CHAPTER 9

crypto ca authenticate through customization Commands

crypto ca authenticate

To install and authenticate the CA certificates associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode. To remove the CA certificate, use the **no** form of this command.

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

no crypto ca authenticate *trustpoint*

Syntax Description

fingerprint	Specifies a hash value consisting of alphanumeric characters the security appliance uses to authenticate the CA certificate. If a fingerprint is provided, the security appliance 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 security appliance displays the computed fingerprint and asks whether to accept the certificate.
hexvalue	Identifies he hexadecimal value of the fingerprint.
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 security appliance accepts the certificate without question.
trustpoint	Specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters.

Defaults

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	**Modification**
7.0	This command was introduced

Usage Guidelines

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

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

Examples

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

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

In the next example, the trustpoint tp9 is configured for terminal-based (manual) enrollment. In this case thesecurity appliance prompts the administrator to paste the CA certificate to the terminal. After displaying the fingerprint of the certificate, the security appliance prompts the administrator to confirm that the certificate should be retained.

```
hostname(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
hostname(config)#
```

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. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode 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. To return to global configuration mode, use the **exit** command.

crypto ca certificate chain *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint for configuring the certificate chain.

Defaults

This command has no default values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters CA certificate chain submode for trustpoint central:

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.

crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca configuration map** command in global configuration mode. Executing this command places you in ca-certificate-map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. 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 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.

Defaults

No default behavior or values for sequence-number.

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

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.
7.2	Added keyword *map-name*.

Usage Guidelines

Issuing this command places the security appliance in CA certificate map configuration mode where the user can configure rules based on the certificate's issuer and subject distinguished names (DNs). 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. For a list of certificate fields, see Related Commands.

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:

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

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(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. Maximum number of characters is 128.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

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:

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

Related Commands

Command	Description
crl configure	Enters crl configuration mode.

crypto ca enroll

To start the enrollment process with the CA, use the **crypto ca enroll** command in global configuration mode. For this command to execute successfully, the trustpoint must have been configured correctly.

crypto ca enroll *trustpoint* [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses all prompts. Enrollment options that might have been prompted for must be pre-configured in the trustpoint. This option is for use in scripts, ASDM, or other such non-interactive needs.
trustpoint	Specifies the name of the trustpoint to enroll with. Maximum number of characters is 128.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When the trustpoint is configured for SCEP enrollment, the security appliance displays a CLI prompt immediately and displays status messages to the console asynchronously. When the trustpoint is configured for manual enrollment, the security appliance writes a base-64-encoded PKCS10 certification request to the console and then displays the CLI prompt.

This command generates interactive prompts that vary depending on the configured state of the referenced trustpoint.

Examples

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

```
hostname(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.

hostname(config)#
```

The next command shows manual enrollment of a CA certificate.

```
hostname(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
hostname(config)#
```

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. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca export

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

crypto ca export *trustpoint* **identify-certificate**

Syntax Description

identify-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. Maximum number of characters for a trustpoint name is 128.

Defaults

This command has no default values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.
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 security device exports the certificates and keys associated with a trust point in base64-encoded PKCS12 format. This feature can be used to move certificates and keys between security devices.

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

Examples

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

```
hostname (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-----
hostname (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. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the 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. The security appliance prompts you to paste the text to the terminal in base 64 format.

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

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

Syntax Description

trustpoint	Specifies the trustpoint with which to associate the import action. Maximum number of characters 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.
certificate	Tells the security appliance to import a certificate from the CA represented by the trustpoint.
pkcs12	Tells the security appliance to import a certificate and key pair for a trustpoint, using PKCS12 format.
passphrase	Specifies the passphrase used to decrypt the PKCS12 data.
nointeractive	(Optional) Imports a certificate using nointeractive mode. This suppresses all prompts. This option for use in scripts, ASDM, or other such non-interactive needs.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

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

```
hostname (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
hostname (config)#
```

The following example manually imports PKCS12 data to trustpoint central:

```
hostname (config)# crypto ca import central pkcs12

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
hostname (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 trustpoint submode for the indicated trustpoint.

crypto ca server

To set up and manage a local CA server on the security appliance, use the **crypto ca server** command in global configuration mode to enter config-ca-server configuration mode and access the CA configuration commands. To delete the configured local CA server from the security appliance, use the **no** form of this command.

crypto ca server

no crypto ca server

Defaults

A certificate authority server is not enabled on the security appliance.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

There can only be one local CA on a security appliance.

