appears.

This command generates interactive prompts that vary, depending on the configured state of the referenced trustpoint. For this command to run successfully, the trustpoint must have been configured correctly.

When a trustpoint is configured for CMP, either a shared secret value (ir) or the name of the trustpoint that contains the cert that will sign the request (cr) can be specified, but not both. The shared-secret or signing-certificate keywords are available only when the trustpoint enrollment protocol is set to CMP.

This command supports certificate enrollment using EST. You can provide the username and password credentials to authenticate the device to the EST server when issuing the enrollment request. Use this command regardless of whether a certificate has already been issued. If you do not provide the username and password credentials, the device uses the pre-existing device certificate to authenticate the device to the server. If a device certificate is not present, the command becomes invalid.

Examples

The following example requests enrollment for an identity certificate with trustpoint tp1 using SCEP enrollment. The ASA prompts for information not stored in the trustpoint configuration.

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
ciscoasa(config)#
```

The following example shows manual enrollment of a CA certificate:

ciscoasa(config)# **crypto ca enroll tp1**

```
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
```

```
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
ciscoasa(config)#
```

Examples

The following example requests enrollment for an identity certificate with trustpoint EST_TP using EST enrollment, when the http credentials are provided:

```
asa(config-ca-trustpoint)# crypto ca enroll EST_TP ?
configure mode commands/options:
  est-username       Specify EST username for HTTP authentication
  <CR>

asa(config)# crypto ca enroll EST_TP username ?

configure mode commands/options:
  WORD < 32 char username required for initial EST enrollment.
asa(config)# crypto ca enroll EST_TP username ESTUSER ?

configure mode commands/options:
 est-password         Specify EST password for HTTP authentication
asa(config)# crypto ca enroll EST_TP user ESTUSER password ?

configure mode commands/options:
  WORD < 32 char password required for initial EST enrollment

asa(config)# crypto ca enroll EST_TP est-username ESTUSER est-password ESTPASSWORD ?

configure mode commands/options:
  noconfirm  Specify this keyword to suppress all interactive prompting.

asa(config)# crypto ca enroll EST_TP est-username ESTUSER est-password ESTPASSWORD
%
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: asa.cisco.com

% The serial number in the certificate will be: FCH1814JT76

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
asa(config)# The certificate has been granted by CA!
```

The following example shows re-enrollment using device certificates:

```
asa(config-ca-trustpoint)# crypto ca enroll EST_TP
%
WARNING: Trustpoint EST_TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the existing certificate will be replaced.

Do you want to continue with re-enrollment? [yes/no]: yes
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: asa.cisco.com
```

```
% The serial number in the certificate will be: FCH1814JT76

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
asa(config)# The certificate has been granted by CA!
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca import pkcs12	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca export

To export the ASA trustpoint configuration with all associated keys and certificates in PKCS12 format, or to export the device identity certificate in PEM format, use the **crypto ca export** command in global configuration mode.

crypto ca export *trustpoint* **identity-certificate**

Syntax Description

identity-certificate	Specifies that the enrolled certificate associated with the named trustpoint is to be displayed on the console.
trustpoint	Specifies the name of the trustpoint whose certificate is to be displayed. The maximum number of characters allowed for a trustpoint name is 128.

Command Default

No default values or behaviors.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	This command was changed to accommodate certificate exporting in PEM format.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The PEM or PKCS12 data is written to the console.

Web browsers use the PKCS12 format to store private keys with accompanying public key certificates protected with a password-based symmetric key. The ASA exports the certificates and keys associated with a trustpoint in base64-encoded PKCS12 format. This feature can be used to move certificates and keys between ASAs.

PEM encoding of a certificate is a base64 encoding of an X.509 certificate enclosed by PEM headers. This encoding provides a standard method for text-based transfer of certificates between ASAs. PEM encoding can be used to export the *proxy-ldc-issuer* certificate using an SSL/TLS protocol proxy when the ASA is acting as a client.

Examples

The following example exports the PEM-formatted certificate for trustpoint 222 as a console display:

```
ciscoasa
```

```
 (config)#
crypto ca export 222 identity-certificate
Exported 222 follows:
```

-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt

hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==

-----END CERTIFICATE-----

```
ciscoasa
 (config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca import

To install a certificate received from a CA in response to a manual enrollment request or to import the certificate and key pair for a trustpoint using PKCS12 data, use the **crypto ca import** command in global configuration mode.

crypto ca import *trustpoint* **certificate** [**nointeractive**]
crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

Syntax Description

certificate	Tells the ASA to import a certificate from the CA represented by the trustpoint.
nointeractive	(Optional) Imports a certificate using nointeractive mode, which suppresses all prompts. This option is for use in scripts, ASDM, or other noninteractive needs.
passphrase	Specifies the passphrase used to decrypt the PKCS12 data.
pkcs12	Tells the ASA to import a certificate and key pair for a trustpoint, using PKCS12 format.
trustpoint	Specifies the trustpoint with which to associate the import action. The maximum number of characters allowed is 128. If you import PKCS12 data and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example manually imports a certificate for the trustpoint Main:

```
ciscoasa
 (config)#
crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com
Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself[ certificate data omitted ]quit
INFO: Certificate successfully imported
```

```
ciscoasa
 (config)#
```

The following example manually imports PKCS12 data to a trustpoint central:

```
ciscoasa
 (config)#
crypto ca import central pkcs12 ?
configure mode commands/options:
 WORD Passphrase used to protect the pkcs12 data
Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:[ PKCS12 data omitted ]quit
INFO: Import PKCS12 operation completed successfully
ciscoasa
 (config)#
```

The following example, entered in global configuration mode with passphrase *Wh0ist*, generates a warning message because there is not enough space in NVRAM to save the RSA keypair:

```
ciscoasa(config)# crypto ca import central pkcs12 Wh0ist

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
INFO: The name for the keys will be: central
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair central. Remove any unnecessary keypairs
 and save the running config before using this keypair.
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca export	Exports a trustpoint certificate and key pair in PKCS12 format.
crypto ca authenticate	Obtains the CA certificate for a trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca trustpoint	Enters the crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca permit-weak-crypto

ASA does not support CA certificates with the SHA-1 with RSA encryption algorithm and RSA key sizes smaller than 2048 bits. You can use the **crypto ca permit-weak-crypto** command to override certification restrictions. We do not recommend you to use this option, because the certificates generated with weak ciphers and key sizes are not as secure as the certificates with bigger key sizes and strong ciphers.

[no] crypto ca permit-weak-crypto

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

When you enable **permit-weak-crypto**, ASA allows the following options when validating certificates:

- SHA-1 with RSA encryption algorithm.
- RSA key sizes smaller than 2048 bits.

If the **permit-weak-crypto** option is not enabled, the certificate validation operations fail when these attributes are present.

Examples

The following example enables weak-crypto on the ASA:

```
asa(config)# crypto ca ?

configure mode commands/options:
permit-weak-crypto (Not Recommended) permit weak key sizes and hash algorithms
```

crypto ca reference-identity

To configure a reference-identity object, use the **crypto ca reference-identity** command in configuration mode. To delete a reference-identity object, use the **no** form of this command.

crypto ca reference-identity *reference_identity_name*
no crypto ca reference-identity *reference_identity_name*

Enter the **crypto ca reference-identity** command in global configuration mode to place the ASA in ca-reference-identity mode. Enter the following reference-ids while in ca-reference-identity mode. Multiple reference-ids of any type may be added. Use the no form of each command to remove reference-ids.

[**no**] **cn-id** *value*
[**no**] **dns-id** *value*
[**no**] **srv-id** *value*
[**no**] **uri-id** *value*

Syntax Description

reference-identity-name	Name of the reference-identity object.
value	Value of each reference-id.
cn-id	Common Name (CN), where the value matches the overall form of a domain name. The CN value cannot be free text. A CN-ID reference identifier does not identify an application service.
dns-id	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.
srv-id	A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of "_imaps.example.net" would be split into a DNS domain name portion of "example.net" and an application service type portion of "imaps."
uri-id	A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a "scheme" and (ii) a "host" component (or its equivalent) that matches the "reg-name" rule specified in RFC 3986. A URI-ID identifier must contain the DNS domain name, not the IP address, and not just the hostname. For example, a URI-ID of "sip:voice.example.edu" would be split into a DNS domain name portion of "voice.example.edu" and an application service type of "sip."

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Enter the **crypto ca reference-identity** command in global configuration mode to place the ASA in ca-reference-identity mode. Enter the following reference-ids while in ca-reference-identity mode: cn-id, dns-id, srv-id, or uri-id. Multiple reference-ids of any type may be added. Use the no form of each command to remove reference-ids.

A reference identity is created when configuring one with a previously unused name. Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

When multiple entries are used, the following behavior is expected if the certificate contains at least one instance of srv-id, uri-id, or dns-id:

- If any instance of uri-id in the certificate matches any instance of uri-id on the named reference id, then the certificate matches the reference identity.
- If any instance of srv-id in the certificate matches any instance of srv-id on the named reference id, then the certificate matches the reference identity.
- If any instance of dns-id in the certificate matches any instance of dns-id on the named reference id, then the certificate matches the reference identity.
- If none of these scenarios exist, the certificate does not match the reference identity.

When multiple entries are used, the following behavior is expected if the certificate does not contain at least one instance of srv-id, uri-id, or dns-id but does contain at least one cn-id:

- If any instance of cn-id in the certificate matches any instance of cn-id on the named reference id, then the certificate matches the reference identity. Otherwise, the certificate does not match the reference identity.
- If the certificate does not contain at least one instance of srv-id, uri-id, dns-id, or cn-id, then the certificate does not match the reference identity.

