



# Manual Certificate Enrollment (TFTP and Cut-and-Paste)

---

The Manual Certificate Enrollment (TFTP and Cut-and-Paste) feature allows users to generate a certificate request and accept certification authority (CA) certificates as well as the router's certificates; these tasks are accomplished via a TFTP server or manual cut-and-paste operations. Users may wish to utilize TFTP or manual cut-and-paste enrollment in the following situations:

- Their CA does not support Simple Certificate Enrollment Protocol (SCEP) (which is the most commonly used method for sending and receiving requests and certificates)
- A network connection between the router and CA is not possible (which is how a router running Cisco IOS software obtains its certificate)

## Feature Specifications for the Manual Certificate Enrollment (TFTP and Cut-and-Paste)

---

### Feature History

Release	Modification
12.2(13)T	This feature was introduced.

---

### Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

---

## Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on 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 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 found at this URL:

<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>

#### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Contents

- [Prerequisites for Manual Certificate Enrollment \(TFTP and Cut-and-Paste\), page 2](#)
- [Restrictions for Manual Certificate Enrollment \(TFTP and Cut-and-Paste\), page 2](#)
- [Information About Manual Certificate Enrollment \(TFTP and Cut-and-Paste\), page 3](#)
- [How to Configure Manual Certificate Enrollment, page 4](#)
- [Configuration Examples for Manual Certificate Enrollment, page 8](#)
- [Additional References, page 11](#)
- [Command Reference, page 13](#)
- [Glossary, page 18](#)

## Prerequisites for Manual Certificate Enrollment (TFTP and Cut-and-Paste)

TFTP and cut-and-paste enrollment will be added to the public key infrastructure (PKI) subsystem. The PKI subsystem requires the crypto subsystem.

## Restrictions for Manual Certificate Enrollment (TFTP and Cut-and-Paste)

A user can switch between TFTP and cut-and-paste; for example, a user can paste the CA certificate via the **enrollment terminal** command, then enter **no enrollment terminal** and **enrollment url tftp://certserver/file\_specification** to TFTP the requests and router certificates. However, Cisco does not recommend switching URLs if SCEP is used; that is, if the enrollment URL is “http://,” *do not* change the enrollment URL between fetching the CA certificate and enrolling the certificate.

# Information About Manual Certificate Enrollment (TFTP and Cut-and-Paste)

To configure the Manual Certificate Enrollment (TFTP and Cut-and-Paste) feature, you must understand the following concepts:

- [TFTP Certificate Enrollment, page 3](#)
- [Cut-and-Paste Certificate Enrollment, page 3](#)

## TFTP Certificate Enrollment

A user may wish to enable TFTP certificate enrollment when his or her CA does not support SCEP, which is the most commonly used method for sending and receiving requests and certificates. This feature takes the existing **enrollment** ca-trustpoint configuration subcommand and enhances the **url url** option to support TFTP certificate enrollment—**enrollment url tftp://certserver/file\_specification**.

This enhanced subcommand specifies that TFTP should be used to send the enrollment requests and to retrieve the certificate of the CA and the certificate of the router. The `file_specification` is optional. However, if the `file_specification` is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url url** option does not include a file specification, the router’s FQDN will be used.) For example, if a user enters **enrollment url tftp://CA-server/TFTPfiles/router1**, the file “TFTPfiles/router1.ca” will be read from the TFTP server “CA-server.” If the router’s FQDN is “router1.cisco.com,” and a user enters **enrollment url tftp://CA.cisco.com**, the file “router1.cisco.com.ca” will be read from the TFTP server “CA.cisco.com.”

The file must contain the certificate of the CA in binary format or base 64 encoded.

When a user enrolls the router via the **crypto ca enroll** command, he or she is prompted for information regarding the enrollment. The filename that is to be written is already determined at this point, and an extension of “.req” is appended to indicate that this is a certificate request.

For usage keys, two requests are generated and two certificates are expected to be granted. Thus, the extension for the certificate requests are “-sign.req” and “-encr.req.”

After the user enters the **crypto ca import** command, the router will attempt to fetch the granted certificate via TFTP using the same filename that was used to send the request, except that “.req” extension will be replaced by a “.cr” extension. (The certificates are expected to be base 64 encoded PKCS#10 format certificates.) The router will parse the files it receives, verify the certificates, and insert the certificates into the internal certificate database.

