



Managing Digital Certificates from the Command Line

This chapter describes how use the command-line interface to manage digital certificates in your certificate store. Your certificate store is the location in your local file system for storing digital certificates. The store for the VPN Client is the Cisco store.

Setting Certificate Keywords

To use certificates for authentication, you must correctly set all keywords that apply to certificates in your user profile. Check your settings for the following keywords:

- **AuthType = 3** (certificate authentication)
- **CertStore = 1** (Cisco certificate store)
- **CertName = Common Name** (This must be the same common name entered for a certificate.)

For more information on setting parameters in your user profile, see “[User Profiles.](#)”

Certificate Command Syntax

The command line interface for certificate management operates in two ways:

- The standard UNIX shell or the DOS command-line prompt at which you enter all arguments for a given command on the same line.

```
cisco_cert_mgr -U -op enroll -f filename -chall challenge_phrase
```

- A prompting mode in which you enter minimum arguments for a given command and are prompted for any remaining information.

The minimum command line argument follows this basic form:

```
cisco_cert_mgr -U -op operation
cisco_cert_mgr -R -op operation
cisco_cert_mgr -E -op operation
```

Where:

- **-U** applies to the user or private certificate.

You can use the **-U** flag for all certificate management command operations, except `enroll_resume`.

- **-R** applies to the root certificate or certificate authority (CA) certificate.
You can use the -R flag for list, view, verify, delete, export, import, and change password operations.
- **-E** applies to certificate enrollment.
You can only use the -E flag with list and delete, and you must specify it using the enroll_resume operation.

The operation for the specified certificate follows the **-op** argument. Valid operations for the certificate manager command are list, view, verify, delete, export, import, enroll, enroll_file, and enroll_resume. For more information on these operations, see the “[Certificate Management Operations](#).”

For example, if you enter the following command:

```
cisco-cert-mgr -R -op import
```

Certificate manager prompts you for the name of the file to import.

Certificate Contents

This section describes the type of information contained in a digital certificate.

A typical digital certificate contains the following information:

- Common name—The name of the owner, usually both the first and last names. This field identifies the owner within the Public Key Infrastructure (PKI) organization.
- Department—The name of the owner’s department. This is the same as the organizational unit.
 - If you are connecting to a VPN 3000 concentrator, this field must match the **Group Name** configured for the owner in the concentrator.
- Company—The company in which the owner is using the certificate. This is the same as the organization.
- State—The state in which the owner is using the certificate.
- Country—The two-character country code in which the owner’s system is located.
- Email—The e-mail address of the owner of the certificate.
- Thumbprint—An MD5 hash of the certificate’s complete contents. The thumbprint provides a means for validating the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this certificate is the correct one to use.
- Key size—The size of the signing key pair in bits.
- Subject—The fully qualified domain name (FQDN) of the certificate’s owner. This field uniquely identifies the owner of the certificate in a format that can be used for LDAP and X.500 directory queries. A typical subject includes the following fields:
 - common name (**cn**)
 - organizational unit, or department (**ou**)
 - organization or company (**o**)
 - locality, city, or town (**l**)
 - state or province (**st**)
 - country (**c**)
 - e-mail address (**e**)

Other items might be included in the Subject, depending on the certificate.

- Serial number—A unique identifier used for tracking the validity of the certificate on the certificate revocation lists (CRLs).
- Issuer—The FQDN of the source that provided the certificate.
- Not before—The beginning date that the certificate is valid.
- Not after—The end date beyond which the certificate is no longer valid.

The following output is an example of the type of information contained in a digital certificate:

```
Common Name: Fred Flintstone
Department: Rock yard
Company: Stone Co.
State: (null)
Country: (null)
Email: fredf@stonemail.fake
Thumb Print: 2936A0C874141273761B7F06F8152CF6
Key Size: 1024
Subject: e=fredf@stonemail.fake,cn=Fred Flintstone,ou=Rockyard,o=Stone Co. l=Bedrock
Serial #: 7E813E99B9E0F48077BF995AA8D4ED98
Issuer: Stone Co.
Not before: Thu May 24 18:00:00 2001
Not after: Mon May 24 17:59:59 2004
```

Certificate Passwords

Each digital certificate is protected by a password. Many operations performed by the certificate management command require that you enter the password before the operation can take place.