When the ASA is acting as a TLS client, it supports rules for verification of an application server's identity as defined in RFC 6125. Reference identities are configured on the ASA, to be compared to the identity presented in a server certificate during connection establishment. These identifiers are specific instances of the four identifier types also specified in RFC 6125.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
cn-id	Configures a Common Name Identifier in the reference-identity object.
dns-id	Configures and DNS domain name Identifier in a reference identity object.
srv-id	Configures a SRV-ID identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

crypto ca server (Deprecated)

To set up and manage a local CA server on the ASA, use the **crypto ca server** command in global configuration mode. To delete the configured local CA server from the ASA, use the **no** form of this command.

crypto ca server
no crypto ca server

Syntax Description

This command has no arguments or keywords.

Command Default

A certificate authority server is not enabled on the ASA.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.12(1)	Provision to configure user's FQDN for the enrollment URL, under smtp command. If not configured, the ASAs' FQDN will be used by default. This command is being deprecated and will be removed in a future release.
9.13(1)	This command was removed.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

There can only be one local CA on an ASA.

The **crypto ca server** command configures the CA server, but does not enable it. Use the **no** form of the **shutdown** command in ca server configuration mode to enable the local CA.

When you activate the CA server with the **no shutdown** command, you establish the RSA keypair of the CA and a trustpoint named LOCAL-CA-SERVER to hold the self-signed certificate. This newly generated self-signed certificate always has digital signature, CRL signing, and certificate signing key usage settings set.

Beginning with version 9.12(1), ASA allows users to configure their FQDN for the enrollment URL. Typically, users have an internal DNS configured as the ASAs FQDN and an external DNS configured with the FQDN that is included in the enrollment email. Using the fqdn command, the users can configure their FQDN for the enrollment URLinstead of ASAs' FQDN. If not configured, ASA uses its FQDN by default.

Caution The **no crypto ca server** command deletes the configured local CA server, its RSA keypair, and the associated trustpoint, regardless of the current state of the local CA server.

Examples

The following example enters ca server configuration mode, then lists the local CA server commands available in that mode:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# ?
CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

The following example shows configuration of user’s fqdn under smtp command and the verification output:

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp fqdn asa1-localCA.server.amazon.com
ciscoasa(config-ca-server)# show run crypto ca server
crypto ca server
smtp fqdn asa1-localCA.server.amazon.com
```

The following example uses the **no** form of the **crypto ca server** command in ca server configuration mode to delete the configured and enabled CA server from the ASA:

```
ciscoasa
(config-ca-server)
# no crypto ca server
Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

Related Commands

Command	Description
debug crypto ca server	Shows debugging messages when you configure the local CA server.
show crypto ca server	Displays the status and parameters of the configured CA server.
show crypto ca server cert-db	Displays local CA server certificates.

crypto ca server crl issue

To force the issuance of a Certificate Revocation List (CRL), use the **crypto ca server crl issue** command in privileged EXEC mode.

crypto ca server crl issue

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use this command to recover a lost CRL. Normally, the CRL is reissued automatically at expiration by resigning the existing CRL. The **crypto ca server crl issue** command regenerates the CRL based on the certificate database and should only be used as required to regenerate a CRL based on the certificate database contents.

Examples

The following example forces the issuance of a CRL by the local CA server:

```
ciscoasa
(config-ca-server)
# crypto ca server crl issue
```

A new CRL has been issued.

```
ciscoasa
```

```
(config-ca-server)
#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
show crypto ca server crl	Displays the current CRL of the local CA.

crypto ca server revoke

To mark a certificate issued by the local Certificate Authority (CA) server as revoked in the certificate database and the CRL, use the **crypto ca server revoke** command in privileged EXEC mode.

crypto ca server revoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of the certificate to be revoked, which must be in hexadecimal format.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You revoke a specific certificate that has been issued by the local CA on an ASA by entering the **crypto ca server revoke** command on that ASA. Revocation is accomplished when this command marks the certificate as revoked in the certificate database on the CA server and in the CRL. You specify the certificate to be revoked by entering the certificate serial number in hexadecimal format.

The CRL is regenerated automatically after the specified certificate is revoked.

Examples

The following example revokes the certificate with the serial number 782ea09f issued by the local CA server:

```
ciscoasa
(config-ca-server)#
# crypto ca server revoke 782ea09f
```

Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server unrevoke	Unrevokes a revoked certificate issued by the local CA server.
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server crl	Displays the current CRL of the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server unrevoke

To unrevoke a revoked certificate issued by the local CA server, use the **crypto ca server unrevoke** command in privileged EXEC mode.

crypto ca server unrevoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of the certificate to be unrevoked, which must be in hexadecimal format.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You unrevoke a revoked certificate issued by the local CA on an ASA by entering the **crypto ca server unrevoke** command. The validity of the certificate is restored when this command marks the certificate as valid in the certificate database and removes it from the CRL. You specify the certificate to be unrevoked by entering the certificate serial number in hexadecimal format.

The CRL is regenerated after the specified certificate is unrevoked.

Examples

The following example unrevokes the certificate with the serial number 782ea09f issued by the local CA server:

```
ciscoasa
(config-ca-server)
# crypto ca server unrevoke 782ea09f
```

Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been issued.

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
crypto ca server user-db add	Adds a user to the CA server user database.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db add

To insert a new user into the CA server user database, use the **crypto ca server user-db add** command in privileged EXEC mode.

crypto ca server user-db *user* [**dn** *dn*] [**email** *e-mail-address*]

Syntax Description

dn *dn*	Specifies a subject-name distinguished name for certificates issued to the added user. If a DN string contains spaces, enclose value with double quotes. You can only use commas to separate DN attributes (for example, “OU=Service, O=Company, Inc.”).
email *e-mail-address*	Specifies the e-mail address for the new user.
user	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or an e-mail address.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The *user argument* can be a simple username such as user1 or an e-mail address such as user1@example.com. The *username* must match the username specified by the end user in the enrollment page.

The *username* is added to the database as a user without privileges. You must use the **crypto ca server allow** command to grant enrollment privileges.

The *username* argument, along with the one-time password, is used to enroll the user on the enrollment interface page.

Note For e-mail notification of the one-time password (OTP), an e-mail address should be specified either in the *username* or *email-address* argument. A missing e-mail address at mailing time generates an error.

The **email** *e-mail-address* keyword-argument pair is used only as an e-mail address to notify the user for enrollment and renewal reminders and does not appear in the issued certificate.

Inclusion of the e-mail address ensures that the user can be contacted with any questions and is notified of the required one-time password for enrollment.

If an optional DN is not specified for a user, the subject name DN is formed using the *username* and the subject-name-default DN setting as cn=*username* , subject-name-default.

Examples

The following example adds a user to the user database with a username of user1@example.com with a complete subject-name DN:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering, o=Example, l=RTP, st=NC, c=US"
```

ciscoasa (config-ca-server) #

The following example grants enrollment privileges to the user named user2.

```
ciscoasa
(config-ca-server)
# crypto ca server user-db allow user2
```

ciscoasa (config-ca-server)

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage a local CA.
crypto ca server user-db allow	Permits a specific user or a subset of users in the CA server database to enroll with the CA.
crypto ca server user-db remove	Deletes a user from the CA server database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
database path	Specifies a path or location for the local CA database. The default location is flash memory.

crypto ca server user-db allow

To permit a user or a group of users to enroll in the local CA server database, use the **crypto ca server user-db allow** command in privileged EXEC mode. This command also includes options to generate and display one-time passwords or to e-mail them to users.

crypto ca server user-db allow { *username* | **all-unenrolled** | **all-certholders** } [**display-otp**] [**email-otp**] [**replace-otp**]

Syntax Description

all-certholders	Specifies that enrollment privileges be granted to all users in the database who have been issued a certificate, whether the certificate is valid or not. This is equivalent to granting renewal privileges.
all-unenrolled	Specifies that enrollment privileges be granted to all users in the database who have not been issued a certificate.
email-otp	(Optional) Sends the specified users one-time passwords by e-mail to their configured e-mail addresses.
replace-otp	(Optional) Specifies that one-time passwords be regenerated for all specified users who originally had valid one-time passwords.
display-otp	(Optional) Displays the one-time passwords for all specified users on the console.
username	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or e-mail address.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Release	Modification
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **replace-otp** keyword generates OTPs for all specified users. These new OTPs replace any valid ones generated for the specified users.

The OTP is not stored on the ASA, but is generated and regenerated as required to notify a user or to authenticate a user during enrollment.

Examples

The following example grants enrollment privileges to all users in the database who have not enrolled yet:

```
ciscoasa
(config-ca-server)#
 crypto ca server user-db allow all-unenrolled
ciscoasa
(config-ca-server)#
```

The following example grants enrollment privileges to the user named user1:

```
ciscoasa
(config-ca-server)#
 crypto ca server user-db allow user1
ciscoasa
(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage a local CA.
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
enrollment-retrieval	Specifies the time in hours that an enrolled user can retrieve a PKCS12 enrollment file.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db email-otp

To e-mail the OTP to a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db email-otp** command in privileged EXEC mode.

crypto ca server user-db email-otp { *username* | **all-unenrolled** | **all-certholders** }

Syntax Description

all-certholders	Specifies that OTPs are e-mailed to all users in the database who have been issued a certificate, whether that certificate is valid or not.
all-unenrolled	Specifies that the OTPs are e-mailed to all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user is e-mailed to that user. The username can be a username or an e-mail address.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example e-mails the OTP to all unenrolled users in the database:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db email-otp all-unenrolled
ciscoasa
(config-ca-server)
#
```

The following example e-mails the OTP to the user named user1:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db email-otp user1
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db show-otp	Displays the one-time password for a specific user or a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db remove

To remove a user from the local CA server user database, use the **crypto ca server user-db remove** command in privileged EXEC mode.

crypto ca server user-db remove *username*

Syntax Description

username	Specifies the name of the user to remove in the form of a username or an e-mail address.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command removes a username from the CA user database so that user cannot enroll. The command also providees the option to revoke previously issued, valid certificates.