## Cut-and-Paste Certificate Enrollment

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. Cut-and-paste enrollment introduces a new ca-trustpoint configuration subcommand—**enrollment**, which is in place of the **enrollment** command that is used for TFTP certificate enrollment. This command should be used when configuring the trustpoint CA. After entering the **crypto ca enroll** command, the user will be asked the same questions regarding the IP address and serial number as a TFTP enrollment. The base 64 encoded certificate request will then be displayed on the terminal.

Much like the TFTP process, the user enters the `crypto ca import` command to enter the granted certificate. With cut-and-paste, the base 64 encoded certificate will be accepted from the console terminal. Certificate input ends after the user enters “quit” on a line by itself.

## How to Configure Manual Certificate Enrollment

To enable manual certificate enrollment via TFTP or cut-and-paste, you must configure a trustpoint CA and the relevant enrollment tasks. This section contains the following procedures:

- [Configuring Certificate Enrollment via TFTP, page 4](#)
- [Configuring Certificate Enrollment via Cut-and-Paste, page 6](#)
- [Verifying Manual Certificate Enrollment, page 7](#)

## Configuring Certificate Enrollment via TFTP

To declare the trustpoint CA that your router should use and configure that trustpoint CA for manual enrollment via TFTP, use the following commands:

### Prerequisites

- You must know the correct URL to use if you are configuring certificate enrollment via TFTP.
- The router must be able to write a file to the TFTP server for the **crypto ca enroll** command.




---

**Note** Some TFTP servers require that the file exist on the server before it may be written.

---




---

**Note** Most TFTP servers require that the file be “write-able” by the world. This requirement may pose a risk because any router or other device may write or overwrite the certificate request; thus, the router will not be able to use the certificate once it is granted by the CA because the request was modified.

---

### SUMMARY STEPS

1. **enable**
2. **configure** { **terminal** | **memory** | **network** }
3. **crypto ca trustpoint** *name*
4. **enrollment** [**mode**] [**retry minutes**] [**retry number**] **url** *url*
5. **crypto ca authenticate** *name*
6. **exit**
7. **crypto ca enroll** *name*
8. **crypto ca import** *name* **certificate**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables higher privilege levels, such as privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<p><code>configure {terminal   memory   network}</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>crypto ca trustpoint name</code></p> <p><b>Example:</b> Router(config)# crypto ca trustpoint MS</p>	<p>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</p>
Step 4	<p><code>enrollment [mode] [retry minutes] [retry number] url url</code></p> <p><b>Example:</b> Router(ca-trustpoint)# enrollment url tftp://CA-Server/TFTPfiles/router1</p>	<p>Specifies the enrollment parameters of your CA.</p> <ul style="list-style-type: none"> <li>• <b>mode</b>—Specifies registration authority (RA) mode if your CA system provides a RA.</li> <li>• <b>retry minutes</b>—Specifies the wait period between certificate request retries. The default is 1 minute between retries.</li> <li>• <b>retry number</b>— Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.</li> <li>• <b>url url</b>—Specifies the URL of the CA where your router should send certificate requests.</li> </ul> <p>If you are using SCEP for enrollment, <i>url</i> must be in the form <code>http://CA_name</code>, where <i>CA_name</i> is the CA's host Domain Name System (DNS) name or IP address.</p> <p>If you are using TFTP for enrollment, <i>url</i> must be in the form <code>tftp://certserver/file_specification</code>.</p>
Step 5	<p><code>crypto ca authenticate name</code></p> <p><b>Example:</b> Router(ca-trustpoint)# crypto ca authenticate MS</p>	<p>Takes the name of the CA as the argument.</p>
Step 6	<p><code>exit</code></p> <p><b>Example:</b> Router(ca-trustpoint)# exit</p>	<p>Exits ca-trustpoint configuration mode and returns to global configuration.</p>

	Command or Action	Purpose
Step 7	<code>crypto ca enroll name</code>  Example: Router(config)# <code>crypto ca enroll MS</code>	Obtains your router's certificate(s) from the CA.
Step 8	<code>crypto ca import name certificate</code>  Example: Router(config)# <code>crypto ca import MS certificate</code>	Imports a certificate via TFTP or manually at the terminal.