The **crypto ca server** command configures the CA server but does not enable it. Use the **no** version of the **shutdown** command in config-ca-server 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.

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

Examples

The following example uses the command to enter config-ca-server configuration mode and then uses the question-mark to list the local CA server commands available in that mode:

```
hostname(config)# crypto ca server
hostname(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 uses the **no** form of the **crypto ca server** command in config-ca-server mode to delete the configured and enabled CA server from the security appliance:

```
hostname(config-ca-server)#no crypto ca server

Certificate server 'remove server' event has been queued for processing.
hostname(config)#
```

Related Commands

Command	Description
debug crypto ca server	Shows debug 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 keywords or arguments.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This seldom-used command is employed to recover a lost CRL. Normally, the CRL is reissued automatically upon 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:

```
hostname(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.

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

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point to be include in the certificates issued by the CA.
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows the user to configure and manage the local CA.

Command	Description
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 certificate to be revoked. Enter the serial number in hexadecimal format.

Defaults

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You revoke a specific certificate that has been issued by the local CA on a security appliance by entering the **crypto ca server revoke** command on that security appliance. 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 hex 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:

```
hostname(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.

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

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server unrevoke	Unrevokes a previously 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 previously 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 certificate to be unrevoked. Enter the serial number in hexadecimal format.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You unrevoke a previously revoked certificate issued by the local CA on a security appliance 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 automatically after the specified certificate is unrevoked.

Examples

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

```
hostname(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been
issued.
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI 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 add *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 a comma, enclose the value string with double quotes (for example, 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The *user* argument can be a simple username such as jandoe or an e-mail address such as jandoe@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.

username, 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* field. A missing e-mail address at mailing time generates an error.

The *user* argument, **email**, 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 a 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 jandoe@example.com along with a complete subject-name DN:

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

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

```
hostname(config-ca-server)# crypto ca server user-db allow jondoe
hostname(config-ca-server)
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI 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 the 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 currently 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 to the console.
username	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or e-mail address.

Defaults

No default behavior or values.

.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Note that the OTP is not stored on the security device 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:

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

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

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

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI 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 is e-mailed to all users in the database who have been issued a certificate, whether that certificate is currently valid or not.
all-unenrolled	Specifies that the OTPs is 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 simple username or e-mail address.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

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

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

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

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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 :

```
hostname(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.

hostname(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.

Command	Description
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 simple username or e-mail address.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

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

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

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

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **crypto ca server user-db write** command is used to save new user-based configuration data to the storage specifed 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:

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

Command	Description
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 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 is 128 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Subcommands added to support Online Certificate Status Protocol. These include **match certificate map**, **ocsp disable-nonce**, **ocsp url**, and **revocation-check**.
8.0(2)	Subcommands added 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** subcommand was added to support enrollment of self-signed certificates between trusted enterprises, such as between Phone-Proxy and TLS-Proxy.

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 sub mode control CA-specific configuration parameters which specify how the security appliance obtains the CA certificate, how the security appliance 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 listed alphabetically in this command reference guide:

- **accept-subordinates**— 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 device.
- **client-types**—Specifies the client connection types for which this trustpoint can be sued to validate the certificates associated with a user connection.
- **crl required | optional | nocheck**—Specifies CRL configuration options.
- **crl configure**—Enters CRL configuration mode (see **crl**).
- **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 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 self**—Specifies enrollment that generates a self-signed certificate.
- **enrollment terminal**—Specifies cut and paste enrollment with this trustpoint.
- **enrollment url** *url*—Specifies 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.
- **ignore-ipsec-keyusage**—Deprecated. Suppress key usage checking on IPsec client certificates.
- **ignore-ssl-keyusage**—Deprecated. Suppress key usage checking on SSL client certificates.
- **ip-addr** *ip-address*—During enrollment, asks the CA to include the IP address of the security appliance in the certificate.
- **keypair** *name*—Specifies the key pair whose public key is to be certified.
- **match certificate** *map-name* **override ocsp**—Matches a certificate map to an OCSP 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 checks all certificates associated with this trustpoint for revocation status.
- **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.
- **proxy-ldc-issuer**—An issuer for TLS proxy local dynamic certificates.
- **revocation check**—Specifies the revocation checking method, which include CRL, OCSP, and none.
- **serial-number**—During enrollment, asks the CA to include the security appliance's serial number in the certificate.

