# Cisco Adaptive Security Appliance（ASA）と Microsoft Access Edge との間における VeriSign を使用したセキュリティ証明書交換



# Cisco Adaptive Security Appliance でのセキュリティ証明書の設定

## 古い証明書およびトラストポイントの削除

この手順では、古い中間証明書、署名済み証明書、およびルート証明書のトラストポイントを Cisco Adaptive Security Appliance で削除する方法について説明します。

### はじめる前に

次の章に記載されている設定タスクを実行したことを確認します。

- SIP フェデレーション用の IM and Presence サービスの設定
- SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、トラストポイントを表示します。

```
show crypto ca trustpoints
```

**ステップ 3** 次のコマンドを入力して、トラストポイントと関連する証明書を削除します。

```
no crypto ca trustpoint trustpoint_name
```

次の警告の出力が表示されます。

```
WARNING: Removing an enrolled trustpoint will destroy allcertificates received from the
related Certificate Authority.
```

**ステップ 4** トラストポイントの削除を確認するメッセージが表示されたら、yes と入力します。

### 次の作業

VeriSign 用の新しいトラストポイントの生成, （2 ページ）

# VeriSign 用の新しいトラストポイントの生成

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、この証明書のキー ペアを生成します。

```
crypto key generate rsa label keys_for_verisign
```

**ステップ 3** 次の一連のコマンドを入力して、IM and Presence Service のトラストポイントを作成します。

```
(config)# crypto ca trustpoint trustpoint_name
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# subject-name
cn=fqdn,OU=organisational_unit,O=organisation_name,C=country,St=state,L=locality
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# exit
```

（注） 更新の証明書署名要求（CSR）ファイルを VeriSign に送信する場合、件名の値には次の情報を含める必要があります。

- 国（Country）（2 文字の国コードのみ）
- 都道府県（State）（省略なし）
- 市区町村（Locality）（省略なし）
- 組織名（Organization Name）
- 組織単位（Organizational Unit）
- 一般名（Common Name）（FQDN）- この値はパブリック IM and Presence の FQDN にする必要があります。

トラブルシューティングのヒント

**show crypto key mypubkey rsa** コマンドを入力して、キー ペアが生成されていることを確認します。

### 次の作業

中間証明書をインポートする，（6 ページ）

# ルート証明書のインポート

### はじめる前に

VeriSign 用の新しいトラストポイントの生成，（2 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を Cisco Adaptive Security Appliance にインポートします。

```
crypto ca authenticate trustpoint_name
```

**ステップ 3** 次のように CA 証明書を入力します。

```
-----BEGIN CERTIFICATE-----MIIDAzCCAmwCEQC5L2DMiJ+hekYJuFtwbIqvMA0GCSqGSIb3DQEBBQUAMIH...
-----END CERTIFICATE----- quit

quit
```

（注） 別の行に "quit" という単語を入力して終了します。

**ステップ 4** 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

### 次の作業

証明書署名要求の生成，（4 ページ）

# 証明書署名要求の生成

### はじめる前に

ルート証明書のインポート，（3 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、CA に対する登録要求を送信します。

```
(config)# crypto ca enroll trustpoint_name
```

次の警告の出力が表示されます。

```
%WARNING: The certificate enrollment is configured with an fqdnthat differs from the system fqdn. If this certificate will be used for VPN authentication this may cause connection problems.
```

**ステップ 3** 登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

```
% Start certificate enrollment..% The subject name in the certificate will be: <fqdn>, OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

**ステップ 4** サブジェクト名にデバイスのシリアル番号を含めることを確認するメッセージが表示されたら、**no** と入力します。

**ステップ 5** 端末に証明書要求を表示することを確認するメッセージが表示されたら、**yes** と入力します。
証明書要求が表示されます。

### 次の作業

証明書署名要求を VeriSign に送信する，（4 ページ）

# 証明書署名要求を VeriSign に送信する

証明書署名要求を送信すると、VeriSign から次の証明書ファイルが提供されます。

- verisign-signed-cert.cer（署名済み証明書）
- trial-inter-root.cer（下位中間ルート証明書）
- verisign-root-ca.cer（ルート CA 証明書）

証明書ファイルをダウンロードしたら、別のメモ帳ファイルに証明書ファイルを保存します。

### はじめる前に

- 証明書署名要求の生成, （4 ページ）の手順を完了します。
- 証明書署名要求を生成するときは、定義したチャレンジ パスワードが必要になります。

### 手順

**ステップ 1** VeriSign Web サイトにアクセスします。

**ステップ 2** 記載されている手順に従って証明書署名要求を入力します。

**ステップ 3** プロンプトが表示されたら、証明書署名要求のチャレンジ パスワードを送信します。

**ステップ 4** 表示されるウィンドウに証明書署名要求を貼り付けます。

（注） **-----BEGIN CERTIFICATE-----** から **-----END CERTIFICATE-----** までを（これらの文字列を含めて）貼り付けなければなりません。

### 次の作業

証明書署名要求に使用した証明書の削除, （5 ページ）

# 証明書署名要求に使用した証明書の削除

証明書署名要求の生成に使用した一時ルート証明書は削除する必要があります。

### はじめる前に

証明書署名要求を VeriSign に送信する, （4 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を表示します。