Examples

The following example removes a user with a username, user1, from the CA server user database :

```
ciscoasa
(config-ca-server)
# crypto ca server user-db remove user1
WARNING: No certificates have been automatically revoked. Certificates issued to user user1
 should be revoked if necessary.
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
show crypto ca server user-db	Displays users included in the CA server user database.
crypto ca server user-db write	Writes the user information configured in the local CA database to the file specified by the **database path** command.

crypto ca server user-db show-otp

To display the OTP for a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db show-otp** command in privileged EXEC mode.

crypto ca server user-db show-otp { *username* | **all-certholders** | **all-unenrolled** }

Syntax Description

all-certholders	Displays the OTPs for all users in the database who have been issued a certificate, whether the certificate is currently valid or not.
all-unenrolled	Displays the OTPs for all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user be displayed. The *username* can be a username or an e-mail address.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example displays the OTP for all users who have valid or invalid certificates in the database:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db show-otp all-certholders
ciscoasa
```

```
(config-ca-server)
#
```

The following example displays the OTP for the user named user1:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db show-otp user1
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db allow	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
crypto ca server user-db email-otp	E-mails the one-time password to a specific user or to a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db write

To configure a directory location to store all the local CA database files, use the **crypto ca server user-db write** command in privileged EXEC mode.

crypto ca server user-db write

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **crypto ca server user-db write** command is used to save new user-based configuration data to the storage specified by the database path configuration. The information is generated when new users are added or allowed with the **crypto ca server user-db add** and **crypto ca server user-db allow** commands.

Examples

The following example writes the user information configured in the local CA database to storage:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db write
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
database path	Specifies a path or location for the local CA database. The default location is flash memory.
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca trustpoint

To enter the crypto ca trustpoint configuration mode for the specified trustpoint, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command.

crypto ca trustpoint *trustpoint-name*
no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

Syntax Description

noconfirm	Suppresses all interactive prompting
trustpoint-name	Identifies the name of the trustpoint to manage. The maximum name length allowed is 128 characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Added options to support the OCSP. These include **match certificate map**, **ocsp disable-nonce**, **ocsp url**, and **revocation-check**.
8.0(2)	Added options to support certificate validation. These include **id-usage** and **validation-policy. The following are being deprecated: accept-subordinates, id-cert-issuer, and support-user-cert-validation.**
8.0(4)	The **enrollment self** option was added to support enrollment of self-signed certificates between trusted enterprises, such as between phone proxy and TLS proxy.
9.13(1)	The **crl required | optional | nocheck** option was removed. The **match certificate** option was modified to include **override CDP** configuration
9.20(1)	The **alt-fqdn** option was added.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA. Issuing this command puts you in crypto ca trustpoint configuration mode.

This command manages trustpoint information. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint mode control CA-specific configuration parameters, which specify how the ASA obtains the CA certificate, how the ASA obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

You can specify characteristics for the trustpoint using the following commands:

- **accept-subordinates**—Deprecated. Indicates whether CA certificates subordinate to the CA associated with the trustpoint are accepted if delivered during phase one IKE exchange when not previously installed on the ASA.
- **alt-fqdn** *fqdn*—During enrollment, asks the CA to include the specified FQDN values in the subject alternative name extension of the certificate or requests.
- **auto-enroll**—Configures the parameters that control if CMPv2 auto update is used, when it is triggered, and if a new keypair is generated. Enter a percentage of the absolute lifetime of the certificate after which auto-enroll will be necessary. Then specify if you want to generate a new key while renewing the certificate: **[no] auto-enroll [<percent>] [regenerate]**
- **crl required | optional | nocheck**—Specifies CRL configuration options. Removed in ASA 9.13(1).
- **crl configure**—Enters crl configuration mode (see the **crl** command).
- **default enrollment**—Returns all enrollment parameters to their system default values. Invocations of this command do not become part of the active configuration.
- **email** *address*—During enrollment, asks the CA to include the specified email address in the subject alternative name extension of the certificate.
- **enrollment protocol cmp|scep** *url*—Specifies either CMP or SCEP enrollment to enroll with this trustpoint and configures the enrollment URL (*url*).
- **enrollment retry period** —Specifies a retry period in minutes for SCEP enrollment.
- **enrollment retry count**—Specifies a maximum number of permitted retries for SCEP enrollment.
- **enrollment terminal**—Specifies cut and paste enrollment with this trustpoint.
- **enrollment self**—Specifies enrollment that generates a self-signed certificate.
- **enrollment url**—Specifies the SCEP enrollment to enroll with this trustpoint and configures the enrollment URL (*url*).
- **exit**—Leaves the configuration mode.
- **fqdn** *fqdn*—During enrollment, asks the CA to include the specified FQDN in the subject alternative name extension of the certificate.
- **id-cert-issuer**—Deprecated. Indicates whether the system accepts peer certificates issued by the CA associated with this trustpoint.
- **id-usage**— Specifies how the enrolled identity of a trustpoint can be used.
- **ip-addr** *ip-address*—During enrollment, asks the CA to include the IP address of the ASA in the certificate.
- **keypair** *name*—Specifies the key pair whose public key is to be certified.

- **keypair** *name*—Specifies the keypair, as either RSA or EDCSA ,whose public key is to be certified and their modulus bits or elliptic curve bits.
- **match certificate** *map-name* **override ocsp | override cdp**—Matches a certificate map to an OCSP override or CDP override rule.
- **ocsp disable-nonce**—Disables the nonce extension, which cryptographically binds revocation requests with responses to avoid replay attacks.
- **ocsp url**—Specifies that the OCSP server at this URL check all certificates associated with this trustpoint for revocation status.
- **exit**—Leaves the configuration mode.
- **password** *string*—Specifies a challenge phrase that is registered with the CA during enrollment. The CA typically uses this phrase to authenticate a subsequent revocation request.
- **revocation check**—Specifies the revocation checking method, which includes CRL, OCSP, and none.
- **serial-number**—During enrollment, asks the CA to include the ASA serial number in the certificate.
- **subject-name** *X.500 name*—During enrollment, asks the CA to include the specified subject DN in the certificate. If a DN string includes a comma, enclose the value string with double quotes (for example, O=”Company, Inc.”)
- **support-user-cert-validation**—Deprecated. If enabled, the configuration settings to validate a remote user certificate can be taken from this trustpoint, provided that it is authenticated to the CA that issued the remote certificate. This option applies to the configuration data associated with the subcommands **crl required | optional | nocheck** and all settings in the CRL mode.
- **validation-policy**—Specifies trustpoint conditions for validating certificates associated with user connections.

Note When you try to connect, a warning occurs to indicate that the trustpoint does not contain an ID certificate when an attempt is made to retrieve the ID certificate from the trustpoint.

Examples

The following example enters ca trustpoint configuration mode for managing a trustpoint named central:

```
ciscoasa(config)# crypto ca trustpoint
central
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca certificate map	Enters crypto ca certificate map configuration mode. Defines certificate-based ACLs.

Command	Description
crypto ca crl request	Requests a CRL based on configuration parameters of a specified trustpoint.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request.

crypto ca trustpool export

To export the certificates that constitute the PKI trustpool, use the crypto ca trustpool export command in privileged EXEC configuration mode.

crypto ca trustpool export *filename*

Syntax Description

filename	The file in which to store the exported trustpool certificates.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command copies the entire contents of the active trustpool to the indicated filepath in pem-coded format.

Examples

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

Related Commands

Command	Description
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.

crypto ca trustpool import

To import the certificates that constitute the PKI trustpool, use the crypto ca trustpool import command in global configuration mode.

crypto ca trustpool import [**clean**] **url** *url [* **noconfirm** *[* **signature-required**]]

Syntax Description

clean	Removes all downloaded trustpool certificates prior to import.
noconfirm	Suppresses all interactive prompts.
signature-required	Indicates that only signed files are accepted.
url	The location of the trustpool file to be imported.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.
9.12(1)	The option to use the ASA's default trusted CA list was removed.

Usage Guidelines

This command provides the ability to validate the signature on the file when a trustpool bundle is downloaded from cisco.com. A valid signature is not mandatory when downloading bundles from other sources or in a format that does not support signatures. Users are informed of the signature status and are given the option to accept the bundle or not.

The possible interactive warnings are:

- Cisco bundle format with invalid signature
- Non-cisco bundle format
- Cisco bundle format with valid signature

The **signature-required** keyword is allowed only if the **noconfirm** option is selected. If the **signature-required** keyword is included but the signature is not present or cannot be verified, the import fails.

Note Unless you have verified the legitimacy of the file through some other means, do not install the certificates if a file signature cannot be verified,

The following example shows the behavior of the **crypto ca trustpool** import command when suppressing interactive prompting and requiring signatures:

ciscoasa(config)# **crypto ca trustpool import url ?**

configure mode commands/options:disk0: Import from disk0: file systemdisk1: Import from disk1: file systemflash: Import from flash: file systemftp: Import from ftp: file systemhttp: Import from http: file systemhttps: Import from https: file systemsmb: Import from smb: file systemsystem: Import from system: file systemtftp: Import from tftp: file system

ciscoasa(config)# **crypto ca trustpool import url http://mycompany.com ?**exec mode commands/options:noconfirm Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# **crypto ca trustpool import url http://mycompany.com noconfirm ?**exec mode commands/options:signature-required Indicate that only signed files will be accepted

Related Commands

Command	Description
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.

crypto ca trustpool policy

To enter a submode that provides the commands that define the trustpool policy, use the crypto ca trustpool policy command in global configuration mode. To set up the automatic import of a trustpool certificate bundle, specify the URL which the ASA uses to download and import the bundle.

crypto ca trustpool policy

Syntax Description

This command has no arguments or keywords.

auto-import	Configure automatic import of trustpool certificates
auto-import [time <H:M:S>] [url <URL address>]	Set custom time and custom URL for downloading certificates in trustpool if you need to schedule this download during off peak hours or any other convenient times.
auto-import time	Specify the download time in hours, minutes, and seconds. An attempt is made for every 24 hours at this specified time. If not provided, the default time of 22:00 hours is used.
auto-import url	Specify automatic import of trustpool certificates. If not provided, the default Cisco URL is used.

Command Default

No default behavior or values.

The automatic import option is turned off by default.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.
9.5(2)	The auto-import command option was added.

Examples

ciscoasa(config)# **crypto ca trustpool ?**

configure mode commands/options: policy Define trustpool policy

ciscoasa(config)# **crypto ca trustpool policy**ciscoasa(config-ca-trustpool)# **?**

CA Trustpool configuration commands:crl CRL optionsexit Exit from certificate authority trustpool entry modematch Match a certificate mapno Negate a command or set its defaultsrevocation-check Revocation checking options

auto-import Configure automatic import of trustpool certificatesciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import?

crypto-ca-trustpool mode commands/options:

time Specify the auto import time in hours, minutes, and secondsDefault is 22:00:00. An attempt is made every 24 hours at the specified time.url Specify the HTTP based URL address for automatic import of trustpool certificates

<cr>

ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import url ?

crypto-ca-trustpool mode commands/options:LINE URL for automatic importciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import time ?H:M:S Specify the auto import time in hours, minutes & seconds. E.g. 18:00:00 (attempt to import is made at every 24 hours at 6PM)ciscoasa(config-ca-trustpool)#

Related Commands

Command	Description
show crypto ca trustpool policy	Displays the configured trustpool policy.

crypto ca trustpool remove

To remove a single specified certificate from the PKI trustpool, use the crypto ca trustpool remove command in privileged EXEC configuration mode.

crypto ca trustpool remove *cert fingerprint* [**noconfirm**]

Syntax Description

cert fingerprint	Hex data.
noconfirm	Specify this keyword to suppress all interactive prompting.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Because this command will commit a change to the trusted root certificate content, interactive users will be prompted to confirm their actions.

Examples

