CHAPTER 8

Cisco Trust Agent's Use of Certificates

CTA uses certificates to establish a PEAP and an EAP FAST session with Cisco Secure Access Control Server (ACS). You need to install the ACS root certificate on the client system for this session to be established.

Typically, this certificate is installed as part of a custom Cisco Trust Agent installation package. If it was not installed, CTA provides a the ctacert utility for installing and updating the posture validation server certificate on the client.

If you have installed a supplicant on the client such as the Cisco Secure Services Client, you may perform machine and user authentication using certificates. You can configure CTA for this authentication after the ACS root certificate has been installed.

This chapter contains the following sections:

About The ACS Server Root Certificate

For ACS to establish a secure PEAP or an EAP FAST session with Cisco Trust Agent, you must install the ACS root certificate on the network client. This certificate is either the CA certificate used to validate the server certificate, or a self-signed certificate generated by the ACS server. On Windows platforms, CTA supports PEM wrappered Base-64 or DER encoded binary X.509 certificates. On Linux platforms, CTA supports PEM wrappered Base-64 certificates only.

Note The ACS certificate must have "server authentication" as the certificate purpose for the PEAP session to be created.

Before you begin reviewing this chapter, obtain the ACS root certificate. If ACS uses self-signed certificates, obtain the certificate from the server. (Refer to the *User Guide for Cisco Secure ACS for Windows Server* for information about obtaining the certificate.) If you use a CA certificate, obtain the certificate from your certificate server.

Cisco Trust Agent installs a utility on the local client to help you add, delete, and manage certificates. See "About The ctacert Utility" section on page 8-3 for detailed procedures describing the use of this utility.

About The ctacert Utility

Use the ctacert utility to install, delete, and manage the root certificate used by Cisco Trust Agent for PEAP (EAPoUDP) sessions with ACS or any other certificates you want to install on the client.

The ctacert utility is installed on Linux, Mac OS X, and Windows platforms. The utility's executable file name on Linux and Mac OS X is ctacert. The utility's executable file name on Windows is ctaCert.exe. This chapter refers to the utility generically as "ctacert."

On Windows, the ctaCert.exe utility can accept PEM wrappered Base-64 or DER encoded binary X.509 certificates. On Linux platforms, the ctacert utility only accepts PEM wrappered Base-64 certificates. However, on Linux platforms, the certificates can be converted from DER to PEM formats. See, the "Converting DER Formatted Certificates to PEM Formatted Certificates" section on page 8-11 for the command to perform the conversion.

Installing or Updating Certificates Using the ctacert Utility

The ctacert utility can be used on Linux, Mac OS X, and Windows operating systems to install or update certificates.

Installing or Updating a Certificate on Linux Operating Systems

Step 1 Copy the certificate to the client.

Step 2 Open a terminal window on the network client.

Step 3 At the prompt type either of the following commands and press **<Enter>**:

- ctacert -a */path/cert_name.cer*
- ctacert --add */path/cert_name.cer*

In these examples, */path/cert_name.cer* represents the full path and file name of the certificate.

After the certificate has been installed, you receive the message, "Certificate successfully added to store with Hashed Name *Number*", where *Number* is the numeric Hashed Name of the certificate.

Installing or Updating a Certificate on Mac OS X Operating System

Step 1 Copy the certificate to the client.

Step 2 Open a terminal window.

Step 3 Change the directory to the **/opt/CiscoTrustAgent/bin** directory.

Step 4 At the prompt enter either of these commands and press **<Enter>**.

- sudo ./ctacert -a */path/cert_name.cer*
- sudo ./ctacert --add */path/cert_name.cer*

In these examples, */path/cert_name.cer* represents the full path and file name of the certificate.

After the certificate has been installed, you receive the message, "Certificate successfully added to store with Hashed Name *Number",* where *Number* is the numeric Hashed Name of the certificate.

Installing or Updating a Certificate on Windows Operating Systems

On Windows operating systems, all certificates are stored in the Microsoft Certificate Store. The ctaCert.exe utility only allows you to add certificates to the Microsoft Certificate Store. All other management of certificates is done through Microsoft's Certificate Management interface.

