



Direct HTTP Enroll with CA Servers

The Direct HTTP Enroll with CA Servers feature allows users to bypass the registration authority (RA) when enrolling with a certification authority (CA) by configuring an enrollment profile. Thus, HTTP enrollment requests can be sent directly to the CA server.

Feature History for Direct HTTP Enroll with CA Servers

Feature History	
Release	Modification
12.2(13)ZH	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The “reenroll using existing certificates” functionality was added; that is, a router that is enrolled with a third-party vendor CA can use its existing certificate to enroll with the Cisco IOS certificate server so the enrollment request is automatically granted. The following commands were added: enrollment credential , grant auto trustpoint .
12.2(18)SXE	The “reenroll using existing certificates” functionality was integrated into Cisco IOS Release 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Direct HTTP Enroll with CA Servers, page 2](#)
- [Restrictions for Direct HTTP Enroll with CA Servers, page 2](#)
- [Information About Direct HTTP Enroll with CA Servers, page 2](#)
- [How to Configure Direct HTTP Enrollment with CA Servers, page 3](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Direct HTTP Enrollment, page 12](#)
- [Additional References, page 13](#)
- [Command Reference, page 14](#)

Prerequisites for Direct HTTP Enroll with CA Servers

This feature is part of the public key infrastructure (PKI) subsystem. The PKI subsystem requires the crypto subsystem.

Restrictions for Direct HTTP Enroll with CA Servers

The CA certificate and router certificates must be returned in the following privacy enhanced mail (PEM) format:

```
-----BEGIN CERTIFICATE-----
base64 encoded cert
-----END CERTIFICATE-----
```

Information About Direct HTTP Enroll with CA Servers

To configure the Direct HTTP Enroll with CA Servers feature, you should understand the following concepts:

- [Supported CA Enrollment Methods, page 2](#)
- [About Registration Authorities, page 3](#)
- [Certificate Enrollment Profiles, page 3](#)

Supported CA Enrollment Methods

Cisco IOS software supports the following methods to obtain a certificate from a certification authority (CA):

- Simple Certificate Enrollment Protocol (SCEP)—A Cisco proprietary enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.
- Public-Key Cryptography Standard #12 (PKCS12)—The router imports certificates in PKCS#12 format from an external server.
- TFTP—The router uses the TFTP protocol to send a request to a TFTP server and to receive the issued certificate. A user may wish to enable TFTP certificate enrollment when his or her CA does not support SCEP.
- Manual (“cut-and-paste”)—The router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal. A user may wish to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and CA.

**Note**

Although most CAs accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

About Registration Authorities

Some CA servers do not support SCEP directly; thus, a RA has to process the SCEP request for the CA. An RA is essentially a server that acts as a proxy for the CA so that CA functions can continue when the CA is offline. Although the RA is often part of the CA server, the RA could also be an additional application, requiring an additional device to run it.

Certificate Enrollment Profiles

Users may configure an enrollment profile for the router to send to the CA if their CA server does not support SCEP and they do not want to use an RA as a proxy. The enrollment profile allows users to send HTTP requests directly to the CA server instead of the RA proxy.

The profile allows users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.

Prior to Cisco IOS Release 12.3(11)T and 12.2(18)SXE, certificate requests could be sent only in a PKCS #10 format; however, an additional parameter has now been added to the profile, allowing users to specify the PKCS #7 format for certificate renewal requests.

**Note**

A single enrollment profile can have up to three separate sections for each task—certificate authentication, enrollment, and reenrollment.

Benefit of Certificate Enrollment Profiles

Configuring two templates enables users to specify different URLs or methods for certificate authentication and enrollment; for example, authentication (getting the certificate of the CA) can be done via TFTP (using the [authentication url](#) command) while enrollment can be done manually (using the [enrollment terminal](#) command).

How to Configure Direct HTTP Enrollment with CA Servers

This section contains the following procedures:

- [Configuring an Enrollment Profile for the Client Router, page 4](#)
- [Configuring an Enrollment Profile for the Client Router Enrolled with a Third-Party Vendor CA, page 7](#)
- [Configuring a Cisco IOS CA to Accept Enrollment Requests from Clients of a Third-Party Vendor CA, page 9](#)

Configuring an Enrollment Profile for the Client Router

Perform this task to configure a certificate enrollment profile.

