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 EST Client Support, 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 4
- Additional References for EST Client Support, on page 6

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EST Client Support</td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The following command was introduced: <code>method-est</code></td>
</tr>
</tbody>
</table>

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.

The devices can obtain CA certificate automatically as part of rekey. The 'PKI - EST CA Certs on Reykey' automates the reenrollment for rekey and the task of extracting CA certificate before the reenrollment process begins. The new CA certificate certifies a public key for a device.

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.

**Prerequisites for EST Client Support**

- Enable the `ip http authentication fore-close` 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**

**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. `authentication url url`
6. `enrollment url url [vrf vrf name]`
7. `reenrollment url url [vrf vrf name]`
8. `enrollment credential label`
9. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable** | Enables privileged EXEC mode.  
- Enter your password if prompted.  

Example:
```
Device> enable
``` |
| **Step 2** | **configure terminal** | Enters global configuration mode.  

Example:
```
Device# configure terminal
``` |
| **Step 3** | **crypto pki profile enrollment label** | 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.  

Example:
```
Device(config)# crypto pki profile enrollment pki_profile
``` |
| **Step 4** | **method-est** | Enables enrollment profile to select usage of EST.  

Example:
```
Device(ca-profile-enroll)# method-est
``` |
| **Step 5** | **authentication url url** | Specifies the authentication URL that is to be used for certificate authentication.  

Example:
```
Device(ca-profile-enroll)# authentication url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1
``` |
| **Step 6** | **enrollment url [vrf vrf name]** | 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.  

Example:
```
Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1
``` |
| **Step 7** | **reenrollment url [vrf vrf name]** | Specifies that the URL of the CA IP address or host name that is to be used for reenrollment.  
**Note** Reauthentication as part of reenrollment uses the same URL for fetching CA certificate.  

Example:
```
Device(ca-profile-enroll)# enrollment url http://entrust_1:81/cda-cgi/clientcgi.exe vrf vrf1
``` |
| **Step 8** | **enrollment credential label** | Provides the trustpoint credentials currently available in the profile for TLS client authentication.  

Example:
```
Device(ca-profile-enroll)# enrollment credential test_label
``` |
| **Step 9** | **exit** | Exits ca-profile-enroll configuration mode.  

Example:
```
Device(ca-profile-enroll)# exit
``` |
Verifying the EST Client Support Configuration

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

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

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
```

Configuring EST Client Support with CA Certification for Rekey

```
crypto pki profile enrollment prof
method-est
authentication url https://10.104.49.213:8085
enrollment url https://10.104.49.213:8085
reenrollment url https://10.104.49.183:8085 (Different ip address from enrollment URL)
enrollment credential TLS

crypto pki trustpoint estclient
enrollment profile prof
subject-name CN=estclientrouter
usage ike
revocation-check none
rsakeypair estclient
auto-enroll 3
```

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-enrollment 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): 00ACFCFD09D3182CBE8
  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
Additional References for EST Client Support

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Security commands</td>
<td>• Cisco IOS Security Command Reference Commands A to C&lt;br&gt;• Cisco IOS Security Command Reference Commands D to L&lt;br&gt;• Cisco IOS Security Command Reference Commands M to R&lt;br&gt;• Cisco IOS Security Command Reference Commands S to Z</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 7030</td>
<td>Enrollment over Secure Transport</td>
</tr>
<tr>
<td>RFC 2818</td>
<td>HTTP Over TLS</td>
</tr>
<tr>
<td>Standard/RFC</td>
<td>Title</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>RFC 6125</td>
<td>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)</td>
</tr>
<tr>
<td>RFC 2510</td>
<td>Internet X.509 Public Key Infrastructure Certificate Management Protocols</td>
</tr>
<tr>
<td>RFC 4210</td>
<td>Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)</td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>