- **subject-name** *X.500 name*—During enrollment, asks the CA to include the specified subject DN in the certificate.
- **support-user-cert-validation**—Deprecated. If enabled, the configuration settings to validate a remote user certificate can be taken from this trustpoint, provided that this trustpoint 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 sub mode.
- **validation-policy**—Deprecated. Specifies trustpoint conditions for validating certificates associated with user connections.

Examples

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

```
hostname(config)# crypto ca trustpoint central
hostname(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 mode. Defines certificate-based ACLs.
crypto ca crl request	Requests a CRL based on configuration parameters of specified trustpoint.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.

crypto dynamic-map match address

To match address of anaccess 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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:

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(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 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 you assign to the crypto dynamic map entry.

Defaults

The default setting is off.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(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.
ip_address	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the **name** command.
hostname	Identifies the peer in the dynamic crypto map entry by hostname, as defined by the **name** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address10.0.0.1:

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(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 specify the dynamic crypto map sets, use the **crypto map dynamic-map set pfs** command in global configuration mode. To remove the specified dynamic-map crypto map set, use the **no** form of this command.

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

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

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.
group1	Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPSec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
set pfs	Configures IPSec to ask for perfect forward secrecy (PFS) when requesting new security associations for this dynamic crypto map entry or configures IPSec to require PFS when receiving requests for new security associations.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to 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.

Usage Guidelines

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 security appliance 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 security appliance 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:

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(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 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.

Defaults

The default value for this command is off.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following command enables RRI for the crypto dynamic-map named mymap:

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

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

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

Specify the names of the transform sets in the **no** form of this command to remove them from a dynamic crypto map entry.

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

Using the **no** form of the command while specifying all or none of the transform sets removes the dynamic crypto map entry.

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set 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 transform-set** command. Each crypto map entry supports up to 11 transform sets.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	Changed maximum number of transform sets in a crypto map entry.

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 security appliance applies a dynamic crypto map to let a peer negotiate a tunnel if its IP address is not already identified in a static 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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-seq-num 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 security appliance accepts any data flow identity the peer proposes.

Caution Do not assign static (default) routes for traffic to be tunneled to a security appliance 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. The "crypto ipsec transform-set (create or remove transform set)" section shows ten transform set example commands.

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

Related Commands

Command	Description
crypto ipsec transform-set	Configures a 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 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 security appliance may fragment the packet to add the IPSec encapsulation.
copy-df	(Optional) Specifies that the security appliance 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 security appliance may fragment the packet if the original packet had the DF bit cleared.
interface	Specifies an interface name.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Use the **crypto ipsec df-bit** command in global configuration mode to configure the security appliance to specify the DF bit in an encapsulated header.

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.

Examples

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

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(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 security appliance to fragment IPSec packets that are close to the maximum MTU size after encryption (disables pre-fragmentation).
before-encryption	Specifies the security appliance to fragment IPSec packets that are close to the maximum MTU size before encryption (enables pre-fragmentation).
interface	Specifies an interface name.

Defaults

This feature is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting security appliance, 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. Pre-fragmentation 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.

Pre-fragmentation 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.

Examples

The following example, entered in global configuration mode, enables pre-fragmentation for IPSec packets globally on the device:

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

The following example, entered in global configuration mode, disables pre-fragmentation for IPSec packets on the interface:

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
hostname(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 security-association lifetime

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

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

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

Syntax Description

kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes.The default is 4,608,000 kilobytes.
seconds	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).
token	Indicates a token-based server for user authentication is used.

Defaults

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

Command Modes

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

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

Command History

Release	**Modification**
Preexisting	This command was preexisting.

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

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached.

The security appliance lets the user change crypto map, dynamic map, and ipsec settings on the fly. If this is changed, the security appliance 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:

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

Related Commands

Command	Description
clear configure crypto map	Clears all IPSec configuration (i.e. global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec security-association replay

To configure the IPSec anti-replay 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 anti-replay checking.

Defaults

The default window size is 64.

Command Modes

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

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

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against 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 anti-replay 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 anti-replay problems.

Examples

The following example specifies the anti-replay window size for security associations:

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

Related Commands

Command	Description
clear configure crypto map	Clears all IPSec configuration (i.e. global lifetimes and transform sets).
shape	Enables traffic shaping.
priority	Enables priority queueing.
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec transform-set (create or remove transform set)

To create or remove a transform set, use the **crypto ipsec transform-set** command in global configuration mode. With **crypto ipsec transform-set** command, the user can identify the IPSec encryption and hash algorithms to be used by the transform set. Tto remove a transform set, use the **no** form of this command.

crypto ipsec transform-set *transform-set-name encryption* [*authentication*]

no crypto ipsec 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.

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

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 security appliance evaluates the peer against the access list of each crypto map until it finds a match. The security appliance then evaluates all of the protocols, algorithms, and other settings negotiated by the peer against those in the transform sets assigned to the crypto map until it finds a match. If the security appliance 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 security appliance 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 you are creating, you must specify the encryption with it. If you specify only the authentication in a transform set 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:

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

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 isakmp am-disable

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

crypto isakmp am-disable

no crypto isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp am-disable** command was introduced.
7.2.(1)	The **crypto isakmp am-disable** command replaces the **isakmp am-disable** command**.**

Examples

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