Restrictions

- If an enrollment profile is specified, an enrollment URL may not be specified in the trustpoint configuration. Although both commands are supported, only one command can be used at a time in a trustpoint.
- Because there is no standard for the HTTP commands used by various CAs, the user is required to enter the command that is appropriate to the CA that is being used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pkitrustpoint** *name*
4. **enrollment profile** *label*
5. **exit**
6. **crypto pki profile enrollment** *label*
7. **authentication url** *url*
or
authentication terminal
8. **authentication command** (optional)
9. **enrollment url** *url*
or
enrollment terminal
10. **enrollment command** (optional)
11. **parameter** *number* {**value** *value* | **prompt** *string*} (optional)
12. **exit**
13. **show crypto ca certificates**
14. **show crypto pki trustpoints**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint Entrust	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment profile label Example: Router(ca-trustpoint)# enrollment profile E	Specifies that an enrollment profile can be used for certificate authentication and enrollment.
Step 5	exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 6	crypto pki profile enrollment label Example: Router(config)# crypto pki profile enrollment E	Defines an enrollment profile and enters ca-profile-enroll configuration mode. <ul style="list-style-type: none"> <i>label</i>—Name for the enrollment profile; the enrollment profile name must match the name specified in the enrollment profile command.

	Command or Action	Purpose
Step 7	<p>authentication url <i>url</i></p> <p>Example: Router(ca-profile-enroll)# authentication url http://entrust:81</p> <p>or</p> <p>authentication terminal</p> <p>Example: Router(ca-profile-enroll)# authentication terminal</p>	<p>(Optional) Specifies the URL of the CA server to which to send certificate authentication requests.</p> <ul style="list-style-type: none"> <i>url</i>—URL of the CA server to which your router should send authentication requests. If using HTTP, the URL should read “http://CA_name,” where CA_name is the host Domain Name System (DNS) name or IP address of the CA. <p>If using TFTP, the URL should read “tftp://certserver/file_specification.” (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)</p> <p>Specifies manual cut-and-paste certificate authentication.</p>
Step 8	<p>authentication command</p> <p>Example: Router(ca-profile-enroll)# authentication command</p>	<p>(Optional) Specifies the HTTP command that is sent to the CA for authentication.</p> <p>This command should be used after the authentication url command has been entered.</p>
Step 9	<p>enrollment url <i>url</i></p> <p>Example: Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe</p> <p>or</p> <p>enrollment terminal</p> <p>Example: Router(ca-profile-enroll)# enrollment terminal</p>	<p>Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP or TFTP.</p> <p>Specifies manual cut-and-paste certificate enrollment.</p>
Step 10	<p>enrollment command</p> <p>Example: Router(ca-profile-enroll)# enrollment command POST reference_number=\$P2&authcode=\$P1 &retrievedAs=rawDER&action=getServerCert&pkcs10 Request=\$REQ</p>	<p>(Optional) Specifies the HTTP command that is sent to the CA for enrollment.</p> <p>Note The enrollment command is all on one line.</p>
Step 11	<p>parameter <i>number</i> {value <i>value</i> prompt <i>string</i>}</p> <p>Example: Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc</p>	<p>(Optional) Specifies parameters for an enrollment profile.</p> <p>This command can be used multiple times to specify multiple values.</p>

	Command or Action	Purpose
Step 12	exit Example: Router(ca-profile-enroll config)# exit Router(config)# exit	Exits ca-profile-enroll configuration mode and global configuration mode.
Step 13	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Verifies information about your certificate, the certificate of the CA, and RA certificates
Step 14	show crypto pki trustpoints Example: Router# show crypto pki trustpoints	(Optional) Displays the trustpoints that are configured in the router.

Configuring an Enrollment Profile for the Client Router Enrolled with a Third-Party Vendor CA

Perform this task to configure a certificate enrollment profile for the client router that is already enrolled with a third-party vendor CA so that the router can reenroll with a Cisco IOS certificate server.

