



# Certificate Enrollment Enhancements

---

## Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This feature module describes the Certificate Enrollment Enhancements feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 5](#)
- [Glossary, page 12](#)

## Feature Overview

The Certificate Enrollment Enhancements feature introduces five new subcommands to the **crypto ca trustpoint** command—**ip-address (ca-trustpoint)**, **password (ca-trustpoint)**, **serial-number (ca-trustpoint)**, **subject-name**, and **usage**. These commands provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. (However, the prompting behavior remains the default if this feature is not enabled.) Thus, users can preload all necessary information into the configuration, allowing each router to obtain its certificate automatically when it is booted.



### Note

Trustpoint certification authorities (CAs) combine and replace the functionality of identity and trusted-root CAs. Thus, the **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands. For more information, refer to the *Trustpoint CLI*, Cisco IOS Release 12.2(8)T feature module.



### Note

For information on certificate automatic enrollment, refer to the *Certificate Autoenrollment*, Cisco IOS Release 12.2(8)T feature module.

## Benefits

The Certificate Enrollment Enhancements feature facilitates the implementation of certificate automatic enrollment.

## Related Documents

- *Certificate Autoenrollment*, Cisco IOS Release 12.2(8)T feature module
- *Trustpoint CLI*, Cisco IOS Release 12.2(9)T feature module
- The chapter “Configuring Certification Authority Interoperability” in *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter “Certification Authority Interoperability Commands” in *Cisco IOS Security Command Reference*, Release 12.2

## Supported Platforms

This feature runs on all platforms that support IP Security (IPSec) and public key infrastructure (PKI).

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1600 series
- Cisco 1600-R series
- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 2400 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

- Cisco ICS 7700
- Cisco CVA120 series
- Cisco MC3810 series
- Cisco uBR7200 series
- Route Processor Module (RPM)

#### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

#### Standards

None

#### MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

#### RFCs

None

## Prerequisites

Before you can configure router certificate fields, you must enable the **crypto ca trustpoint** command, which declares the CA that your router should use and enters ca-trustpoint configuration mode.

## Configuration Tasks

See the following sections for configuration tasks for the Certificate Enrollment Enhancements feature. Each task in the list is identified as either required or optional.

- [Configuring Router Certificate Fields](#) (required)
- [Verifying Enrollment Options](#) (optional)

### Configuring Router Certificate Fields

To preload all necessary information into the configuration for certificate requests, use the following commands in `ca-trustpoint` configuration mode. After these commands are enabled, you will not be prompted for the attributes during enrollment for the trustpoint.

	Command	Purpose
Step 1	Router(ca-trustpoint)# <b>ip-address</b> { <i>ip-address</i>   <i>interface</i> }	Specifies an IP address or an interface (from which the router can get an IP address) that will be included in the certificate request.  If this command is not specified, it will be prompted for during certificate enrollment.
Step 2	Router(ca-trustpoint)# <b>subject-name</b> [ <i>x.500-name</i> ]	Specifies the requested subject name that will be used in the certificate request..  If the <i>x-500-name</i> argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.
Step 3	Router(ca-trustpoint)# <b>serial-number</b> [ <b>none</b> ]	Specifies the router serial number in the certificate request, unless the <b>none</b> keyword is issued.  If this command is not specified, it will be prompted for during certificate enrollment.
Step 4	Router(ca-trustpoint)# <b>usage</b> <i>method1</i> [ <i>method2</i> , [ <i>method3</i> ]]	Specifies the intended use for the certificate. The default is ike.
Step 5	Router(ca-trustpoint)# <b>password</b> <i>string</i>	Specifies the revocation password for the certificate.  If this command is not specified, it will be prompted for during certificate enrollment.

### Verifying Enrollment Options

To verify CA information and autoenrollment options, use any of the following EXEC commands:

Command	Purpose
Router# <b>show crypto ca certificates</b>	Displays information about your certificates, the certificates of the CA, and registration authority (RA) certificates.
Router# <b>show crypto ca timers</b>	Displays the status of the managed timers that are maintained by Cisco IOS for PKI.

# Configuration Examples

This section provides the following configuration example:

- [Autoenrollment Configuration Example](#)