This is the /add command syntax for ctaCert.exe:

```
ctaCert.exe /ui {2 | 3| 4 | 5} /add "cert_path" /store "cert_store"
```

Command Parameters

Table 8-1 describes the command parameters for the ctaCert utility.

Table 8-1 ctaCert Utility Command Parameters

Parameter	Description
/ui	Specifies silent or verbose install. Accepts the following values: • **2** or **3**—Silent installation. • **4** or **5**—Full user interaction installation. Any other value entered is treated as full user interaction.
/add	Specifies the full path to the certificate being added. You can also specify *.cer to all certificates in the specified directory, for example: `c:\My_Certs\*.cer`.
/store	Specifies the system certificate store. Specifying **Root** stores the certificate in the Trusted Root Certification Authorities store.

To install a certificate using the ctaCert.exe utility, follow this procedure:

Step 1 Copy the certificate to the network client.

Step 2 Open a command prompt on the network client.

Step 3 Change directory to the location of the ctaCert.exe utility. By default, the location is `C:\Program Files\Cisco Systems\CiscoTrustAgent\`.

Step 4 At the prompt, type the following and press **<Enter>**.

`ctaCert.exe /ui x /add C:\path\cert_name.cer /store Root`

Where **/ui x** specifies the level of user interaction and where ***C:\path\cert_name.cer*** is the full path and file name of the certificate.

The certificate is added to the Trusted Root Certification Authorities store on the network client.

Listing Certificates in the Certificate Store

The ctacert utility can be used on Linux and Mac OS X to list the certificates in the client certificate store. Use the Microsoft's Certificate Management interface to perform this task on Windows operating systems.

Listing Certificates in the Certificate Store on Linux Operating Systems

Step 1 Open a terminal window on the network client.

Step 2 From any prompt enter either of these commands and press **<Enter>**.

- ctacert -l
- ctacert --list

This command displays the hashed file name, certificate version, signature algorithm, subject/issuer name, validity period, and MD5 fingerprint information. Output pertaining to different certificates are separated by a string of dashes.

Example 8-1 ctacert --list command output on Linux

```
#ctacert --list
hashed file name: 814661db.0
Version: 3 (0x2)
Serial Number: 0 (0x0)
```

```
Signature Algorithm: md5WithRSAEncryption
Issuer: O=Cisco Systems, Inc., CN=Stress
Validity
Not Before: Aug  7 11:38:06 2002 GMT
Not After : Aug 20 05:09:50 2048 GMT
Subject: O=Cisco Systems, Inc., CN=Stress
MD5 Fingerprint=13:5A:A9:B5:98:DE:78:F5:1A:7E:27:FA:E0:8B:1D:D7
------------------------------------------------------------
```

Listing Certificates in the Certificate Store on Mac OS X Operating System

Step 1 Open a terminal window on the network client.

Step 2 Change the directory to /opt/CiscoTrustAgent/bin directory.

Step 3 At the prompt enter either of these commands and press **<Enter>**.

- sudo ./ctacert -l
- sudo ./ctacert --list

Step 4 When prompted, type the root user's password.

This command displays the hashed file name, certificate version, signature algorithm, subject/issuer name, validity period, and MD5 fingerprint information. Output pertaining to different certificates are separated by a string of dashes.

Example 8-2 ctacert --list command output on Mac OS X

```
Hashed Name: 5e8a8166.0
Certificate:
    Data:
      Version: 3 (0x2)
      Serial Number: 1 (0x1)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: CN=Cisco Systems
      Validity
        Not Before: Jul 19 15:12:24 2006 GMT
        Not After : Jul 19 15:12:24 2007 GMT
      Subject: CN=Cisco Systems
        X509v3 extensions:
          X509v3 Basic Constraints:
            CA:TRUE
```

```
X509v3 Key Usage:
  Digital Signature, Key Encipherment, Key Agreement, Certificate Sign
X509v3 Subject Key Identifier:
  B5:79:DE:6A:C7:42:47:25:42:BC:68:43:93:04:69:2E:9B:08:0E:64
X509v3 Extended Key Usage:
  TLS Web Server Authentication
Netscape Cert Type:
  SSL Server
```

Deleting Certificates from the Certificate Store

The ctacert utility can be used on Linux and Mac OS X to delete certificates in the client certificate store. Use the Microsoft's Certificate Management interface to perform this task on Windows operating systems.