Prerequisites

Before configuring a certificate enrollment profile for the client router, you should have already performed the following tasks at the client router:

- Defined a trustpoint that points to a third-party vendor CA
- Authenticated and enrolled the client router with the a third-party vendor CA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment profile** *label*
5. **exit**
6. **crypto pki profile enrollment** *label*
7. **enrollment url** *url*
8. **enrollment credential** *label*
9. **exit**
10. **show crypto ca certificates**
11. **show crypto pki trustpoints**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint cs	Declares the CA that your router should use and enters ca-trustpoint configuration mode. Here you should name the Cisco IOS CA that is to be used.
Step 4	enrollment profile label Example: Router(ca-trustpoint)# enrollment profile cs1	Specifies that an enrollment profile is to be used for certificate reenrollment.
Step 5	exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 6	crypto pki profile enrollment label Example: Router(config)# crypto pki profile enrollment cs1	Defines an enrollment profile and enters ca-profile-enroll configuration mode. <ul style="list-style-type: none"><i>label</i>—Name for the enrollment profile; the enrollment profile name must match the name specified in the enrollment profile command.
Step 7	enrollment url url Example: Router(ca-profile-enroll)# enrollment url http://cs:80	Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP. The enrollment URL should point to the Cisco IOS CA.
Step 8	enrollment credential label Example: Router(ca-profile-enroll)# enrollment credential msca-root	Specifies the non-Cisco IOS CA trustpoint that is to be enrolled with the Cisco IOS CA.
Step 9	exit Example: Router(ca-profile-enroll)# exit Router(config)# exit	Exits ca-profile-enroll configuration mode and global configuration mode.

	Command or Action	Purpose
Step 10	<code>show crypto pki certificates</code> Example: Router# show crypto pki certificates	(Optional) Verifies information about your certificate, the certificate of the CA, and RA certificates
Step 11	<code>show crypto pki trustpoints</code> Example: Router# show crypto pki trustpoints	(Optional) Displays the trustpoints that are configured in the router.

What to Do Next

Configure the Cisco IOS certificate server to accept enrollment requests only from clients already enrolled with the specified third-party vendor CA trustpoint. For more information, see the section [“Configuring a Cisco IOS CA to Accept Enrollment Requests from Clients of a Third-Party Vendor CA.”](#)

Configuring a Cisco IOS CA to Accept Enrollment Requests from Clients of a Third-Party Vendor CA

Perform this task to configure a Cisco IOS certificate server to accept enrollment requests only from clients who are already enrolled with the third-party vendor CA trustpoint.

Restrictions

- The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.
- The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the non-Cisco IOS CA. All other requests must be manually granted—unless the server is set to be in auto grant mode (via the **grant automatic** command).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database url** *root-url*
6. **database level** { **minimal** | **names** | **complete** }
7. **issuer-name** *DN-string*
8. **grant auto trustpoint** *label*
9. **lifetime** { **ca-certificate** | **certificate** } *time*
10. **lifetime crl** *time*
11. **cdp-url** *url*

12. **shutdown**
13. **exit**
14. **exit**
15. **show crypto pki server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http server Example: Router(config)# ip http server	Enables the HTTP server on your system.
Step 4	crypto pki server cs-label Example: Router(config)# crypto pki server cs	Enables the certificate server and enters certificate server configuration mode. The <i>cs-label</i> argument must match the name that was specified via the crypto pki trustpoint command for the client router.
Step 5	database url root-url Example: Router(cs-server)# database url nvram:	Specifies the location where all database entries for the certificate server will be written out. Note If this command is not specified, all database entries will be written to NVRAM.
Step 6	database level {minimal names complete} Example: Router(cs-server)# database level minimal	Controls what type of data is stored in the certificate enrollment database. <ul style="list-style-type: none"> minimal—Enough information is stored only to continue issuing new certificates without conflict; the default value. names—In addition to the information given in the minimal level, the serial number and subject name of each certificate. complete—In addition to the information given in the minimal and names levels, each issued certificate is written to the database. Note The complete keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server in which to store the data via the database url command.

