

EST Client Support

The EST Client Support feature allows you to enable EST (Enrolment Over Secure Transport) for all trustpoints while using SSL or TLS to secure transport.

- Feature Information for Overview of Cisco TrustSec, on page 1
- Information About EST Client Support, on page 1
- How to Configure EST Client Support, on page 2
- Configuration Examples for EST Client Support, on page 7
- Additional References for EST Client Support, on page 9

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.

Information About EST Client Support

Overview of EST Client Support

The EST Client Support feature allows you to use Enrollment over Secure Transport (EST) as a certificate management protocol for provisioning certificates. With the existing SCEP enrollment integrated within the PKI component, the addition of EST will introduce a new component that will use SSL or TLS to secure the transport. PKI will store all certificates.

To enable EST support, the EST client is required to authenticate the server during TLS connection establishment. For this authentication, the TLS server may require the client's credentials.

Note From Cisco IOS XE 17.16 release onwards, HTTP-based client authentication is enabled for EST Client Support.

Prerequisites for EST Client Support

- Enable the **ip http secure-server** command.

Restrictions for EST Client Support

- The EST client supports only TLS 1.2
- The certificate Attribute request is not supported.
- CA-Certificate rollover is not supported.
- Certificate-less TLS authentication is not supported.

How to Configure EST Client Support

Configure a profile for EST

Perform this task to configure a profile for EST (Enrollment Over Secure Transport).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki profile enrollment***label*
4. **method-est**
5. **enrollment url***url* [**vrf** *vrf name*]
6. **enrollment credential** *label*
7. **exit**

DETAILED STEPS

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki profile enrollment***label*

Example:

```
Device(config)# crypto pki profile enrollment pki_profile
```

Defines an enrollment profile and enters ca-profile-enroll configuration mode.

- *label*—Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.

Step 4 **method-est**

Example:

```
Device(ca-profile-enroll)# method-est
```

Enables enrollment profile to select usage of EST.

Step 5 **enrollment url***url* [**vrf** *vrf name*]

Example:

```
Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1
```

Specifies that an enrollment profile is to be used for certificate enrollment.

Note
If the authentication URL is not specified, then the enrollment URL will be considered for authentication.

Step 6 **enrollment credential** *label*

a) **enrollment credential** *label*

Example:

```
Device(ca-profile-enroll)# enrollment credential test_label
```

Provides the trustpoint credentials currently available in the profile for TLS client authentication.

b) **enrollment http username** [*http_ username*] **password** [*http_passowrd*]

Example:

```
Device(ca-profile-enroll)# enrollment http username test password test123
```

Provides HTTP credentials for HTTP based authentication over TLS.

Step 7 **exit**

Example:

```
Device(ca-profile-enroll)# exit
```

Exits ca-profile-enroll configuration mode.

Configure a trustpoint for EST

Before you begin

Create an enrollment profile for the Enrollment Over Secure Transport (EST) cryptographic protocol, which is used to manage certificate lifecycles. Refer to Configure a profile for EST, on page 2.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki trustpoint** *name-of-trustpoint*

Example:

```
Device(config)# crypto pki trustpoint tp01
```

Creates an Enrollment Over Secure Transport (EST) trustpoint.

Step 4 **revocation-check** [**crl** | **ocsp** | **none**]

Example:

```
Device(ca-trustpoint)# revocation-check crl none
```

Configures the certificate revocation methods. You can include more than one method. The device attempts to use the first specified method, and if that does not work, it uses the next in the list.

Step 5 **subject-name** [**C** | **CN** | **E** | **EMAIL** | **L** | **O** | **OU** | **ST**]

Example:

```
Device(ca-trustpoint)#subject-name CN=id.cisco.com, C=US
```

Specifies the subject name parameters, separated by commas. The certificate authority includes these parameters in certificates.

- C (Country): Two-letter ISO 3166 country code (example: C=US).
- CN (Common name): Hostname, website, or user associated with the certificate (example: CN=example.com).

- E or EMAIL: Email address associated with the organization.
- L (Localtiy): City where the organization is located (example: L=NY).
- O (Organization): Legal name of the organization.
- OU (Organizational unit): Department or division within the organization.
- ST (State or province): State or province where the organization is located.

Step 6 **enrollment profile** *profile-name*

Example:

```
Device(ca-trustpoint)# enrollment profile est-profile
```

Specifies the profile to use for the trustpoint.

Step 7 **end**

Example:

```
Device(ca-trustpoint)# end
```

Exit configuration mode.

What to do next

You can use the trustpoint when authenticating and enrolling certificates. Refer to Authenticate and enroll certificates for EST, on page 5.

Authenticate and enroll certificates for EST

On a device, send an enrollment request to a certificate authority (CA) and obtain a certificate for the device. This is called device or router certification.

Cisco IOS XE validates the CA certificate received from an EST server during the EST trustpoint authentication step, which is **crypto pki authenticate** *est-trustpoint-name*.

Cisco IOS XE retrieves the CA certificate from the EST server and validates it before installing it in the EST trustpoint. The device attempts to confirm trust for the received CA certificate by one of these methods:

- It matches a fingerprint configured on the EST trustpoint.
- It is an issuing CA certificate that validates through a root or parent CA certificate already authenticated on the device.