Deleting a Certificate from the Certificate Store on Linux Operating Systems

Step 1 Open a terminal window on the network client.

Step 2 From any prompt, enter either of these commands and press **<Enter>**.

- `ctacert -d` *HASHED-CERT-FILENAME*
- `ctacert --delete` *HASHED-CERT-FILENAME*

The `hashed-cert-file-name` can be obtained from the `ctacert --list` output. In Example 8-1, the hashed certificate file name is `814661db.0`.

For example:

ctacert -d 814661db.0

Note The hashed file name for a certificate may change when other certificates are removed.

Step 3 When prompted, type **y** to confirm your desire to delete the certificate.

Deleting a Certificate from the Certificate Store on Mac OS X Operating System

Step 1 Open a terminal window on the network client.

Step 2 Change the directory to /opt/CiscoTrustAgent/bin directory.

Step 3 At the prompt enter either of these commands and press **<Enter>**.

- `sudo ./ctacert -d` *HASHED-CERT-FILENAME*
- `sudo ./ctacert --delete` *HASHED-CERT-FILENAME*

The `hashed-cert-file-name` can be obtained from the `ctacert --list` output. In Example 8-1, the hashed certificate file name is `814661db.0`.

For example:

```
# sudo ./ctacert -d 814661db.0
```

Step 4 When prompted, type the root user's password.

Step 5 When prompted, type **y** to confirm your desire to delete the certificate.

Note The hashed file name for a certificate may change when other certificates are removed.

Clearing Certificates from the Certificate Store

The ctacert utility can be used on Linux and Mac OS X to clear all the certificates in the client certificate store. Use the Microsoft's Certificate Management interface to perform this task on Windows operating systems.

Clearing All Certificates from the Certificate Store on Linux Operating Systems

Step 1 Open a terminal window on the network client.

Step 2 From any prompt enter either of these commands:

- `ctacert -c`
- `ctacert --clear`

Clearing All Certificates from the Certificate Store on Mac OS X Operating Systems

Step 1 Open a terminal window on the network client.

Step 2 Change the directory to /opt/CiscoTrustAgent/bin directory.

Step 3 At the prompt enter either of these commands and press **<Enter>**.

- `sudo ./ctacert -c`
- `sudo ./ctacert --clear`

Step 4 When prompted, type the root user's password.

Step 5 When prompted, type **y** to confirm your desire to clear the certificate store.

Distinguished Name Matching

When using CA certificates to validate your Cisco Secure ACS server certificate, you can implement additional security using distinguished name (DN) matching to validate the server certificate. This prevents other servers or processes that may be using the same root certificate from gaining a trust relationship with the network client.

DN matching occurs at the end of the TLS handshake, after the certificate chain is built. Invalid DN matching rules are ignored, but logged. Matched rules are logged. Failed rules are not logged.

DN matching rules are configured in the [ServerDNVerification] section of the ctad.ini configuration file. If the [ServerDNVerification] section does not exist, or if there are no rules configured, then the DN matching feature is disabled and the system accepts connections with any validated certificate chain. Otherwise, the server certificate must match one of the DN matching rules for the connection to continue.

If the configuration file does not exist, the default values for these settings are used. To change the value for any of these items, you need to create the configuration file and save it to the appropriate location.

Any changes made to the [ServerDNVerification] section of the ctad.ini configuration file are detected and are implemented by Cisco Trust Agent the next time DN matching occurs.

To learn more about configuring Domain Name matching in the ctad.ini file, see "Certificate Distinguished Name Matching" section on page 5-25.

Converting DER Formatted Certificates to PEM Formatted Certificates

On Linux and Mac OS X platforms, CTA supports PEM wrappered Base-64 certificates but not DER encoded binary X.509 certificates. However DER certificates can be converted to PEM certificates using the following procedure. (For the sake of this procedure, assume that the name of the DER formatted certificate is **ca.der**.)

Note This procedure requires that OpenSSL is installed on the computer.

Step 1 Log in to the Linux or Mac computer as the root user.

Step 2 Open a terminal window.

Step 3 At the prompt, type the following:

```
openssl x509 -inform DER -outform PEM -in ca.der -out ca.pem
```