## Autoenrollment Configuration Example

The following example shows how to configure the router to autoenroll with a CA on startup and how to specify all necessary enrollment information in the configuration:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 serial-number none
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
!
crypto ca certificate chain frog
certificate ca 0B
30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
0355040A 130C4369 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit
```

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [ip-address \(ca-trustpoint\)](#)
- [password \(ca-trustpoint\)](#)
- [serial-number \(ca-trustpoint\)](#)
- [subject-name](#)
- [usage](#)

## ip-address (ca-trustpoint)

To specify a dotted IP address or an interface that will be included as “unstructuredAddress” in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

**ip-address** { *ip-address* | *interface* | **none** }

**no ip-address**

### Syntax Description

<i>ip-address</i>	Specifies a dotted IP address that will be included in the certificate request.
<i>interface</i>	Specifies an interface, from which the router can get an IP address, that will be included in the certificate request.
<b>none</b>	Specifies that an IP address is not to be included in the certificate request.

### Defaults

An IP address is not configured. You are prompted for the IP address during certificate enrollment.

### Command Modes

Ca-trustpoint configuration

### Command History

Release	Modification
12.2(8)T	This command was introduced.

### Usage Guidelines

Before you can issue this command, you must enable the **crypto ca | pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command is a subcommand that allows you to specify a certificate enrollment parameter.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you will not be prompted for an IP address during certificate enrollment.

### Examples

The following example shows how to include the IP address of the ethernet-0 interface in the certificate request for the trustpoint “frog”:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
```

The following example shows that an IP address is not to be included in the certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 fqdn none
 ip-address none
```

```
subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

## password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

**password** *string*

**no password**

Syntax Description	
<i>string</i>	Name of the password.

Defaults	
	You are prompted for the password during certificate enrollment.

Command Modes	
	Ca-trustpoint configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines	
	<p>Before you can issue the <b>password</b> command, you must enable the <b>crypto ca trustpoint</b> command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.</p> <p>This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.</p> <p>If this command is enabled, you will not be prompted for a password during certificate enrollment.</p>

Examples	
	<p>The following example shows how to specify the password “revokme” for the certificate request:</p>

```
crypto ca trustpoint frog
enrollment url http://frog.phoobin.com/
subject-name OU=Spiral Dept., O=tiedye.com
ip-address ethernet-0
auto-enroll regenerate
password revokme
```

Related Commands	Command	Description
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

## serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

**serial-number [none]**

**no serial-number**

<b>Syntax Description</b>	<b>none</b>	(Optional) Specifies that a serial number will not be included in the certificate request.
---------------------------	-------------	--

<b>Defaults</b>	Not configured. You will be prompted for the serial number during certificate enrollment.
-----------------	---

<b>Command Modes</b>	Ca-trustpoint configuration
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

**Usage Guidelines** Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

**Examples** The following example shows how to omit a serial number from the “root” certificate request:

```
crypto ca trustpoint root
enrollment url http://10.3.0.7:80
ip-address none
fqdn none
serial-number none
subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
enrollment url http://10.3.0.7:80
serial-number
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# subject-name

To specify the subject name in the certificate request, use the **subject-name** command in `ca-trustpoint` configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

**subject-name** [*x.500-name*]

**no subject-name** *x.500-name*

## Syntax Description

<i>x.500-name</i>	(Optional) Specifies the subject name used in the certificate request.
-------------------	--

## Defaults

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

## Command Modes

Ca-trustpoint configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.

## Usage Guidelines

Before you can issue the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters `ca-trustpoint` configuration mode.

**subject-name** is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

## Examples

The following example shows how to specify the subject name for the “frog” certificate:

```
crypto ca trustpoint frog
  enrollment url http://frog.phoobin.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet-0
  auto-enroll regenerate
  password revokme
```

## Related Commands

Command	Description
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

## usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

```
usage method1 [method2, [method3]]
```

```
no usage method1 [method2, [method3]]
```

### Syntax Description

<i>method1</i> [ <i>method2</i> [ <i>method3</i> ]]	The intended use for the certificate; the available options are ike, ssl-client, and ssl-server.  You must choose at least one method, and you may choose all three methods.
--	--

### Defaults

ike

### Command Modes

Ca-trustpoint configuration

### Command History

Release	Modification
12.2(8)T	This command was introduced.

### Usage Guidelines

Before you can issue the **usage** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

### Examples

The following example shows how to specify the certificate named “frog” for Internet Key Exchange (IKE):

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
```

### Related Commands

Command	Description
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# Glossary

**certification authority (CA)**—A service responsible for managing certificate requests and issuing certificates to participating IPSec network devices. This service provides centralized key management for the participating devices and is explicitly entrusted by the receiver to validate identities and to create digital certificates.

**enrollment**—The process of obtaining a new certificate from a CA.

**Internet Key Exchange (IKE)**—A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPSec. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

**IP Security (IPSec)**—A framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers.

**peer certificate**—The certificate presented by a peer, which contains the peer’s public key and is signed by the peer’s identity CA.

**public key infrastructure (PKI)**—Provides trusted and efficient key and certificate management to support security protocols such as IPSec.

**registration authority (RA)**—A server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

**RSA keys**—RSA keys come in pairs—one public key and one private key—and are used to sign and encrypt IKE key management messages and are required before you can obtain a certificate for your router.

**trustpoint ca**—A CA that combines and replaces the functionality of the identity CA (which uses its own certificate to sign the certificate of a router, thereby validating the identity of the router) and root CA (which has a self-signed certificate that contains its own public key).