The operations that require you to enter a password are:

- Delete
- Import
- Export
- Enroll



Note

For the enroll operation, the password to protect the digital certificate is a separate password from the optional challenge password that you enter for the server certificate.

You are prompted for any passwords that are required to complete the command. You must enter the password and verify the password again before the command can execute. If the password is not accepted, you must re-enter the command.

When you establish a VPN connection with a certificate, a certificate password is also required.

All passwords can be up to 32 alphanumeric characters in length, and are case sensitive.

Certificate Tags

A certificate tag is the identifier for each unique certificate. Each certificate added to the certificate store is assigned a certificate tag. An enroll operation also generates a certificate tag, even if the enroll operation does not complete.

Some certificate management operations require that you enter a certificate tag argument before the operation can take place. Operations that require certificate tags are listed in [Table 6-1](#). Use the **list** operation to find your certificate tag.

To enter a certificate tag argument, use the **-ct** command followed by the certificate identifier, listed as **-ct Cert #** next to the operation.

The following example shows the **view** command with a required certificate tag:

```
cisco_cert_mgr -U -op view -ct 0
```

Where the operation is **view**, and the certificate tag is **0**.

If you do not enter the **-ct** argument and certificate tag, the command line prompts you for them. If you enter an invalid certificate tag, the command line lists all certificates in the certificate store, and prompts you again for the certificate tag.

Certificate Management Operations

List all certificate management operations on the command line following the minimum command line argument. Valid operation strings allow you to list, view, verify, delete, export, import, and enroll digital certificates in your store.

The following is an example of a certificate management command with the **list** operation, and a sample output.

```
cisco_cert_mgr -U -op list
```

```
cisco_cert_mgr Version 3.0.7
```

Cert #	Common Name
0	Fred Flinstone
1	Dino

[Table 6-1](#) describes the operations that can be used with the certificate management command.

Table 6-1 Parameters for the cert_mgr Command

Parameter	Description
list	Lists all certificates in the certificate store. Each certificate in the list is identified by a unique certificate tag (<i>Cert #</i>).
view -ct Cert #	Views the specified certificate. You must enter a certificate tag.

Table 6-1 Parameters for the `cert_mgr` Command (continued)

Parameter	Description
verify -ct <i>Cert #</i>	Verifies that the specified certificate is valid. You must enter a certificate tag. If the certificate is verified, the message ‘Certificate <i>Cert #</i> verified’ appears. If the certificate fails verification for any reason, the message ‘Certificate <i>Cert #</i> failed verification’ appears. Following this message is a text string that describes the reason for the failure.
delete -ct <i>Cert #</i>	Deletes the specified certificate. You must enter a certificate tag.
export -ct <i>Cert # -f filename</i>	Exports the identified certificate from the certificate store to a specified file. You must enter a certificate tag and a filename. If either is omitted, the command line prompts you for them. You must enter the full path of the destination. If you enter only the filename, the file is placed in your working directory.
import -f filename	Imports a certificate from a specified file to the certificate store. This operation requires two different passwords: the password that protects the file (assigned by your administrator), and the password you select to protect the certificate.
enroll -cn <i>common_name</i> -ou <i>organizational_unit</i> -o <i>organization</i> -st <i>state</i> -c <i>country</i> -e <i>email</i> -ip <i>IP_Address</i> -dn <i>domain_name</i> -caurl <i>url_of_CA</i> -cadn <i>domain_name</i> [-chall <i>challenge_phrase</i>]	For user certificates only. Obtains a certificate by enrolling you with a Certificate Authority (CA) over the network. Enter each keyword individually on the command line. See the “ Enrolling Certificates ” for more information. You can obtain a challenge phrase from your administrator or from the CA.
enroll_file -cn <i>common_name</i> -ou <i>organizational_unit -o</i> <i>organization</i> -st <i>state</i> -c <i>country</i> -e <i>email</i> -ip <i>IP_Address</i> -dn <i>domain_name</i> -f <i>filename</i> -enc [base64 binary]	For user certificates only. Generates an enrollment request file that you can e-mail to the CA or paste into a webpage form. When CA generates the certificate, you must import it using the import operation. See the “ Enrolling Certificates ” for more information.

