



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.

- [Finding Feature Information, page 1](#)
- [Prerequisites for EST Client Support, page 1](#)
- [Restrictions for EST Client Support, page 2](#)
- [Information About EST Client Support, page 2](#)
- [How to Configure EST Client Support, page 2](#)
- [Configuration Examples for EST Client Support, page 4](#)
- [Additional References for EST Client Support, page 4](#)
- [Feature Information for EST Client Support, page 5](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Prerequisites for EST Client Support

- The `ip http authentication fore-close` command must be enabled.
- Only RSA certificate will be used for TLS authentication.

Restrictions for EST Client Support

- Only TLS 1.0 is supported on the EST client.
- Certificate Attribute request is not supported.
- CA-Certificate rollover is not supported.
- Certificate-less TLS authentication is not supported.

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.

How to Configure EST Client Support

Configuring a Trustpoint to Use EST

Perform this task to configure a trustpoint to use EST (Enrolment Over Secure Transport) by enabling the user to use the enrollment profile.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto pki profile enrollment <i>label</i> Example: Device(config)# crypto pki profile enrollment pki_profile	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 4	method-est Example: Device(ca-profile-enroll)# method-est	Enables enrollment profile to select usage of EST.
Step 5	enrollment url <i>url</i> [<i>vrf name</i>] 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 authentication and enrollment.
Step 6	enrollment credential <i>label</i> Example: Device(ca-profile-enroll)# enrollment credential test_label	Provides the server trustpoint credentials currently available in the profile for TLS client authentication.
Step 7	exit Example: Device(ca-profile-enroll)# exit	Exits ca-profile-enroll configuration mode.
Step 8	show crypto pki profile Example: Device# show crypto pki profile	(Optional) Displays information about PKI profile.
Step 9	show crypto pki trustpoint Example: Device# show crypto pki trustpoint	(Optional) Displays information about PKI trustpoints.

Configuration Examples for EST Client Support

Example: 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
```

Additional References for EST Client Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	<ul style="list-style-type: none"> • 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	<i>Enrollment over Secure Transport</i>
RFC 2818	<i>HTTP Over TLS</i>
RFC 6125	<i>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)</i>
RFC 2510	<i>Internet X.509 Public Key Infrastructure Certificate Management Protocols</i>

Standard/RFC	Title
RFC 4210	<i>Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)</i>

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

Feature Information for EST Client Support

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 EST Client Support

Feature Name	Releases	Feature Information
EST Client Support	Cisco IOS XE Release 3.14S	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. The following command was introduced: method-est