## Configuring Certificate Enrollment via Cut-and-Paste

To declare the trustpoint CA that your router should use and configure that trustpoint CA for manual enrollment via cut-and-paste, use the following commands:

### SUMMARY STEPS

1. `enable`
2. `configure {terminal | memory | network}`
3. `crypto ca trustpoint name`
4. `enrollment terminal`
5. `crypto ca authenticate name`
6. `exit`
7. `crypto ca enroll name`
8. `crypto ca import name certificate`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  Example: Router> <code>enable</code>	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<code>configure {terminal   memory   network}</code>  Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>crypto ca trustpoint name</code>  Example: Router(config)# <code>crypto ca trustpoint MS</code>	Declares the CA that your router should use and enters ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 4	<code>enrollment terminal</code>  <b>Example:</b> Router(ca-trustpoint)# enrollment terminal	Specifies manual cut-and-paste certificate enrollment.
Step 5	<code>crypto ca authenticate name</code>  <b>Example:</b> Router(ca-trustpoint)# crypto ca authenticate MS	Takes the name of the CA as the argument.
Step 6	<code>exit</code>  <b>Example:</b> Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	<code>crypto ca enroll name</code>  <b>Example:</b> Router(config)# crypto ca enroll MS	Obtains your router's certificate(s) from the CA.
Step 8	<code>crypto ca import name certificate</code>  <b>Example:</b> Router(config)# crypto ca import MS certificate	Imports a certificate via TFTP or manually at the terminal.  You must enter the <b>crypto ca import</b> command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

## What to Do Next

After performing manual certificate enrollment (via TFTP or cut-and-paste), you should always verify your configuration to be sure that you successfully completed all steps. The following section [“Verifying Manual Certificate Enrollment”](#) provides steps on how to verify your configuration.

## Verifying Manual Certificate Enrollment

To verify that the Manual Certificate Enrollment feature is working, perform the following optional steps:

### SUMMARY STEPS

1. `enable`
2. `show crypto ca certificates`
3. `show crypto ca trustpoints`



```

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)#
Router(config)#crypto ca enroll MS
% Start certificate enrollment..

% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Display Certificate Request to terminal? [yes/no]:y
Signature key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYw5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxhdhXFDiWAn/hIZs9zfOtssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWYQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RrvONwx042pQchFnx9EkMuZC7evwRxJEqR
mBHXBZ8GmP3jYQsjS8MCAwEAAAhMB8GCSqGSIB3DQEBBAUAA4GBAMT6WtyFw95POY7Uf+YIYHiVRUf4SQCg
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
087fnLCNiD5Tov5jKogFHIki2EGGZxBosUw91JlenQdNdPbJc5LIWdfDvciA6j0
Nl8rOtKnt8Q+

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYw5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwG60QojpDbzbKnyj8FyTiOcv
ThkDP7XD4vLT1XaJ409z0gSIOGnIcdFtXhVlBWtpq3/O9zYFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPqev7SPXpsAIsY8a6FMq7TiwLOBqiQjLKL4cbuV0Frjl0Yuv5A/Z+
kqM0m7c+pWNWfdLe9lsCAwEAAAhMB8GCSqGSIB3DQEBBAUAA4GBACF7feURj/fJMoJPB1R6fa9Br1MJx+2F
H91YM/CIiz2n4mHTEWTWKhLoT8wUfa9NGOk7yi+nF/F7035twLfq6n2bSCTW4aem
8jLMMaeFwxkrV/ceQKrucmNC1uVx+fBy9rhnKx8j60XE25tnp1U08r6om/pBQABU
eNPFhozcaQ/2

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
n
Router(config)#crypto ca import MS certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJXBjXjYsY1I
b290MB4XDTAyMDYwODAxMTY0Ml0xDTAzMDYwODAxMjY0Ml0wJTEjMCEGCSqGSIB3
DQEBJAHMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADGy0A
MIGJAoGBAMXYVxQ4lGJ/4SGbPc3zrbLCgHWqFmLtJrPRXvz3sNNXYdeL13cYgnLL
TrNj6+cJOoyzj8ab8TiT1skD0oqS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcmDnQUHIRZ8fRJDLMQu3r8EcSRKkZgR1wWfBpj942ELI0vDAGmBAAGjggHM
MIIBYDALBgnVHQ8EBAMCB4AwHQYDVR0OBBYEFL8Quz8dyz4EGIEkx9A8UMNHLE4s
MHAGA1UdIwRpmGeAFKIacs16dKAFuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJXBjXjYsY1Y2b290
ghA6wKZe1UfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmcYwDnZXIuY2l2