```
hostname(config)# crypto isakmp am-disable
```

Related Commands

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

crypto isakmp disconnect-notify

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

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp disconnect-notify** command was introduced.
7.2.(1)	The **crypto isakmp disconnect-notify** command replaces the **isakmp disconnect-notify** command**.**

Examples

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

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

Related Commands

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

crypto isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance, use the **crypto isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

crypto isakmp enable *interface-name*

no crypto isakmp enable *interface-name*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This **isakmp enable** command was preexisting.
7.2(1)	The **crypto isakmp enable** command replaces the **isakmp enable** command.

Examples

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

```
hostname(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.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp identity

To set the Phase 2 ID to be sent to the peer, use the **crypto isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
Preexisting	The **isakmp identity** command was preexisting.
7.2(1)	The **crypto isakmp identity** command replaces the **isakmp identity** command.

Examples

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

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

Related Commands

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

crypto isakmp ipsec-over-tcp

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

crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

no crypto isakmp 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 1-65535. The default port number is 10000.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp ipsec-over-tcp** command was introduced.
7.2.(1)	The **crypto isakmp ipsec-over-tcp** command replaces the **isakmp ipsec-over-tcp** command**.**

Examples

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

```
hostname(config)# crypto isakmp ipsec-over-tcp port 45
hostname(config)#
```

Related Commands

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

crypto isakmp nat-traversal

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

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

Syntax Description

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

Defaults

By default, NAT traversal is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp nat-traversal** command was preexisting.
7.2.(1)	The **crypto isakmp nat-traversal** command replaces the **isakmp nat-traversal** command**.**
8.0(2)	NAT traversal is now enabled by default.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To remove the ISAKMP authentication method, use the related **clear configure** command.

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

crypto isakmp policy encryption

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

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

Examples

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

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

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

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

Related Commands

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

crypto isakmp policy group

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

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

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

Syntax Description

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

Defaults

The default group policy is group 2.

Command Modes

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

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

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

crypto isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPSec security associations. The peers negotiate new security associations before current security associations expire.

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

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

Examples

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

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

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

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

Related Commands

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

crypto isakmp reload-wait

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

crypto isakmp reload-wait

no crypto isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **isakmp reload-wait** command was introduced.
7.2.(1)	The **crypto isakmp reload-wait** command replaces the **isakmp reload-wait** command**.**

Examples

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

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

Related Commands

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

crypto key generate rsa

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

crypto key generate rsa [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

Syntax Description

general-keys	Generates a single pair of general purpose keys. This is the default key-pair type.
label *key-pair-label*	Specifies the name to be associated with the key pair(s). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the security appliance displays an warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>.
modulus *size*	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.
usage-keys	Generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.

