EST クライアント サポート

EST クライアント サポート機能を使用すると、SSL または TLS を使用して転送の安全性を保護しながら、すべてのトラストポイントの EST（Enrollment Over Secure Transport）を有効にできます。

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

EST クライアント サポートの情報

EST クライアント サポートの概要

EST クライアント サポート機能を使用すると、証明書をプロビジョニングするための証明書管理プロトコルとして Enrollment over Secure Transport（EST）を使用できます。PKI コンポーネント内に統合された既存の SCEP 登録では、EST を追加すると、転送を保護する SSL または TLS を使用する新しいコンポーネントが導入されます。PKI にはすべての証明書が格納されます。

EST サポートを有効にするには、EST クライアントが、TLS 接続の確立中にサーバを認証する必要があります。この認証では、TLS サーバがクライアントのクレデンシャルを要求する場合があります。

EST クライアント サポートの前提条件

- **ip http authentication fore-close** コマンドを有効にします。

EST クライアント サポートの制約事項

- EST クライアントは TLS 1.2 のみをサポートしています。
- 証明書属性要求はサポートされていません。
- CA 証明書のロールオーバーはサポートされていません。
- 証明書のない TLS 認証はサポートされていません。
- HTTP ベースのクライアント認証はサポートされていません。

EST クライアント サポートの設定方法

EST を使用するためのトラストポイントの設定

ユーザが登録プロファイルを使用できるようにすることで、EST（Enrolment Over Secure Transport）を使用するトラストポイントを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki profile enrollment**ラベル

4. **method-est**
5. **enrollment url***url*［**vrf** *vrf name*］
6. **enrollment credential** *label*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki profile enrollment**ラベル 例： `Device(config)# crypto pki profile enrollment pki_profile`	登録プロファイルを定義し、ca-profile-enroll コンフィギュレーション モードを開始します。 • *label*：登録プロファイルの名前。登録プロファイル名は、**enrollment profile** コマンドで指定された名前と同じである必要があります。
ステップ 4	**method-est** 例： `Device(ca-profile-enroll)# method-est`	登録プロファイルでESTの使用を選択できるようにします。
ステップ 5	**enrollment url***url*［**vrf** *vrf name*］ 例： `Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1`	証明書登録に登録プロファイルを使用するように指定します。 （注） 認証 URL が指定されていない場合は、登録 URL が認証に使用されます。
ステップ 6	**enrollment credential** *label* 例： `Device(ca-profile-enroll)# enrollment credential test_label`	TLS クライアント認証にプロファイルで現在利用可能なトラストポイントログイン情報を提供します。
ステップ 7	**exit** 例： `Device(ca-profile-enroll)# exit`	ca-profile-enroll コンフィギュレーション モードを終了します。

EST クライアントサポートの設定の確認

次の show コマンドを使用すると、EST クライアントサポートの設定を確認できます。

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

EST クライアント サポートの設定例

EST を使用するためのトラストポイントの設定

次の例では、Enrollment over Secure Transport（EST）を使用するためにトラストポイントを設定する方法について示します。

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

EST クライアントサポートの確認

次に、EST クライアントサポートの設定を確認する **show crypto pki trustpoints estclient status** コマンドの出力例を示します。

```
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
```

次に、再登録前と再登録後のステータスを示す **show crypto pki certificate estclient** コマンドの出力例を示します。

```
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
```

EST クライアント サポートの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『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』

標準および RFC

標準/RFC	タイトル
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)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。