```
ciscoasa# crypto ca trustpool remove ?
  Hex-data  Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm  Specify this keyword to suppress all interactive prompting.
```

Related Commands

Command	Description
clear crypto ca trustpool	Removes all certificates from the trustpool.
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.

crypto dynamic-map match address

To match the address of an access list for the dynamic crypto map entry, use the crypto dynamic-map match address command in global configuration mode. To disable the address match, use the **no** form of this command.

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

Syntax Description

acl-name	Identifies the access list to be matched for the dynamic crypto map entry.
dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

For a dynamic crypto map (with the crypto dynamic-map command), the access-list 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 increase.

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.

See the crypto map match address command for additional information about this command.

Examples

The following example shows the use of the **crypto dynamic-map** command to match address of an access list named aclist1:

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
ciscoasa(config)#
```

Related Commands

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

crypto dynamic-map set df-bit

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

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

Syntax Description

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

Command Default

The default setting is off.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

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 dynamic-map set ikev1 transform-set

To specify the IKEv1 transform sets to use in a dynamic crypto map entry, use the **crypto dynamic-map set ikev1 transform-set** command in global configuration mode.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*...transform-set-name11*]

To remove the transform sets from the dynamic crypto map entry, specify the transform set name in the **no** form of this command:

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*...transform-set-name11*]

To remove the dynamic crypto map entry, use the no form of the command and specify all or none of the transform sets:

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic 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 ikev1 transform-set** command. Each crypto map entry supports up to 11 transform sets.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was added.
7.2(1)	Changed the maximum number of transform sets in a crypto map entry.
8.4(1)	Added the ikev1 keyword.

Release	Modification
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A dynamic crypto map is a crypto map without all of the parameters configured. It acts as a policy template where the missing parameters are later dynamically learned, as the result of an IPsec negotiation, to match the peer requirements. The ASA applies a dynamic crypto map to let a peer negotiate a tunnel if its IP address is not already identified in a previous static or dynamic crypto map. This occurs with the following types of peers:

- Peers with dynamically assigned public IP addresses.

Both LAN-to-LAN and remote access peers can use DHCP to obtain a public IP address. The ASA uses this address only to initiate the tunnel.

- Peers with dynamically assigned private IP addresses.

Peers requesting remote access tunnels typically have private IP addresses assigned by the headend. Generally, LAN-to-LAN tunnels have a predetermined set of private networks that are used to configure static maps and therefore used to establish IPsec SAs.

As an administrator configuring static crypto maps, you might not know the IP addresses that are dynamically assigned (via DHCP or some other method), and you might not know the private IP addresses of other clients, regardless of how they were assigned. VPN clients typically do not have static IP addresses; they require a dynamic crypto map to allow IPsec negotiation to occur. For example, the headend assigns the IP address to a Cisco VPN client during IKE negotiation, which the client then uses to negotiate IPsec SAs.

Dynamic crypto maps can ease IPsec configuration and we recommend them for use in networks where the peers are not always predetermined. Use dynamic crypto maps for Cisco VPN clients (such as mobile users) and routers that obtain dynamically assigned IP addresses.

Tip Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If the traffic covered by such a **permit** entry could include multicast or broadcast traffic, insert **deny** entries for the appropriate address range into the access list. Remember to insert **deny** entries for network and subnet broadcast traffic, and for any other traffic that IPsec should not protect.

Dynamic crypto maps work only to negotiate SAs with remote peers that initiate the connection. The ASA cannot use dynamic crypto maps to initiate connections to a remote peer. With a dynamic crypto map configured, if the outbound traffic matches a permit entry in an access list and the corresponding SA does not yet exist, the ASA drops the traffic.

A crypto map set may include a dynamic crypto map. Dynamic crypto map sets should be the lowest priority crypto maps in the crypto map set (that is, they should have the highest sequence numbers) so that the ASA evaluates other crypto maps first. It examines the dynamic crypto map set only when the other (static) map entries do not match.

Similar to static crypto map sets, a dynamic crypto map set consists of all of the dynamic crypto maps with the same dynamic map name. The dynamic sequence number differentiates the dynamic crypto maps in a set. If you configure a dynamic crypto map, insert a permit ACL to identify the data flow of the IPsec peer for the crypto access list. Otherwise the ASA accepts any data flow identity the peer proposes.

Caution Do not assign static (default) routes for traffic to be tunneled to a ASA interface configured with a dynamic crypto map set. To identify the traffic that should be tunneled, add the ACLs to the dynamic crypto map. Use care to identify the proper address pools when configuring the ACLs associated with remote access tunnels. Use Reverse Route Injection to install routes only after the tunnel is up.

You can combine static and dynamic map entries within a single crypto map set.

Examples

The following example creates a dynamic crypto map entry named "dynamic0" consisting of the same ten transform sets.

```
ciscoasa(config)# crypto dynamic-map dynamic0 1 set
ikev1
transform-set 3des-md5 3des-sha 56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5
192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec **ikev1** transform-set	Configures an IKEv1 transform set.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto dynamic-map set ikev2 ipsec-proposal

To specify the IPsec proposals for IKEv2 to use in a dynamic crypto map entry, use the **crypto dynamic-map set ikev2 ipsec-proposal** command in global configuration mode. To remove the names of the transform sets from a dynamic crypto map entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name 1* [*...transform-set-name11*]
no crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name 1* [*...transform-set-name11*]

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
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 ikev2 transform-set** command. Each crypto map entry supports up to 11 transform sets.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

crypto dynamic-map set nat-t-disable

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

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

Syntax Description

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

Command Default

The default setting is off.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
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 dynamic-map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command disables NAT-T for the crypto dynamic map named mymap:

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

Related Commands

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

crypto dynamic-map set peer

See the crypto map set peer command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
hostname	Identifies the peer in the dynamic crypto map entry by hostname, as defined by the **name** command.
ip_address	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the **name** command.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address 10.0.0.1:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
ciscoasa(config)#
```

Related Commands

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

crypto dynamic-map set pfs

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

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

Syntax Description

group14	Specifies which Diffie-Hellman key exchange group to use.
group15	Specifies which Diffie-Hellman key exchange group to use.
group16	Specifies which Diffie-Hellman key exchange group to use.
group19	Specifies which Diffie-Hellman key exchange group to use.
group20	Specifies which Diffie-Hellman key exchange group to use.
group21	Specifies which Diffie-Hellman key exchange group to use.
group24	Specifies which Diffie-Hellman key exchange group to use.
map-name	Specifies the name of the crypto map set.
map-index	Specifies the number you assign to the crypto map entry.

Command Default

By default, PFS is not set.

Command Modes

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

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

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.

Release	Modification
9.0(1)	Support for multiple context mode was added.
9.12(1)	Support was removed for DH group 1. The **group 1** commands was deprecated.
9.13(1)	Support for group14, 15, and 16 command option was added. The **group 2** and **group 5** commands were deprecated and will be removed in later releases.
9.15(1)	Support for **group 1, 2, 5** and **24** command options is removed in this release.

With PFS, every 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.

The **crypto dynamic-map** commands, such as **match address**, **set peer**, and **set pfs** are described with the crypto map commands. 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 does not specify PFS, it accepts any offer of PFS from the peer.