Defaults

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

Command Modes

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

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

Command History

Release	**Modification**
7.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Related Commands

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

crypto key zeroize

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

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

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

Related Commands

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

crypto map interface

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

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

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

Note The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance 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.

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

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

Examples

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

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

The following example shows the minimum required crypto map configuration:

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

Related Commands

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

crypto map ipsec-isakmp dynamic

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

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified to remove the **ipsec-manual** keyword.

Usage Guidelines

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

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

IPSec dynamic crypto maps identify the following:

- The traffic to protect
- IPSec peer(s) with which to establish a security association
- Transform sets to use with the protected traffic

- How to use or manage keys and security associations

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

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

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

Examples

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

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

Related Commands

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

crypto map match address

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

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

The security appliance 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 protections.

When the security appliance matches a packet to a deny statement, it skips the evaluation of the packet against the remaining ACEs in the crypto map, and resumes evaluation of the packet against the ACEs in the next crypto map in sequence. *Cascading ACLs* involves the use of deny ACEs to bypass evaluation of the remaining ACEs in an ACL, and the resumption of evaluation of traffic against the ACL assigned to the next crypto map in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security.

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

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

Related Commands

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

crypto map set connection-type

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

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

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

Syntax Description

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

Defaults

The default setting is bidirectional.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

This feature works only between the following platforms:

- Two Cisco ASA 5500 series security appliances

- A Cisco ASA 5500 series security appliance and a Cisco VPN 3000 concentrator
- A Cisco ASA 5500 series security appliance and a security appliance running Cisco PIX security appliance software v7.0, or higher

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

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

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

Table 9-1 lists all supported configurations. Other combinations may result in unpredictable routing issues.

Table 9-1 Supported Backup LAN-to-LAN Connection Types

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

Examples

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

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

Related Commands

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

crypto map set inheritance

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

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

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

Syntax Description

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

Defaults

Default value is **rule**.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

crypto map set nat-t-disable

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

crypto map set peer

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

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

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

Syntax Description

hostname	Specifies a peer by its host name as defined by the security appliance **name** command.
ip_address	Specifies a peer by its IP address.
map-name	Specifies the name of the crypto map set.
peer	Specifies an IPSec peer in a crypto map entry either by hostname of IP address.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified to allow up to 10 peer addresses.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

crypto map set pfs

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

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

Syntax Description

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

Defaults

By default PFS is not set.

Command Modes

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

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

Command History

Release	Modification
7.0	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.

Usage Guidelines

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.

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

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

For a negotiation to succed PFS has to be set on both ends. If set, the groups have to be an exact match; The security appliance does not accept just any offer of PFS from the peer.

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

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

Examples

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

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

Related Commands

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

crypto map set phase1-mode

To specify the IKE mode for phase 1 when initiating a connection to either main or aggressive, use the **crypto map set phase1 mode** command in global configuration mode. To remove the setting for phase 1 IKE negotiations, use the **no** form of this command. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the security appliance uses group 2.

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

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

Syntax Description

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

Defaults

Default phase one mode is **main**.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

This command works only in initiator mode; not in responder mode.

Examples

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

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

Related Commands

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

crypto map set reverse-route

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

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

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

Syntax Description

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

Defaults

The default setting for this command is off.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

crypto map set security-association lifetime

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

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

Assuming that the particular crypto map entry has lifetime values configured, when the security appliance 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 security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

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

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

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

Examples

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

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

Related Commands

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

crypto map set transform-set

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

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

To specifically remove the names of the transform sets from a crypto map entry, use the **no** form of this commandwith the specified transform set name.

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	Changed maximum number of transform sets in a crypto map entry.

Usage Guidelines

This command is required for all crypto map entries.

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

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

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

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

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

crypto map set trustpoint

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

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	**Modification**
7.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

csc

To enable the adaptive security appliance to send network traffic to the CSC SSM, use the **csc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

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

no csc

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

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

- FTP connections opened to TCP port 21.