```
(config)# show running-config crypto calook for crypto ca certificate chain trustpoint_name
```

**ステップ 3** 次のコマンドを入力して、証明書を削除します。

```
(config)# crypto ca certificate chain trustpoint_name

(config-cert-chain)# no certificate ca 00b92f60cc889fa17a4609b85b70$
```

次の警告の出力が表示されます。

```
WARNING: The CA certificate will be disassociated from this trustpoint andwill be removed
if it is not associated with any other trustpoint. Any other certificates issued by this
CA and associated with this trustpoint will also be removed.
```

**ステップ 4** トラストポイントの削除を確認するメッセージが表示されたら、**yes** と入力します。

### 次の作業

中間証明書をインポートする, （6 ページ）

# 中間証明書をインポートする

### はじめる前に

証明書署名要求に使用した証明書の削除, （5 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable

> <password>

> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を Cisco Adaptive Security Appliance にインポートします。

```
crypto ca authenticate trustpoint_name
```

**ステップ 3** 次のように CA 証明書を入力します。

```
-----BEGIN CERTIFICATE-----MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQU....
-----END CERTIFICATE-----

quit
```

（注） 別の行に "quit" という単語を入力して終了します。

**ステップ 4** 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

### 次の作業

ルート証明書のトラストポイントの作成, （7 ページ）

# ルート証明書のトラストポイントの作成

### はじめる前に

中間証明書をインポートする，（6 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、トラストポイントを生成します。

```
(config)# crypto ca trustpoint verisign_root
(config-ca-trustpoint)#
```

**ステップ 3** 次の一連のコマンドを入力します。

```
(config-ca-trustpoint)# revocation-check none
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# exit
```

# ルート証明書のインポート

### はじめる前に

ルート証明書のトラストポイントの作成，（7 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を Cisco Adaptive Security Appliance にインポートします。

```
crypto ca authenticate verisign_root
```

**ステップ 3** 次のように CA 証明書を入力します。

```
-----BEGIN CERTIFICATE-----MIICmDCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAw....
-----END CERTIFICATE-----
```

**quit**

（注） 別の行に “quit” という単語を入力して終了します。

**ステップ 4** 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

### 次の作業

署名付き証明書のインポート，（8 ページ）

# 署名付き証明書のインポート

### はじめる前に

ルート証明書のインポート，（7 ページ）の手順を完了します。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を Cisco Adaptive Security Appliance にインポートします。

```
crypto ca import verisignca certificate
```

次の警告の出力が表示されます。

```
WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems.
```

**ステップ 3** 証明書の登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

**ステップ 4** 次のように CA 証明書を入力します。

```
-----BEGIN CERTIFICATE-----MIIFYTCCBEmgAwIBAgIQXtEPGWzZ0b9gejHejq+HazANBgkqhkiG9w0B....
-----END CERTIFICATE-----
```

**quit**

（注） 別の行に “quit” という単語を入力して終了します。

**ステップ 5** 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

### 次の作業

VeriSign 証明書を Microsoft Access Edge にインポートする，（9 ページ）

# VeriSign 証明書を Microsoft Access Edge にインポートする

この手順では、VeriSign のルート証明書と中間証明書を Microsoft のアクセス エッジ サーバにインポートする方法について説明します。

### はじめる前に

VeriSign から提供された証明書をアクセス エッジ サーバ（C:\ など）に保存します。

### 手順

**ステップ 1** アクセス エッジ サーバで、run コマンドから **mmc** を実行します。
**ステップ 2** [File（ファイル）] > [Add/Remove Snap-in（スナップインを追加/削除）] を選択します。
**ステップ 3** [Add（追加）] をクリックします。
**ステップ 4** [Certificates（証明書）] をクリックします。
**ステップ 5** [Add（追加）] をクリックします。
**ステップ 6** [Computer account（コンピュータ アカウント）] を選択します。
**ステップ 7** [Next（次へ）] をクリックします。
**ステップ 8** [Local Computer（ローカル コンピュータ）] を選択します。
**ステップ 9** [Finish（完了）] をクリックします。
**ステップ 10** **[Add/Remove Snap-In（スナップインを追加/削除）]** ウィンドウを閉じるには、[OK（OK）] をクリックします。
**ステップ 11** メイン コンソールで、[Certificates（証明書）] ツリーを展開します。
**ステップ 12** [Trusted Root Certificates（信頼済みのルート証明書）] ブランチを開きます。
**ステップ 13** [Certificates（証明書）] を右クリックします。
**ステップ 14** [All Tasks（すべてのタスク）] > [Import（インポート）] を選択します。
**ステップ 15** 証明書ウィザードの [Next（次へ）] をクリックします。
**ステップ 16** C:\ ディレクトリにある VeriSign 証明書を参照します。
**ステップ 17** [Place all certificates in the following store（すべての証明書を次のストアに配置）] をクリックします。
**ステップ 18** 証明書ストアとして、[Trusted Root Certification Authorities（信頼されたルート証明機関）] を選択します。
**ステップ 19** ステップ 13 ～ 18 を繰り返して追加の VeriSign 証明書をインポートします。