	Command or Action	Purpose
Step 7	<p>issuer-name <i>DN-string</i></p> <p>Example: Router(cs-server)# issuer-name CN=cs</p>	Sets the CA issuer name to the specified DN-string. The default value is as follows: issuer-name CN=cs-label }.
Step 8	<p>grant auto trustpoint <i>label</i></p> <p>Example: Router(cs-server)# grant auto trustpoint msca-root</p>	<p>Enables the certificate server to automatically grant only the requests from clients that are already enrolled with the specified non-Cisco IOS CA trustpoint.</p> <p>Note The <i>label</i> argument should match the trustpoint that was specified for the client router's enrollment profile (via the enrollment credential command).</p>
Step 9	<p>lifetime {ca-certificate certificate} <i>time</i></p> <p>Example: Router(cs-server)# lifetime ca certificate 30</p>	<p>(Optional) Specifies the lifetime, in days, of a CA certificate or a certificate. Valid values range from 1 day to 1825 days.</p> <p>The default CA certificate lifetime is 3 years; the default certificate lifetime is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate.</p>
Step 10	<p>lifetime crl <i>time</i></p> <p>Example: Router(cs-server)# lifetime crl 24</p>	(Optional) Defines the lifetime, in hours, of the CRL that is used by the certificate server. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).
Step 11	<p>cdp-url <i>url</i></p> <p>Example: Router(cs-server)# cdp-url http://myhttpserver/mycdp.mycs.crl</p>	(Optional) Defines a CDP to be used in the certificates that are issued by the certificate server. URL must be an HTTP url.
Step 12	<p>shutdown</p> <p>Example: Router(cs-server)# no shutdown</p>	<p>Disables a certificate server without removing the configuration.</p> <p>You should issue this command only after you have completely configured your certificate server.</p>
Step 13	<p>exit</p> <p>Example: Router(cs-server)# exit</p>	Exits certificate server configuration mode.
Step 14	<p>exit</p> <p>Example: Router(config)# exit</p>	Exits global configuration mode.
Step 15	<p>show crypto pki server</p> <p>Example: Router# show crypto pki server</p>	(Optional) Displays the current state and configuration of the certificate server.

Configuration Examples for Direct HTTP Enrollment

This section provides the following configuration examples:

- [Direct HTTP Enrollment Configuration: Example, page 12](#)
- [Different Authentication and Enrollment Methods Configuration: Example, page 12](#)
- [Configuring a Certificate Profile for a Client Router Already Enrolled with a Third-Party Vendor CA: Example, page 12](#)
- [Configuring a Certificate Server to Automatically Accept Enrollment Requests Only from the Client Router: Example, page 13](#)

Direct HTTP Enrollment Configuration: Example

The following example show how to configure an enrollment profile for direct HTTP enrollment with a CA server:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial

crypto pki profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Different Authentication and Enrollment Methods Configuration: Example

The following example shows how to configure the enrollment profile named “E” to perform certificate authentication via TFTP and certificate enrollment via cut-and-paste (manually):

```
crypto pki profile enrollment E
  authentication url tftp://server/filename
  enrollment terminal
```

Configuring a Certificate Profile for a Client Router Already Enrolled with a Third-Party Vendor CA: Example

The following example shows how to configure the following tasks on the client router:

- Define the trustpoint “msca-root” that points to the third-party vendor CA and enroll and authenticate the client with the third-party vendor CA.
- Define trustpoint “cs” for the Cisco IOS CA.
- Define enrollment profile “cs1,” which points to Cisco IOS CA and mention (via the **enrollment credential** command) that “msca-root” is being initially enrolled with the Cisco IOS CA.

```
! Define trustpoint “msca-root” for non-Cisco IOS CA.
crypto pki trustpoint msca-root
  enrollment mode ra
```

```

enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
ip-address FastEthernet2/0
revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
  enrollment profile cs1
  revocation-check crl
!
! Define enrollment profile "cs1."
crypto pki profile enrollment cs1
  enrollment url http://cs:80
  enrollment credential msca-root!

```

Configuring a Certificate Server to Automatically Accept Enrollment Requests Only from the Client Router: Example

The following example shows how to configure the certificate server, and issue the **grant auto trustpoint** command to instruct the certificate server to accept enrollment request only from clients who are already enrolled with trustpoint "msca-root."

```

crypto pki server cs
  database level minimum
  database url nvram:
  issuer-name CN=cs
  grant auto trustpoint msca-root
!
crypto pki trustpoint cs
  revocation-check crl
  rsa-keypair cs
!
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  revocation-check crl

```

Additional References

The following sections provide references related to Direct HTTP Enroll with CA Servers.

Related Documents

Related Topic	Document Title
Cisco IOS Certificate Server configuration information and tasks	Cisco IOS Certificate Server , 12.3(11)T feature module
Additional certificate enrollment configuration tasks and information	The chapter "Configuring Certification Authority Interoperability" in the <i>Cisco IOS Security Configuration Guide</i>
Additional CA commands	Cisco IOS Security Command Reference , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new commands only.