Table 6-1 Parameters for the `cert_mgr` Command (continued)

Parameter	Description
<code>enroll_resume -E -ct Cert #</code>	You cannot use this operation with user or root certificates. Resumes an interrupted network enrollment. You must enter the <code>-E</code> argument and a certificate tag.
<code>changepassword -ct Cert #</code>	Changes a password for a specified digital certificate. You must enter a certificate tag. You must enter the current password before you select the new password and confirm it.

Enrolling Certificates

A Certificate Authority (CA) is a trusted organization that issues digital certificates to users for verifying that they are who they claim to be. The certificate enrollment operations allow you to obtain your certificate from a CA over the network or from an enrollment request file.

There are three types of certificate enrollment operations.

- The **enroll** operation allows you to obtain a certificate by enrolling with a CA over the network. You must enter the URL of the CA, the domain name of the CA, and the common name.
- The **enroll_file** operation generates an enrollment request file that you can e-mail to a CA or post into a webpage form. You must enter a filename, a common name, and an encoding type.

With the `enroll` and `enroll_file` operations, you can include keywords to supply additional information (see [Table 6-2](#)).

- The **enroll_resume** operation resumes an interrupted network enrollment. You must enter the `-E` argument and a certificate tag. To find your certificate tag, use the **list** operation.

Enrollment Operations

To use enrollment operations, enter the certificate manager command, an enroll operation, and the associated keywords on the command line.

- The following example shows the `enroll` command with the minimum required keywords for common name (`-cn`), URL of the CA (`-caurl`) and domain name of the CA (`-cadn`):

```
cisco_cert_mgr -U -op enroll -cn Ren Hoek -caurl
http://172.168.0.32/certsrv/mscep/mscep.dll -cadn nobody.fake
```

- The following example shows the `enroll_file` command with the minimum required keywords for filename (`-f`), common name (`-cn`), and encoding type (`-enc`):

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -enc base64
```

- The following example shows the `enroll_file` command with the required minimum arguments and additional keywords:

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -ou Customer Service -o
Stimpy, Inc, -st CO -c US -e ren@fake.fake -ip 10.10.10.10 -dn fake.fake -enc binary
```

- The following example shows the `enroll_resume` command:

```
cisco_cert_mgr -E -op enroll_resume -ct 4
```

Table 6-2 describes options for the `enroll`, `enroll_file`, and `enroll_resume` operations.

Table 6-2 Keywords for Enrollment Operations

Parameter	Description
-cn <i>common_name</i>	The common name for the certificate.
-ou <i>organizational_unit</i>	The organizational unit for the certificate.
-o <i>organization</i>	The organization for the certificate.
-st <i>state</i>	The state for the certificate.
-c <i>country</i>	The country for the certificate.
-e <i>email</i>	The user e-mail address for the certificate.
-ip <i>IP_Address</i>	The IP address of the user's system.
-dn <i>domain_name</i>	The FQDN of the user's system.
-caurl <i>url_of_CA</i>	The URL or network address of the CA.
-cadn <i>domain_name</i>	The CA's domain name.
[-chall <i>challenge_phrase</i>]	You can obtain the challenge phrase from your administrator or from the CA.
-enc [base64 binary]	Select encoding of the output file. The default is base64. <ul style="list-style-type: none"> base64 is an ASCII-encoded PKCS10 file that you can display because it is in a text format. Choose this type when you want to cut and paste the text into the CA's website. binary is a base-2 PKCS10 (Public-Key Cryptography Standards) file. You cannot display a binary-encoded file.

Enrollment Troubleshooting Tip

If the enrollment request for a user certificate, using either the `enroll` or `enroll_file` operation, generates a CA certificate instead of a user certificate, the CA might be overwriting some of the distinguished naming information. This might be caused by a configuration issue on the CA, or a limitation of how the CA responds to enrollment requests.

The common name and subject in the enrollment request must match the certificate generated by the CA for the VPN Client to recognize it as the user certificate you requested. If it does not match, the VPN Client does not install the new user certificate as requested.

To check for this problem, view the enrollment request on the VPN Client and compare the common name and subject lines with a view of the certificate from the CA. If they do not match, then the CA is overwriting information from the client request.

To work around this issue, use the invalid certificate as an example and create an enrollment request that matches the output of the CA certificate.



Note

If the CA's certificate contains multiple department (multiple `ou` fields), you can add multiple departments to the VPN Client enrollment request by using the plus sign (+) between the department fields.