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 specifies that PFS should be used whenever a new security association is negotiated for the crypto dynamic-map mymap 10. The group specified is group 2:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
The following example specifies support for group14:
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs groyp14
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2 (DEPRECATED)
```

Related Commands

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

crypto dynamic-map set reverse route

See the crypto map set reverse-route command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

Syntax Description

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

Command Default

The default value for this command is off.

Command Modes

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

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

Command History

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

Examples

The following command enables Reverse Route Injection for the crypto dynamic map named mymap:

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

Related Commands

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

crypto dynamic-map set security-association lifetime

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

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

Syntax Description

kilobytes {*number* | **unlimited**}	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The global default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
map-name	Specifies the name of the crypto map set.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The global default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.1(2)	Added **unlimited** argument.

Usage Guidelines

The dynamic 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.

For site-to-site VPN connections, there are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.

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 dynamic-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 dynamic crypto dynamic map mymap:

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

Related Commands

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

crypto dynamic-map set tfc-packets

To enable dummy Traffic Flow Confidentiality (TFC) packets on an IPsec SA, use the **crypto dynamic-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 dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]
no crypto dynamic-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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

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

crypto dynamic-map set validate-icmp-errors

To specify whether 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 dynamic-map set validate-icmp-errors** command in global configuration mode. To remove validation of incoming ICMP error messages from a crypto dynamic map entry, use the **no** form of this command.

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

Syntax Description

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

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

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

crypto engine accelerator-bias

To change the allocation of the cryptographic cores on Symmetric Multi-Processing (SMP) platforms, use the **crypto engine accelerator-bias** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]
no crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

Syntax Description

balanced	Equally distributes cryptographic hardware resources (Admin/SSL and IPsec cores)
ipsec	Allocates cryptographic hardware resources to favor IPsec cores (includes SRTP encrypted voice traffic). This is the default bias on ASA 5500-X series devices.
ssl	Allocates cryptographic hardware resources to favor Admin/SSL cores. Use this bias when you support SSL-based Secure Client remote access VPN sessions.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Cryptographic core rebalancing is available on the following platforms: ASA 5585, 5580, 5545/5555, ASASM, FP4110, FP4120, FP4140, FP4150, FP9300, SM-24, SM-36, and SM-44.

This command causes traffic disruption to services that require crypto operations. You must apply it in a maintenance window and without IPsec failure being configured.

Examples

The following examples show the options available for configuring the crypto engine acccelerator-bias command:

```
ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

To switch large modulus operations on an ASA 5510, 5520, 5540, or 5550 from software to hardware, use the **crypto engine large-mod-accel** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

crypto engine large-mod-accel
no crypto engine large-mod-accel

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA performs large modulus operations in the software.

Command Modes

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

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

Command History

Release	Modification
8.3(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is available only with the ASA models 5510, 5520, 5540, and 5550. It switches large modulus operations from software to hardware. The switch to hardware accelerates the following:

- 2048-bit RSA public key certificate processing.
- Diffie Hellman Group 5 (DH5) key generation.

We recommend that you use this command when necessary to improve the connections per second. Depending on the load, it might have a limited performance impact on SSL throughput.

We also recommend that you use either form of this command during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware or hardware to software.

Note The ASA 5580/5500-X platforms already integrate this capability to switch large modulus operations; therefore, **crypto engine** commands are not applicable on these platforms.

Examples

The following example switches large modulus operations from software to hardware:

```
ciscoasa(config)# crypto engine large-mod-accel
```

The following example removes the previous command from the configuration and switches large modulus operations back to software:

```
ciscoasa(config)# no crypto engine large-mod-accel
```

Related Commands

Command	Description
show running-config crypto engine	Shows if large modulus operations are switched to hardware.
clear configure crypto engine	Returns large modulus operations to software. This command is equivalent to the **no crypto engine large-mod-accel** command.

crypto ikev1 enable

To enable ISAKMP IKEv1 negotiation on the interface on which the IPsec peer communicates with the ASA, use the **crypto ikev1 enable** command in global configuration mode. To disable ISAKMP IKEv1 on the interface, use the **no** form of this command.

crypto ikev1 enable *interface-name*
no crypto ikev1 enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP IKEv1 negotiation.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This **isakmp enable** command was added.
7.2(1)	The **crypto isakmp enable** command replaced the **isakmp enable** command.
8.4(1)	With the addition of IKEv2 capability, the crypto isakmp enable command was changed to the crypto ikev1 enable command.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
ciscoasa(config)# no crypto isakmp enable
 inside
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.

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

crypto ikev1 ipsec-over-tcp

To enable IPsec over TCP, use the **crypto ikev1 ipsec-over-tcp** command in global configuration mode. To disable IPsec over TCP, use the **no** form of this command.

crypto ikev1 ipsec-over-tcp [**port** *port1 ... port10*]
no crypto ikev1 ipsec-over-tcp [**port** *port1 ... port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPsec over TCP connections. You can list up to 10 ports. Port numbers can be in the range of 1-65535. The default port number is 10000.

Command Default

The default value is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp ipsec-over-tcp** command was added.
7.2.(1)	The **crypto isakmp ipsec-over-tcp** command replaced the **isakmp ipsec-over-tcp** command**.**
8.4(1)	The command name was changed from **crypto isakmp ipsec-over-tcp to crypto ikev1 ipsec-over-tcp.**
9.0(1)	Support for multiple context mode was added.

Examples

This example, entered in global configuration mode, enables IPsec over TCP on port 45:

```
ciscoasa(config)# crypto ikev1 ipsec-over-tcp port 45
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.

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

crypto ikev1 limit max-in-negotiation-sa

To limit the number of IKEv1 in-negotiation (open) SAs on the ASA, use the **crypto ikev1 limit max-in-negotiation-sa** command in global configuration mode. To disable limits on the number of open SAs, use the **no** form of this command:

crypto ikev1 limit max-in-negotiation-sa *threshold percentage*
no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

Syntax Description

threshold percentage	The percentage of the total allowed SAs for the ASA that are allowed to be in negotiation (open). After reaching the threshold, additional connections are denied. The range is 1 to 100%. The default is 20% for all ASA platforms except ASA5506/ASA5508 (which is 100%).

Command Default

The default is 20%. The ASA limits the number of open SAs to 20% except ASA5506/ASA5508.

Usage Guidelines

The **crypto ikev1 limit-max-in-negotiation-sa** command limits the maximum number of SAs that can be in negotiation at any time. 1

The **crypto ikev1 limit max in-negotiation-sa** command stops further connections from negotiating to protect current connections and prevent memory and/or CPU attacks that the cookie-challenge feature may be unable to thwart.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.

Examples

The following example limits the number of IKEv1 connections that are in negotiation to 70 percent of the maximum allowable IKEv1 connections:

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

Related Commands

Command	Description
crypto ikev1 limit max-sa	Limits the number of IKEv1 connections on the ASA,

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 ikev1 policy

To create an IKEv1 security association (SA) for IPsec connections, use the crypto ikev2 policy command in global configuration mode. To remove the policy, use the **no** form of this command:

crypto ikev1 policy *priority*
no crypto ikev1 policy *priority*

Syntax Description

priority	The policy suite priority. The range is 1-65535, with 1 being the highest and 65535 the lowest.

Command Default

No default behavior or values.

Usage Guidelines

The command enters IKEv1 policy configuration mode, in which you specify additional IKEv1 SA settings. An IKEv1 SA is a key used in phase 1 to enable IKEv1 peers to communicate securely in phase 2. After entering the crypto ikev1 policy command, you can use additional commands to set the SA encryption algorithm, DH group, integrity algorithm, lifetime, and hash algorithm.

As the 3DES encryption cipher has been deprecated, the default encryption cipher for newly created IKE policies and IPsec proposals will now be AES-128. This applies only to new policies and proposals and will not affect any existing configuration items.

Command Modes

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

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

Command History

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

9.13(1)	• Support for DH groups 14, 15, and 16 was added. The **groups 1, 2** and **group 5** option is considered as insecure. These options were deprecated and will be removed in the later release.
	• Several integrity and PRF ciphers used ASA/Lina IKE, IPsec, and SSH modules are considered as insecure. The following ciphers are deprecated and will be removed in the later release:
	  • HMAC-MD5 integrity and PRF ciphers
	  • HMAC-MD5 integrity ciphers in IPsec
	  • HMAC-MD5, HMAC-MD5-96, and HMAC-SHA1-96 integrity ciphers
	  • AES-GMAC,3DES, DES.

Release	Modification

9.15(1)	• Support for DH groups **groups 1, 2** and **group 5** option is considered as insecure and are removed.
	• The following integrity and PRF ciphers used ASA/Lina IKE, IPsec, and SSH are considered insecure; they are removed from IKEv1 policy configuration:
	  • HMAC-MD5 integrity and PRF ciphers
	  • HMAC-MD5 integrity ciphers in IPsec
	  • HMAC-MD5, HMAC-MD5-96, and HMAC-SHA1-96 integrity ciphers
	  • AES-GMAC,3DES, DES.

Examples

The following example creates the priority 1 IKEv1 SA and enters IKEv1 policy configuration mode:

```
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)# authentication rsa-sig
ciscoasa(config-ikev1-policy)# hash md5
ciscoasa(config-ikev1-policy)# group 14
ciscoasa(config-ikev1-policy)# lifetime 300
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiate packets,
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 ikev2 cookie-challenge

To enable the ASA to send cookie challenges to peer devices in response to SA initiate packets, use the crypto ikev2 cookie-challenge command in global configuration mode. To disable cookie challenges, use the **no** form of this command:

crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**
no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

Syntax Description

threshold percentage	The percentage of the total allowed SAs for the ASA that are in negotiation, which triggers cookie challenges for any future SA negotiations. The range is zero to 99%. The default is 50%.
always	Always cookie-challenges incoming SAs.
never	Never cookie-challenges incoming SAs.