Cisco IOS Release 12.2(13)ZH and 12.3(4)T

- [authentication command](#)
- [authentication terminal](#)
- [authentication url](#)
- [crypto ca profile enrollment](#)
- [enrollment command](#)
- [enrollment profile](#)
- [enrollment terminal](#)

- [enrollment url](#)
- [parameter](#)

Cisco IOS Release 12.3(11)T and 12.2(18)SXE

- [enrollment credential](#)
- [grant auto trustpoint](#)

authentication command

To specify the HTTP command that is sent to the certification authority (CA) for authentication, use the **authentication command** in ca-profile-enroll configuration mode.

authentication command

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use the **authentication command** to send the HTTP request to the CA server for certificate authentication. Before enabling this command, you must use the **authentication url** command.

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure certificate authentication via HTTP for the enrollment profile named "E":

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Related Commands

Command	Description
authentication url	Specifies the URL of the CA server to which to send authentication requests.
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

authentication terminal

To specify manual cut-and-paste certificate authentication requests, use the **authentication terminal** command in `ca-profile-enroll` configuration mode. To delete a current authentication request, use the **no** form of this command.

authentication terminal

no authentication terminal

Syntax Description This command has no arguments or keywords.

Defaults An authentication request is not specified.

Command Modes Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests when a network connection between the router and certification authority (CA) is not available. After this command is enabled, the authentication request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples

The following example shows how to specify manual certificate authentication and certificate enrollment via HTTP:

```
crypto ca profile enrollment E
 authentication terminal
 enrollment terminal
 enrollment url http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command POST reference_number=$P2&authcode=$P1
 &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

authentication url

To specify the URL of the certification authority (CA) server to which to send authentication requests, use the **authentication url** command in ca-profile-enroll configuration mode. To delete the authentication URL from your enrollment profile, use the **no** form of this command.

authentication url *url*

no authentication url *url*

Syntax Description

<i>url</i>	<p>URL of the CA server to which your router should send authentication requests.</p> <p>If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the <i>url</i> argument must be in the form <code>http://CA_name</code>, where <i>CA_name</i> is the host Domain Name System (DNS) name or IP address of the CA.</p> <p>If you are using TFTP for enrollment, the <i>url</i> argument must be in the form <code>tftp://certserver/file_specification</code>. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)</p>
------------	---

Defaults

Your router does not recognize the CA URL until you declare one using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

If you do not specify the **authentication command** after you enable the **authentication url** command, the **authentication url** command functions the same as the **enrollment url url** command in trustpoint configuration mode. That is, the **authentication url** command will then be used only for certificate enrollment—not authentication.

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to configure an enrollment profile for direct HTTP enrollment with a CA server. In this example, the **authentication command** is also present.

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
```

```
crypto ca profile enrollment E
authentication url http://entrust:81
authentication command GET /certs/cacert.der
enrollment url http://entrust:81/cda-cgi/clientcgi.exe
enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
parameter 1 value aaaa-bbbb-cccc
parameter 2 value 5001
```

The following example shows how to configure the enrollment profile named “E” to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
authentication url http://entrust:81
authentication command GET /certs/cacert.der
enrollment terminal
parameter 1 value aaaa-bbbb-cccc
parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment	Specifies the enrollment parameters of your CA.

crypto ca profile enrollment

To define an enrollment profile, use the **crypto ca profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto ca profile enrollment *label*

no crypto ca profile enrollment *label*

Syntax Description

<i>label</i>	Name for the enrollment profile; the enrollment profile name must match the name specified in the enrollment profile command.
--------------	--

Defaults

An enrollment profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto ca profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal**—Specifies manual cut-and-paste certificate authentication requests.
- **authentication url**—Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command**—Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal**—Specifies manual cut-and-paste certificate enrollment.
- **enrollment url**—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.



Note

The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

The following example shows how to define the enrollment profile named “E” and associated profile parameters:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.

enrollment command

To specify the HTTP command that is sent to the certification authority (CA) for enrollment, use the **enrollment command** in ca-profile-enroll configuration mode.

enrollment command

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Ca-profile-enroll configuration

Command History	Release	Modification
	12.2(13)ZH	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples The following example shows how to configure the enrollment profile name “E” for certificate enrollment:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Related Commands	Command	Description
	crypto ca profile enrollment	Defines an enrollment profile.
	parameter	Specifies parameters for an enrollment profile.

enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the **enrollment credential** command in ca-profile-enroll configuration mode.

enrollment credential *label*

Syntax Description	<i>label</i>	Name of the certification authority (CA) trustpoint of another vendor.
Defaults	No default behavior or values.	
Command Modes	Ca-profile-enroll configuration	
Command History	Release	Modification
	12.3(11)T	This command was introduced.