Only one of the methods is required to succeed, so a fingerprint match is not necessary. If the second method is true, that the EST server returns an issuing CA certificate signed by an already authenticated root CA, then Cisco IOS XE validates the certificate chain and installs the issuing CA certificate without requiring a fingerprint.

If the received CA certificate cannot be validated, the **crypto pki authenticate** *est-trustpoint-name* step fails and the CA certificate is not installed. Correct the fingerprint or configure the required trusted CA certificate before retrying authentication.

After CA authentication succeeds, the process uses **crypto pki enroll** *est-trustpoint-name* to request the device identity certificate.

Before you begin

Configure a trustpoint for EST. Refer to Configure a trustpoint for EST, on page 4.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki authenticate** *est-trustpoint-name*

Example:

```
Device(config)# crypto pki authenticate tp01
```

Obtains and authenticates the certificate of the certificate authority (CA).

Step 4 **crypto pki enroll** *est-trustpoint-name*

Example:

```
Device(config)# crypto pki enroll tp01
```

Sends an enrollment request to the CA and obtains a certificate for the device executing the procedure. This is called device or router certification.

When prompted, accept the certificate.

Step 5 **end**

Example:

```
Device(ca-trustpoint)# end
```

Exit configuration mode.

After completing this successfully, the device has an authentication certificate.

Verifying the EST Client Support Configaration

You can use the following show commands to verify EST Client Support configuration.

- **show crypto pki profile**
- **show crypto pki trustpoints estclient status**

Configuration Examples for EST Client Support

Configuring a Trustpoint to Use EST

The following example shows how to configure a trustpoint to use Enrollment over Secure Transport (EST):

```
crypto pki profile enrollment pki_profile
 method-est
 enrollment url http://www.example.com/BigCA/est/simpleenroll.dll
 enrollment credential test_label
```

Verifying EST Client Support

The following sample output from the **show crypto pki trustpoints estclient status** command verifies EST Client Support configuration.

```
Router# show crypto pki trustpoints estclient status
Trustpoint estclient:
  Issuing CA certificate configured:
    Subject Name:
     cn=estExampleCA
    Fingerprint MD5: B9D0403C 7D33F1AA F9957796 CA6E86AA
    Fingerprint SHA1: F3698C9C DCB2B5F2 A38EBCB4 1DBA6A90 9F877A5B
  Router Signature certificate configured:
    Subject Name:
     cn=estclientrouter
    Fingerprint MD5: B740849B 37016DB7 A6797CE4 D6140D27
    Fingerprint SHA1: F032B015 50BB5742 2619EFC6 F1F0B8B1 31D9906D
  State:
    Keys generated ..... Yes (Signature, non-exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following sample output from the **show crypto pki certificate estclient** command shows the status before re-enrollement and after re-enrollment.

```
BEFORE REENROLLMENT

Router# show crypto pki certificate estclient


Certificate
  Status: Available
  Certificate Serial Number (hex): 2603
  Certificate Usage: Signature
  Issuer:
    cn=estExampleCA
  Subject:
    Name: estclientrouter
```

```
    cn=estclientrouter
  CRL Distribution Points:
    http://example.com/crl.pem
  Validity Date:
    start date: 19:31:24 GMT Feb 8 2019
    end   date: 19:31:24 GMT Feb 8 2020
    renew date: 19:35:50 GMT Feb 8 2019
  Associated Trustpoints: estclient

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00ACFCD09D3182CBEB
  Certificate Usage: General Purpose
  Issuer:
    cn=estExampleCA
  Subject:
    cn=estExampleCA
  Validity Date:
    start date: 09:40:47 GMT Mar 28 2018
    end   date: 09:40:47 GMT Mar 28 2019
  Associated Trustpoints: estclient ROOT


AFTER REENROLLMENT

show crypto pki certificates estclient
Certificate
  Status: Available
  Certificate Serial Number (hex): 4B
  Certificate Usage: Signature
  Issuer:
    cn=estExampleCA
  Subject:
    Name: estclientrouter
    cn=estclientrouter
  CRL Distribution Points:
    http://example.com/crl.pem
  Validity Date:
    start date: 07:34:05 GMT Feb 9 2019
    end   date: 07:34:05 GMT Feb 9 2020
    renew date: 19:38:35 GMT Feb 8 2019
  Associated Trustpoints: estclient

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00E5EEC53E0FBD597D
  Certificate Usage: General Purpose
  Issuer:
    cn=estExampleCA
  Subject:
    cn=estExampleCA
  Validity Date:
    start date: 04:59:30 GMT Dec 20 2018
    end   date: 04:59:30 GMT Dec 20 2019
  Associated Trustpoints: estclient ROOT_SEC
```

Additional References for EST Client Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z

Standards and RFCs

Standard/RFC	Title
RFC 7030	*Enrollment over Secure Transport*
RFC 2818	*HTTP Over TLS*
RFC 6125	*Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)*
RFC 2510	*Internet X.509 Public Key Infrastructure Certificate Management Protocols*
RFC 4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html