```

```
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JSMIGUBggrBgEFBQcBAQSBhZCBhDA/BggrBgEF
dEVuUm9sbFxtc2NhLXJvb3QuY3JSMIGUBggrBgEFBQcBAQSBhZCBhDA/BggrBgEF
BQcwoAozYzaHR0cDovL21zY2Etc9vdC9DZXJ0RW5yb2xsL21zY2Etc9vdF9tc2Nh
LXJvb3QuY3J0MEEGCSGAQUFBzAChjVmaWx1Oi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTOX2EDoJpR/A2UHXRyqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3WOjz9wZo=
```

```
% Router Certificate successfully imported
```

```
Router(config)#
Router(config)#crypto ca import MS certificate
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
```

```
MIIDajCCAxSgAwIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31zdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0NVoXDTAzMDYwODAxMjY0NVowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dldi5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMButEKI6Q282yp8o/Bck4jnL0x5Az+1w+Ly09V2ieNpc9IEiKbpyHHR
bV4VZVQraat/zvc2BV69bR/gTAKUIty7bNCKcWgtw/YhT6nr+0j16bACLGPguhTK
u04sCzm6okIyyi+HG7ldBa45dGLr+QP2fPKjDpu3PqVjVhXS3vZbAgMBAAGjggHM
MIIBYDALBgNVHQ8EBAMCBSAwHQYDVR0OBBYEFPDO29oRdlEUSgBMg6jZR+YFRWlj
MHAGA1UdIwRpMGcAFKIAcsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ21zY28gU31zdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY21z
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JSMIGUBggrBgEFBQcBAQSBhZCBhDA/BggrBgEF
BQcwoAozYzaHR0cDovL21zY2Etc9vdC9DZXJ0RW5yb2xsL21zY2Etc9vdF9tc2Nh
LXJvb3QuY3J0MEEGCSGAQUFBzAChjVmaWx1Oi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAHaU
hyCwL1rUghNxCmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdmNPPyApuh8SoT2zBP
ZKjZU2WjcZG/nZF4W5k=
```

```
% Router Certificate successfully imported
```

## Verify Manual Certificate Enrollment Example

The following sample output is displayed after manual certificate enrollment via the **enrollment terminal** command (cut-and-paste) has been successfully configured:

```
Router# show crypto ca certificates
```

```
Certificate
  Status: Available
  Certificate Serial Number: 14DECE050000000000C48
  Certificate Usage: Encryption
  Issuer:
    CN = msca-root
    O = Cisco Systems
    C = US
  Subject:
    Name: Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root/CertEnroll/msca-root.crl
```

```
Validity Date:
  start date:18:16:45 PDT Jun 7 2002
  end   date:18:26:45 PDT Jun 7 2003
  renew date:16:00:00 PST Dec 31 1969
Associated Trustpoints:MS
```

```
Certificate
Status:Available
Certificate Serial Number:14DEC2E9000000000C47
Certificate Usage:Signature
Issuer:
  CN = msca-root
  O = Cisco Systems
  C = US
Subject:
  Name:Router.cisco.com
  OID.1.2.840.113549.1.9.2 = Router.cisco.com
CRL Distribution Point:
  http://msca-root/CertEnroll/msca-root.crl
Validity Date:
  start date:18:16:42 PDT Jun 7 2002
  end   date:18:26:42 PDT Jun 7 2003
  renew date:16:00:00 PST Dec 31 1969
Associated Trustpoints:MS
```

```
CA Certificate
Status:Available
Certificate Serial Number:3AC0A65E9547C2874AAF2468A942D5EE
Certificate Usage:Signature
Issuer:
  CN = msca-root
  O = Cisco Systems
  C = US
Subject:
  CN = msca-root
  O = Cisco Systems
  C = US
CRL Distribution Point:
  http://msca-root/CertEnroll/msca-root.crl
Validity Date:
  start date:16:46:01 PST Feb 13 2002
  end   date:16:54:48 PST Feb 13 2007
Associated Trustpoints:MS
```

## Additional References

The following sections provide information related to Manual Certificate Enrollment (TFTP and Cut-and-Paste):

- [Related Documents, page 12](#)
- [Standards, page 12](#)
- [MIBs, page 12](#)
- [RFCs, page 12](#)
- [Technical Assistance, page 13](#)

## Related Documents

Related Topic	Document Title
CA configuration tasks	The chapter “Configuring Certification Authority Interoperability” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional certificate and CA commands	The chapter “Certification Authority Interoperability Commands” in the <i>Cisco IOS Security Command Reference</i> , Release 12.2
Additional ca-trustpoint configuration commands	<i>Trustpoint CLI</i> , Cisco IOS Release 12.2(8)T feature module

## Standards

Standards	Title
None	—

## MIBs

MIBs	MIBs Link
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:  <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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 found at this URL:

<http://www.cisco.com/register>

## 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.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

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

### New Commands

- [crypto ca import](#)
- [enrollment terminal](#)

### Modified Command

- [enrollment](#)

# crypto ca import

To import a certificate manually via TFTP or cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode.