Command Default

No default behavior or values.

Usage Guidelines

Cookie challenging a peer prevents possible denial-of-service (DoS) attacks. An attacker initiates a DoS attack when the peer device sends an SA initiate packet and the ASA sends its response, but the peer device does not respond further. If the peer device does this continually, all the allowed SA requests on the ASA can be used up until it stops responding.

Enabling a threshold percentage using the crypto ikev2 cookie-challenge command limits the number of open SA negotiations. For example, with the default setting of 50%, when 50% of the allowed SAs are in negotiation (open), the ASA cookie-challenges any additional SA initiate packets that arrive. For the Cisco ASA 5580 with 10000 allowed IKEv2 SAs, after 5000 SAs have become open, any more incoming SAs are cookie-challenged.

If used in conjunction with the **crypto kev2 limit max in-negotiation-sa** command, configure the cookie-challenge threshold lower than the maximum in-negotiation threshold for an effective cross-check.

Command Modes

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

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

Command History

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

Examples

In the following example, the cookie-challenge threshold is set to 30%:

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

Related Commands

Command	Description
crypto ikev2 limit max-sa	Limits the number of IKEv2 connections on the ASA,
crypto ikev2 limit max-in-negotiation-sa	Limits the number of IKEv2 in-negotiation (open) SAs on the ASA.
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 ikev2 enable

To enable ISAKMP IKEv2 negotiation on the interface on which the IPsec peer communicates with the ASA, use the **crypto ikev2 enable** command in global configuration mode. To disable ISAKMP IKEv2 on the interface, use the **no** form of this command.

crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]
no crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP IKEv2 negotiation.
client-services	Enables client services for IKEv2 connections on the interface. The Client Services Server provides HTTPS (SSL) access to allow the Secure Client Downloader to receive enhanced Secure Client features including software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy. If you disable client services, the Secure Client still establishes basic IPsec connections with IKEv2. If you do not enable the Client Services Server, users will not be able to download any of these files that the Secure Client might need. **Note** You can use the same port that you use for SSL VPN running on the same device. Even if you have an SSL VPN configured, you must select this option to enable file downloads over SSL for IPsec-IKEv2 clients.
port port	Specifies a port to enable client services for IKEv2 connections. The range is 1-65535. The default is port 443.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

Using this command alone will not enable client services. This command requires SSL functionality.

Examples

The following example, entered in global configuration mode, shows how to enable IKEv2 on the outside interface:

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

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 ikev2 fragmentation

To configure fragmentation settings for IKEv2, use the **crypto ikev2 fragmentation** command in global configuration mode.

[**no**] **crypto ikev2 fragmentation** [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]
no crypto ikev2 fragmentation [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

Syntax Description

mtu-size	The MTU size, 68-1500. The MTU value used should include the IPv4/IPv6 header + UDP header size. If you specify a value, the same value is used for both IPv4 and IPv6.
preferred-method	The preferred fragmentation method: Standard RFC-7383 based method (**ietf**) or Cisco Proprietary method (**cisco**).

Command Default

By default both the IKEv2 Fragmentation methods are enabled, the MTU is 576 for IPv4 or 1280 for IPv6, and the IETF method is preferred:

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Use this command to:

- Set the MTU used to determine whether the IKE packets need fragmentation, packets exceeding this value will be fragmented.
- Change the preferred fragmentation method.
- Disable IKE fragmentation all together.

IETF RFC-7383 standard based IKEv2 fragmentation method will be used when both peers specify support and preference during negotiation. Using this method, encryption is done after fragmentation, providing individual protection for each IKEv2 Fragment message.

Cisco proprietary fragmentation will be used if it is the only method provided by a peer, such as the Secure Client, or if both peers specify support and preference during negotiation. Using this method fragmentation is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received.

Examples

The following example, entered in global configuration mode, shows how to enable IKEv2 on the outside interface:

Change the MTU value to 600:

```
ciscoasa(config)# crypto ikev2 fragmentation mtu 600
```

To change the preferred method of fragmentation to Cisco:

```
ciscoasa(config)# crypto ikev2 fragmentation preferred-method cisco
```

Related Commands

Command	Description
show crypto ikev2 sa detail	Shows the MTU.
show running-config all crypto ikev2	Displays the configuration.

crypto ikev2 limit max-in-negotiation-sa

To limit the number of IKEv2 in-negotiation (open) SAs on the ASA, use the **crypto ikev2 limit max-in-negotiation-sa** command in global configuration mode. To disable limits on the number of open SAs, use the **no** form of this command:

crypto ikev2 limit max-in-negotiation-sa { *percentage* | **value** *limit*
no crypto ikev2 limit max-in-negotiation-sa *value*

Syntax Description

percentage	The threshold percentage of the number of SAs that are allowed to be in negotiation. The range is 1 to 100%. The default is 100%.
value *limit*	The maximum number of SAs that are allowed to be in negotiation. The possible range differs by device; use ? to see the range allowed for your device.

Command Default

The default is disabled. There is no limit to the number of open SAs.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.15(1)	Support was added to configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity, rather than only a percentage.

Usage Guidelines

The **crypto ikev2 limit-max-in-negotiation-sa** command limits the maximum number of SAs that can be in negotiation at any time. Once the limit is reached, additional connections are denied. If used in conjunction with the crypto ikev2 cookie-challenge command, configure the cookie-challenge threshold lower than this limit for an effective cross-check.

Unlike the crypto ikev2 cookie-challenge command which challenges incoming connections with a cookie, the **crypto kev2 limit max in-negotiation-sa** command stops further connections from negotiating to protect current connections and prevent memory and/or CPU attacks that the cookie-challenge feature may be unable to thwart.

Examples

The following example limits the number of IKEv2 connections that are in negotiation to 70 percent of the maximum allowable IKEv2 connections:

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

Related Commands

Command	Description
crypto ikev2 limit max-sa	Limits the number of IKEv2 connections on the ASA,
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
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 ikev2 limit max-sa

To limit the number of IKEv2 connections on the ASA, use the **crypto ikev2 limit max-sa** command in global configuration mode. To disable the limit on the number of connections, use the **no** form of this command:

crypto ikev2 limit max-sa *number*
no crypto ikev2 limit max-sa *number*

Syntax Description

number	The number of IKEv2 connections allowed on the ASA. After reaching the limit, additional connections are denied. The range is 1 to 10000.

Command Default

The default is disabled. The ASA does not limit the number of IKEv2 connections. The maximum number of allowed IKEv2 connections equals the maximum number of connections specified by the license.

Usage Guidelines

The **crypto ikev2 limit max-sa** command limits the maximum number of SAs on the ASA.

If used in conjunction with the crypto ikev2 cookie-challenge command, configure the cookie-challenge threshold lower than this limit for an effective cross-check.

Command Modes

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

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

Command History

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

Examples

The following example limits the number of IKEv2 connections to 5000:

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.

Command	Description
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 ikev2 limit queue sa_init

To limit the number of security association (SA) initial packets to be processed per second in IKEv2 connections on the ASA, use the **crypto ikev2 limit queue sa_init** command in global configuration mode. To disable the limit on the number of SA initial packets, use the **no** form of this command:

crypto ikev2 limit queue sa_init *number*
no crypto ikev2 limit queue sa_init

Syntax Description

number	The maxim number of IKEv2 SA INIT packets allowed on the ASA. After reaching the limit, more connections are denied. By default, the SA_INIT queue limit is the default platform SA limit.

Command Default

By default, the SA_INIT queue limit is the default platform SA limit. You can use the **crypto ikev2 limit queue sa_init** command to change the default limit.

Usage Guidelines

The **crypto ikev2 limit queue sa_init**command limits the maximum number of SA INIT packets on the ASA.

When many remote access VPN sessions are established at same time or instability (link-down), CPU-hog can happen and most of the SA-INIT packets can stay in queue way past their allowed time. You can use this command to limit the number of SA-INIT packets that can be present in the queue at any time, rejecting the remaining packets.

Command Modes

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

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

Command History

Release	Modification
9.16(1)	This command was added.

Examples

The following example limits the number of IKEv2 SA_INIT packets to 5000:

```
ciscoasa(config)# crypto ikev2 limit queue sa_init 500
```

Related Commands

Command	Description
show crypto ikev2 stats	Display the IKEv2 runtime statistics.

Command	Description
show crypto ikev2 sa	Displays the IKEv2 runtime SA database.

crypto ikev2 notify

To allow an administrator to enable sending an IKE notification to the peer when an inbound packet is received on an SA that does not match the traffic selectors for that SA, use the **crypto ikev2 notify** command. To disable sending this notification, use the no form of the command:

crypto ikev2 notify invalid-selectors
[**no**] **crypto ikev2 notify invalid-selectors**

Syntax Description

invalid-selectors	Notify the peer if a packet is received on an SA but does not match the traffic selectors.
notify	Enable/disable IKEv2 notification to be sent to the peer.

Command Default

Sending the notification is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.

Examples

```
100/act(config) # crypto ikev2 ?
configure mode commands/options:
 cookie-challenge     Enable and configure IKEv2 cookie challenges based on half-open SAs
 enable     Enable IKEv2 on the specified interface
 limit     Enable limits on IKEv2 SAs
 policy     Set IKEv2 policy suite
 redirect     Set IKEv2 redirect
 remote-access     Configure IKEv2 for Remote Access
 notify     Enable/Disable IKEv2 notifications to be sent to the peer
100/act(config)# crypto ikev2 notify ?
configure mode commands/options:
 invalid-selectors     Notify the peer if a packet is received on an SA but does not match
 the traffic selectors
```

crypto ikev2 policy

To create an IKEv2 security association (SA) for IPsec connections, use the crypto ikev2 policy command in global configuration mode. To remove the policy, use the **no** form of this command:

crypto ikev2 policy *policy_index group* < *number* >
no crypto ikev2 policy *policy_index group* < *number* >

Syntax Description

group <number>	Specifies the Diffie-Hellman group(s) for this policy index as 14, 15, 16, 19, 20, 21, or 31.
policy index	Accesses the IKEv2 policy configuration mode and specifies the priority of the policy entry.