Usage Guidelines

To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the **crypto pki profile enrollment** command). Thereafter, you should issue the **enrollment credential** command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  ip-address FastEthernet2/0
  revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
  enrollment profile cs1
  revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
  enrollment url http://cs:80
  enrollment credential msca-root!
```

```
! Configure the certificate server, and issue and the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
  database level minimum
  database url nvram:
  issuer-name CN=cs
  grant auto trustpoint msca-root
!
crypto pki trustpoint cs
  revocation-check crl
rsa-keypair cs
!
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment profile

To specify that an enrollment profile can be used for certificate authentication and enrollment, use the **enrollment profile** command in ca-trustpoint configuration mode. To delete an enrollment profile from your configuration, use the **no** form of this command.

enrollment profile *label*

no enrollment profile *label*

Syntax Description

<i>label</i>	Creates a name for the enrollment profile.
--------------	--

Defaults

Your router does not recognize any enrollment profiles until you declare one using this command.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you can enable this command, you must enter the **crypto ca trustpoint** command.

The **enrollment profile** command enables your router to accept an enrollment profile, which can be configured via the **crypto ca profile enrollment** command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

Examples

The following example shows how to declare the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-profile-enroll configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description This command has no arguments or keywords.

Defaults A certificate enrollment request is not specified.

Command Modes Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.



Note

Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

Examples

The following example shows how to configure the enrollment profile named “E” to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url http://entrust:81
 authentication command GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

enrollment url

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the **enrollment url** command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the **no** form of this command.

enrollment url *url*

no enrollment url *url*

Syntax Description

<i>url</i>	<p>URL of the CA server to which your router should send certificate requests.</p> <p>If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the <i>url</i> argument must be in the form <code>http://CA_name</code>, where <i>CA_name</i> is the host Domain Name System (DNS) name or IP address of the CA.</p> <p>If you are using TFTP for enrollment, the <i>url</i> argument must be in the form <code>tftp://certserver/file_specification</code>. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)</p>
------------	--

Defaults

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name "E":

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
```

■ enrollment url

```
parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server will automatically grant certificate enrollment requests, use the **grant auto trustpoint** command in certificate server configuration mode.

grant auto trustpoint *label*

Syntax Description

<i>label</i>	Name of the non-Cisco IOS CA trustpoint.
--------------	--

Defaults

No default behavior or values.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the **grant auto trustpoint** command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.



Note

The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted—unless the server is set to be in auto grant mode (via the **grant automatic** command).



Caution

The **grant automatic** command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  ip-address FastEthernet2/0
```

■ grant auto trustpoint

```

    revocation-check crl
    !
    ! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
    enrollment profile cs1
    revocation-check crl
    !
    ! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
    ! enrollment credential command) that "msca-root" is being initially enrolled with the
    ! Cisco IOS CA.
crypto pki profile enrollment cs1
    enrollment url http://cs:80
    enrollment credential msca-root!

    ! Configure the certificate server, and issue the grant auto trustpoint command to
    ! instruct the certificate server to accept enrollment request only from clients who are
    ! already enrolled with trustpoint "msca-root."
crypto pki server cs
    database level minimum
    database url nvram:
    issuer-name CN=cs
    grant auto trustpoint msca-root
    !
crypto pki trustpoint cs
    revocation-check crl
rsa-keypair cs
    !
crypto pki trustpoint msca-root
    enrollment mode ra
    enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
    revocation-check crl

```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

parameter

To specify parameters for an enrollment profile, use the **parameter** command in `ca-profile-enroll` configuration mode. To disable specified parameters, use the **no** form of this command.

```
parameter number { value value | prompt string }
```

```
no parameter number { value value | prompt string }
```

Syntax Description

<i>number</i>	User parameters. Valid values range from 1 to 8.
value <i>value</i>	To be used if the parameter has a constant value.
prompt <i>string</i>	To be used if the parameter is supplied after the crypto ca authenticate command or the crypto ca enroll command has been entered.
Note	The value of the <i>string</i> argument does not have an effect on the value that is used by the router.

Defaults

No enrollment profile parameters are specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **parameter** command can be used within an enrollment profile after the **authentication command** or the **enrollment command** has been enabled.

Examples

The following example shows how to specify parameters for the enrollment profile named "E":

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

Related Commands	Command	Description
	authentication command	Specifies the HTTP command that is sent to the CA for authentication.
	crypto ca profile enrollment	Defines an enrollment profile.
	enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.