**crypto ca import** *name* **certificate**

<b>Syntax Description</b>	<i>name</i> <b>certificate</b> Specifies the name of the CA. This name is the same name used when the certification authority (CA) was declared with the <b>crypto ca trustpoint</b> command.
---------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.

<b>Usage Guidelines</b>	You must enter the <b>crypto ca import</b> command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)
-------------------------	---

<b>Examples</b>	The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."
-----------------	--

```
crypto ca trustpoint MS
  enroll terminal
  crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.
	<b>enrollment</b>	Specifies the enrollment parameters of your CA.
	<b>enrollment</b>	Specifies manual cut-and-paste certificate enrollment.

# enrollment

To specify the enrollment parameters of your certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**enrollment** [**mode**] [**retry minutes**] [**retry number**] **url** *url*

**no enrollment** [**mode**] [**retry minutes**] [**retry number**] **url** *url*

## Syntax Description

<b>mode</b>	(Optional) Specifies registration authority (RA) mode if your CA system provides a RA.
<b>retry minutes</b>	(Optional) Specifies the wait period between certificate request retries. The default is 1 minute between retries.
<b>retry number</b>	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.)
<b>url url</b>	Specifies the URL of the CA where your router should send certificate requests.  If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, <i>url</i> must be in the form http://CA_name, where CA_name is the CA's host Domain Name System (DNS) name or IP address.  If you are using TFTP for enrollment, <i>url</i> must be in the form tftp://certserver/file_specification. (The file_specification is optional. See the "Usage Guidelines" for additional information.)

## Defaults

RA mode is turned off until you enable the **mode** keyword.  
The router will send the CA another certificate request every 1 minute unless otherwise specified.  
There is no limit to the number of retries unless you specify a number via **retry number**.  
Your router does not know the CA URL until you specify it via **url url**.

## Command Modes

Ca-trustpoint configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The <b>url url</b> option was enhanced to support TFTP enrollment.

## Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded. By default, the router will keep sending requests forever, unless you can change this parameter to a finite number using the **retry** *number* option.

Use the **url** *url* option to specify or change the URL of the CA. You can specify enrollment via SCEP (an HTTP URL) or TFTP (a TFTP URL).

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the *file\_specification* is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the router’s FQDN will be used.)



#### Note

The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all *ca-identity* and *trusted-root* configuration mode commands). If you enter a *ca-identity* or *trusted-root* subcommand, the configuration mode and command will be written back as *ca-trustpoint*.

#### Examples

The following example shows how to declare a CA named “ka” and specify the URL of the CA as “http://kahului:80”:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

#### Related Commands

Command	Description
<b>crypto ca authenticate</b>	Authenticates the CA (by getting the CA’s certificate).
<b>crypto ca trustpoint</b>	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-trustpoint 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** No default behavior or values.

**Command Modes** Ca-trustpoint configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

**Usage Guidelines** 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 certification authority (CA). When this command is enabled, the certificate 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 manually certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
  enroll terminal
  crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands	Command	Description
	<b>crypto ca import</b>	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# Glossary

**base 64**—A method for encoding binary data in ASCII readable format. The base 64 encoded data may be handled as text instead of binary data.

**certificate**—A data structure defined in ISO X.509 to associate an entity (a person or a machine) with that entity's public key. The certificate contains specific fields including the name of the entity. The certificate is normally issued by a CA on behalf of the entity. (In this feature, the router acts as its own CA.) Common fields within a certificate include the entity's DN, the DN of the authority issuing the certificate, and the entity's public key.

**CA**—certification authority. 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.

**DN**—distinguished name. A name based on the ISO X.500 standard. The DN includes subfields that identify (or distinguish) the entity possessing the DN. Common subfields include the country in which the entity resides, the company and organization where the entity works, and the common name of the entity.

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

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

**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).



---

**Note**

Refer to the [Networking Terms and Acronyms](#) for terms not included in this glossary.

---