Command Default

No default behavior or values.

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, you enter IKEv2 policy configuration mode, in which you specify additional IKEv2 SA settings. You can use additional commands to set the SA encryption algorithm, DH group, integrity algorithm, lifetime, and hash algorithm.

Command Modes

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

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

Command History

Release	Modification
9.20(1)	Support is added for configuring additional key exchange to secure the IPsec communication from quantum computer attacks.
9.16(1)	Support is added for DH group 31.

Release	Modification
9.15(1)	The following integrity, encryption, and ciphers are removed from this release in strong crypto license mode: • md5 • 3des encryption • des encryption • null encryption (removed from both strong and weak crypto license modes) Support is removed for DH groups 1, 2, 5, and 24.
9.13(1)	The following integrity, encryption, and ciphers are deprecated and will be removed in the future release: • md5 • 3des encryption • des encryption • null encryption Added Diffie-Hellman groups 15 and 16 and deprecated DH groups 1, 2, 5, and 24.
9.0(1)	Support for multiple context mode was added. Added policy index option.
8.4(1)	This command was added.

Examples

The following example creates the priority 1 IKEv2 SA and enters IKEv2 policy configuration mode:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5(DEPRECATED)
ciscoasa(config-ikev2-policy)# integrity sha
ciscoasa(config-ikev2-policy)# prf mad5(DEPRECATED)
ciscoasa(config-ikev2-policy)# prf sha
ciscoasa(config-ikev2-policy)# encryption 3des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption null(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption aes
ciscoasa(config-ikev2-policy)# encryption aes-192
ciscoasa(config-ikev2-policy)# additional-key-exchange 1
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
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.

Command	Description
show running-config crypto isakmp	Displays all the active configuration.
additional-key-exchange	Configures an additional key exchange transform for an IKEv2 policy.
show running-config crypto ikev2	Shows the details of the IKEv2 policy.
show crypto ikev2 sa detail	Shows the details of the IKEv2 SAs.

crypto ikev2 redirect

To specify the IKEv2 phase at which load-balancing redirection from master to cluster member occurs, use the **crypto ikev2 redirect** command in global configuration mode. To remove the command, use the **no** form of this command:

crypto ikev2 redirect { **during-init** | **during-auth** }
no crypto ikev2 redirect { **during-init** | **during-auth** }

Syntax Description

during-auth	Enables load-balancing redirection to a cluster member during the IKEv2 authentication exchange.
during-init	Enables load-balancing redirection to a cluster member during the IKEv2 SA initiated exchange.

Command Default

The default is load-balancing redirection to a cluster member, which occurs during the IKEv2 authentication exchange.

Command Modes

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

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

Command History

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

Examples

The following example sets the load-balancing redirection to a cluster member to occur during the IKEv2 initiated exchange:

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.

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

crypto ikev2 remote-access trust-point

To specify a global trustpoint to be referenced and used as the identity certificate trustpoint of the ASA for AnyConnect IKEv2 connections, use the **crypto ikev2 remote-access trust-point** command in tunnel group configuration mode. To remove the command from the configuration, use the no form of the command.

crypto ikev2 remote-access trust-point *name* [*line number*]
no crypto ikev2 remote-access trust-point *name* [*line number*]

Syntax Description

name	The name of the trustpoint, up to 65 characters.
line number	Specifies where in the line number you want the trustpoint inserted. Typically, this option is used to insert a trustpoint at the top without removing and readding the other line. If a line is not specified, the ASA adds the trustpoint at the end of the list.

Command Default

No default behavior or values.

Usage Guidelines

Use the this command to configure a trustpoint for the ASA to authenticate itself to the Secure Client for all IKEv2 connections. Using this command allows the Secure Client to support group selection for the user.

You can configure two trustpoints at the same time: two RSA, two ECDSA, or one of each. The ASA scans the configured trustpoint list and chooses the first one that the client supports. If ECDSA is preferred, you should configure that trustpoint before the RSA trustpoint. If you try to add a trustpoint that already exists, you receive an error.

Note

1. If you use the no form of command without specifying which trustpoint name to remove, all trustpoint configuration is removed.
2. If there are one or more certificates with the same attributes, and one of them has expired, a "Certificate Validation Failure" error occurs. We recommend that you delete the expired certificate using the no form of this command.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was added..

Release	Modification
9.0(1)	Support for multiple context mode and the configuration of two trustpoints were added.

Examples

The following example specifies the trustpoint *cisco_asa_trustpoint* :

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

To configure DF-bit policy for IPsec packets, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

Syntax Description

clear-df	(Optional) Specifies that the outer IP header will have the DF bit cleared and that the ASA may fragment the packet to add the IPsec encapsulation.
copy-df	(Optional) Specifies that the ASA will look in the original packet for the outer DF bit setting.
set-df	(Optional) Specifies that the outer IP header will have the DF bit set; however, the ASA may fragment the packet if the original packet had the DF bit cleared.
interface	Specifies an interface name.

Command Default

This command is disabled by default. If this command is enabled without a specified setting, the ASA uses the **copy-df** setting as the default.

Command Modes

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

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

Command History

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

Usage Guidelines

The DF bit with IPsec tunnels feature lets you specify whether or not the ASA can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet.

Use the **crypto ipsec df-bit** command in global configuration mode to configure the ASA to specify the DF bit in an encapsulated header. This command treats the DF-bit setting of the clear-text packet and either clears, set, or copies it to the outer IPsec header when encryption is applied.

When encapsulating tunnel mode IPsec traffic, use the **clear-df** setting for the DF bit. This setting lets the device send packets larger than the available MTU size. Also, this setting is appropriate if you do not know the available MTU size.

Caution

Packets will get dropped if you set the following conflicting configuration: **crypto ipsec fragmentation after-encryption** (fragment packets) **crypto ipsec df-bit set-df outside** (set the DF bit)

Examples

The following example, entered in global configuration mode, sets the IPsec DF policy to **clear-df**:

```
ciscoasa(config)# crypto
 ipsec df-bit clear-df outside
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.
show crypto ipsec fragmentation	Displays the fragmentation policy for a specified interface.

crypto ipsec fragmentation

To configure the fragmentation policy for IPsec packets, use the **crypto ipsec fragmentation** command in global configuration mode.

crypto ipsec fragmentation { **after-encryption** | **before-encryption** } *interface*

Syntax Description

after-encryption	Specifies the ASA to fragment IPsec packets that are close to the maximum MTU size after encryption (disables prefragmentation).
before-encryption	Specifies the ASA to fragment IPsec packets that are close to the maximum MTU size before encryption (enables prefragmentation).
interface	Specifies an interface name.

Command Default

Before-encryption is enabled by default.

Command Modes

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

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

Command History

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

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting ASA, and it is encapsulated with IPsec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting device reassemble in the process path. Prefragmentation for IPsec VPNs increases the performance of the device when decrypting by letting it operate in the high performance CEF path instead of the process path.

Prefragmentation for IPsec VPNs lets an encrypting device predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPsec SA. If the device predetermines that the packet will exceed the MTU of the output interface, the device fragments the packet before encrypting it. This avoids process level reassembly before decryption and helps improve decryption performance and overall IPsec traffic throughput.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Note

Layer 2 Tunneling Protocol (L2TP) over IPsec supports only post fragmentation. Changes to the fragmentation policy **crypto ipsec fragmentation before-encryption/after-encryption <interface>** does not apply to L2TP.

Caution

Packets will get dropped if you set the following conflicting configuration: **crypto ipsec fragmentation after-encryption** (fragment packets) **crypto ipsec df-bit set-df outside** (set the DF bit)

Examples

The following example, entered in global configuration mode, enables prefragmentation for IPsec packets on the inside interface only:

```
ciscoasa(config)# crypto
 ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

The following example, entered in global configuration mode, disables prefragmentation for IPsec packets on the interface:

```
ciscoasa(config)# crypto
 ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPsec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

crypto ipsec ikev1 transform-set

To create or remove an IKEv1 transform set, use the **crypto ipsec ikev1 transform-set** command in global configuration mode. To remove a transform set, use the **no** form of this command.

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]
no crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

Syntax Description

authentication	(Optional) Specify one of the following authentication methods to ensure the integrity of IPsec data flows: **esp-md5-hmac** to use the MD5/HMAC-128 as the hash algorithm. **esp-sha-hmac** to use the SHA/HMAC-160 as the hash algorithm. **esp-none** to not use HMAC authentication.
encryption	Specify one of the following encryption methods to protect IPsec data flows: **esp-aes** to use AES with a 128-bit key. **esp-aes-192** to use AES with a 192-bit key. **esp-aes-256** to use AES with a 256-bit key. **esp-des** to use 56-bit DES-CBC. **esp-3des** to use triple DES algorithm. **esp-null** to not use encryption.
transform-set-name	Name of the transform set being created or modified. To view the transform sets already present in the configuration, enter the **show running-config ipsec** command.

Command Default

The default authentication setting is esp-none (no authentication).

Command Modes

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

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

Command History

Release	Modification
7.0	This command was added.
7.2(1)	This section was rewritten.

Release	Modification
8.4(1)	The ikev1 keyword was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	This following options are deprecated and will be removed in the later release: • esp-md5-hmac • esp-3des • esp-des
9.15(1)	This following options are removed from this release: • esp-md5-hmac • esp-3des • esp-des

Usage Guidelines

This command identifies the IPsec encryption and hash algorithms to be used by the transform set.

Following the configuration of a transform set, you assign it to a crypto map. You can assign up to six transform sets to a crypto map. When the peer attempts to establish an IPsec session, the ASA evaluates the peer using the access list of each crypto map until it finds a match. The ASA then evaluates all of the protocols, algorithms, and other settings negotiated by the peer using those in the transform sets assigned to the crypto map until it finds a match. If the ASA matches the peer's IPsec negotiations to the settings in a transform set, it applies them to the protected traffic as part of its IPsec security association. The ASA terminates the IPsec session if it fails to match the peer to an access list and find an exact match of the security settings of the peer to those in a transform set assigned to the crypto map.

You can specify either the encryption or the authentication first. You can specify the encryption without specifying the authentication. If you specify the authentication in a transform set that you are creating, you must specify the encryption with it. If you specify only the authentication in a transform set that you are modifying, the transform set retains its current encryption setting.

If you are using AES encryption, we recommend that you use the **isakmp policy priority group 5** command, also in in global configuration mode, to assign Diffie-Hellman group 5 to accommodate the large key sizes provided by AES.

Tip When you apply transform sets to a crypto map or a dynamic crypto map and view the transform sets assigned to it, you will find it helpful if the names of the transform sets reflect their configuration. For example, the name "3des-md5" in the first example below shows the encryption and authentication used in the transform set. The values that follow the name are the actual encryption and authentication settings assigned to the transform set.

Examples

The following commands show all possible encryption and authentication options, excluding those that specify no encryption and no authentication:

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
```