- HTTP connections opened to TCP port 80.
- POP3 connections opened to TCP port 110.
- SMTP connections opened to TCP port 25.

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

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

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

FTP Scanning

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

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

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

For more information about FTP inspection or the default inspection configuration, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Examples

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

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

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

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

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

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

hostname(config)# service-policy csc_out_policy interface inside

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

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

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

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

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

Related Commands

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

csd enable

To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in webvpn configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.

csd enable

no csd enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

You can enter the **show webvpn csd** command to determine whether Cisco Secure Desktop is enabled.

The **csd image** *path* command must be in the running configuration before you enter the **csd enable** command.

The **no csd enable** command disables Cisco Secure Desktop in the running configuration. If Cisco Secure Desktop is disabled, you cannot access Cisco Secure Desktop Manager and remote users cannot use Cisco Secure Desktop.

If you transfer or replace the data.xml file, disable and then enable Cisco Secure Desktop to load the file into the running configuration.

Examples

The following example commands shows how to view the status of the Cisco Secure Desktop image and enable it:

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

Related Commands

Command	Description
show webvpn csd	Identifies the version of Cisco Secure Desktop if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd image	Copies the Cisco Secure Desktop image named in the command, from the flash drive specified in the path to the running configuration.

csd image

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

csd image *path*

no csd image [*path*]

Syntax Description

path	Specifies the path and filename of the Cisco Secure Desktop package, up to 255 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Enter the **show webvpn csd** command to determine whether the Cisco Secure Desktop image is enabled before entering this command. The CLI indicates the version of Cisco Secure Desktop image that is currently installed if it is enabled.

Use the **csd image** command to install a new Cisco Secure Desktop image, or upgrade an existing image, after you download it from http://www.cisco.com/cisco/software/navigator.html to your computer, and transfer it to the flash drive. When downloading it, be sure to get the correct file for the security appliance; it is in the form **securedesktop_asa_<*n*>_<*n*>*.pkg**.

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

Note Enter the **write memory** command to save the running configuration to ensure Cisco Secure Desktop is available the next time the security appliance reboots.

Examples

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

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

38600704 bytes available (24281088 bytes used)

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

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

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

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

Related Commands

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

ctl

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

ctl install

no ctl instal

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled by default.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ctl-file (global)

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

ctl-file *ctl_name* **noconfirm**

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

If users have phones that require LSC provisioning, you must also import the CAPF certificate into the ASA from the CUMC when configuring the CTL file instance with the **ctl-file** command. See the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

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

Using the **no** form of the command removes the CTL file and all enrolled trustpoints internally created by Phone Proxy. Additionally, removing the CTL file destroys all certificates received from the related Certificate Authority.

Examples

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

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

Related Commands

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

ctl-file (phone-proxy)

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

ctl-file *ctl_name*

no ctl-file *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL instance.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

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

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

Related Commands

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

ctl-provider

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

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL provider instance.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

customization

To specify the customization to use for a tunnel-group, group, or user, use the **customization** command from the following modes:

In tunnel-group webvpn-attributes configuration mode and webvpn configuration mode (accessible from global configuration mode):

customization *name*

no customization *name*

In webvpn configuration mode (accessible from group-policy attributes configuration mode or username attributes configuration mode):

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

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

Syntax Description

name	Specifies the name of the WebVPN customization to apply.
none	Disables customization for the group or user, and displays the default WebVPN pages.
value *name*	Specifies the name of a customization to apply to the group policy or user.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

Mode-Dependent Command Options

The keywords available with the **customization** command differ depending on the mode you are in. In group-policy attributes > webvpn configuration mode and username attributes > webvpn configuration mode, the additional keywords **none** and **value** appear. The complete syntax from these modes is:

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

None disables customization for the group or user, and prevents the customization from being inherited. For example, if you enter the **customization none** command from username attributes > webvpn mode, the security appliance will not look for the value in the group policy or tunnel group.

name is the name of a customization to apply to the group or user.

To remove the command from the configuration, and cause the value to be inherited, use the **no** form of the command.

Examples

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

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

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

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

Related Commands

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