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-des (DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-3des(DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-md5-hmac (DEPRECATED)
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev1 transform-set mode transport

To specify the transport mode for IPsec IKEv1 connections, use the **crypto ipsec ikev1 transform-set** mode transport command in global configuration mode. To remove the command, use the **no** form of this command:

crypto ipsec ikev1 transform-set *transform-set-name* **mode** { **transport** }
no crypto ipsec ikev1 transform-set *transform-set-name* **mode** { **transport** }

Syntax Description

transform-set-name	Name of the transform set being modified. To view the transform sets already present in the configuration, enter the **show running-config ipsec** command.

Command Default

The default setting for the transport mode is disabled. IPsec uses the networked tunnel mode.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was rewritten.
8.4(1)	The ikev1 keyword was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **crypto ipsec ikev1 transform-set** mode transport command to specify the host-to-host transport mode for IPsec, instead of the default networked tunnel mode.

Examples

The following commands show all possible encryption and authentication options, excluding those that specify no encryption and no authentication:

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.

Command	Description
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev2 ipsec-proposal

To create an IKEv2 proposal, use the **crypto ipsec ikev2 ipsec-proposal** command in global configuration mode.To remove the proposal, use the **no** form of this command.

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*
no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

Syntax Description

proposal name	Accesses the IPsec ESP proposal sub-mode.
proposal tag	The name of the IKEv2 IPsec proposal, a string from 1 to 64 characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	The following IKEv2/IPsec proposal integrity and encryption ciphers are deprecated and will be removed in the later release: • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

Release	Modification
9.15(1)	The following IKEv2/IPsec proposal integrity and encryption ciphers are removed from this release: • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

Usage Guidelines

This command creates a proposal and enters ipsec proposal configuration mode, in which you can specify multiple encryption and integrity types for the proposal.

Examples

The following example creates the IPsec proposal named secure, and enters IPsec proposal configuration mode:

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)# protocol esp encryption ?
```

ciscoasa(config-ipsec-proposal)# **protocol esp aes**ciscoasa(config-ipsec-proposal)# **protocol esp 3des**(**DEPRECATED**

```
ciscoasa(config-ipsec-proposal)# protocol esp integrity ?
ciscoasa(config-ipsec-proposal)# protocol esp sha
ciscoasa(config-ipsec-proposal)# protocol esp md5
(DEPRECATED
)
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev2 sa-strength-enforcement

Ensures that the strength of the IKEv2 encryption cipher is higher than the strength of its child IPsec SA's encryption ciphers. To disable this feature, use the **no** form of this command.

crypto ipsec ikev2 sa-strength-enforcement
no crypto ipsec ikev2 sa-strength-enforcement

Command Default

Enforcement is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

Security is not increased when a child SA has a stronger encryption cipher than its parent IKEv2 connection. It is good security practice to configure the IPsec so this does not happen. The strength enforcement setting only affects the encryption cipher; it does not alter the integrity or key exchange algorithms. The IKEv2 system compares the relative strength of each child SA's selected encryption cipher as follows:

When enabled, verifies that the configured encryption cipher for the child SA is not stronger than the parent IKEv2 encryption cipher. If found, then the child SA will be updated to use the parent cipher. If no compatible cipher is found, then the child SA negotiation is be aborted. The syslog and debug message logs these actions.

The supported encryption ciphers are listed below in order of strength, from highest to lowest. Ciphers on the same line have equivalent strength for purposes of this check.

- AES-GCM-256, AES-CBC-256
- AES-GCM-192, AES-CBC, 192
- AES-GCM-128, AES-CBC-128
- 3DES
- DES
- AES-GMAC (any size), NULL

Related Commands

Command	Description
show running-config ipsec	Displays crypto ipsec ikev2 sa-strength-enforcement when enabled.

crypto ipsec inner-routing-lookup

To enable IPsec inner routing lookup, use the **crypto ipsec inner-routing-lookup** command in configuration mode. To disable IPsec inner routing lookup, use the **no** form of this command.

crypto ipsec inner-routing-lookup
no crypto ipsec inner-routing-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IPsec inner-routing-lookup is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

By default, per-packet adjacency lookups are done for the outer ESP packets, but lookups are not done for packets sent through the IPsec tunnel.

In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination.

To prevent this, enable per-packet routing lookups for the IPsec inner packets. To avoid any performance impact from these lookups, this feature is disabled by default. Enable it only when necessary.

When this command is enabled, packets are punted to CPU for a route lookup before encryption is done. If too much traffic is sent to CPU, it will be discarded and the ASP drop counter will increase (punt-no-mem). This command is disabled by default. To avoid any potential impact on traffic, enable the command only when required.

This command, when configured, is only applicable for non-VTI based tunnels.

Examples

The following example configures and shows that inner-routing-lookup is enabled.:

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec

crypto ipsec inner-routing-lookup
```

Related Commands

Command	Description
show run crypto ipsec	Show the running crypto ipsec configuration.

crypto ipsec profile

To create a new IPsec profile, use the **crypto ipsec profile** command in the Global Configuration mode. Use the no form of the command to delete the IPsec profile.

crypto ipsec profile *name set pfs < group# >*
no crypto ipsec profile *name set pfs < group# >*

Syntax Description

name	Specifies a name for a new IPsec profile. The name can contain less than 65 characters.
group #	Specifies which Diffie-Hellman key exchange group to use.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	No	• Yes	No	—

Command History

Release	Modification
9.7(1)	We introduced this command and its submodes.

Examples

In the following example, VTIipsec is the new IPsec profile:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
```

Related Commands

Command	Description
responder-only	Sets the VTI tunnel interface to responder only mode.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.

Command	Description
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

crypto ipsec security-association lifetime

To configure global lifetime values, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a global lifetime value to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }
no crypto ipsec security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }

Syntax Description

kilobytes {*number* | **unlimited**}	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.
unlimited	Does not send Kilobytes in quick mode 1 packet when ASA is the initiator of the tunnel.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.1(2)	The **unlimited** argument was added.

Usage Guidelines

The **crypto ipsec security-association lifetime** command changes global lifetime values used when negotiating IPsec security associations.

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

Assuming that the particular crypto map entry has no lifetime values configured, when the ASA requests new security associations during negotiation, it specifies its global lifetime value in the request to the peer; it uses this value 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 value as the lifetime of the new security associations.

For site-to-site VPN connections, there are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.

The ASA lets the user change crypto map, dynamic map, and IPsec settings on the fly. If this is changed, the ASA brings down only the connections affected by the change. If the user changes 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 global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed or after the amount of traffic in kilobytes has passed.

Examples

The following example specifies a global timed lifetime for security associations:

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPsec configuration (that is, global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec security-association pmtu-aging

To enable path maximum transfer unit (PMTU) aging, use the **crypto ipsec security-association pmtu-aging** command in global configuration mode. To disable PMTU aging, use the no form of the command:

crypto ipsec security-association pmtu-aging *reset-interval*
no crypto ipsec security-association pmtu-aging *reset-interval*

Syntax Description

reset-interval	Sets the interval at which the PMTU value is reset.

Command Default

This feature is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The reset interval is specified in seconds.

crypto ipsec security-association replay

To configure the IPsec antireplay window size, use the **crypto ipsec security-association replay** command in global configuration mode. To reset the window size to the default value, use the **no** form of this command.

crypto ipsec security-association replay { **window-size** *n* | **disable** }
no crypto ipsec security-association replay { **window-size** *n* | **disable** }

Syntax Description

n	Sets the window size. Values can be 64, 128, 256, 512, or 1024. The default is 64.
disable	Disables antireplay checking.

Command Default

The default window size is 64.

Command Modes

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

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

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Cisco IPsec authentication provides antireplay protection from an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association antireplay is a security service in which the receiver can reject old or duplicate packets to protect itself from replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, QoS gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor; this event can generate warning syslog messages that are false alarms. The **crypto ipsec security-association replay** command lets you expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the antireplay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future antireplay problems.

Examples

The following example specifies the antireplay window size for security associations:

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPsec configuration (that is, global lifetimes and transform sets).
shape	Enables traffic shaping.
priority	Enables priority queuing.
show running-config crypto map	Displays all configuration for all the crypto maps.