



セキュリティの設定

この章では、セキュリティ証明書を設定および管理する手順について説明します。この章は、次の項で構成されています。

- 「セキュリティの概要」(P.291)
- 「証明書とプライベート キーの入手」(P.292)
- 「証明書とキーのペアの表示」(P.293)
- 「デフォルトの証明書とキーのペアの変更」(P.293)
- 「証明書とキーのペアの削除」(P.294)

セキュリティの概要

Cisco Unity Express には、セキュリティ証明書を設定し、管理するためのインフラストラクチャが用意されています。

この証明書を入手するには、次のいずれかの方法を使用します。

- 512 ~ 2048 の絶対値サイズで RSA 暗号アルゴリズムを使用し、自己署名証明書を生成します。



(注) 自己署名証明書の場合、一部のクライアントは警告メッセージを表示し、ユーザに証明書の承認を要求します。

- Certificate Authority (CA; 証明機関) から証明書を入手します。Cisco Unity Express コンソールからこれらの証明書をインポートするか、FTP サーバまたは HTTP サーバからアップロードします。

証明書は、Distinguished Encoding Rules (DER) または Privacy Enhanced Mail (PEM; プライバシーエンハンスド メール) のいずれかの符号化形式を使用します。

セキュアな接続を確立するために証明書を必要とする任意の機能で、このインフラストラクチャを使用できます。



(注) この設定とインフラストラクチャは、Cisco Unity Express デバイスだけに適用されます。その他のデバイスについては、それぞれのデバイスのドキュメントを参照してください。

証明書とプライベート キーの入手

SSL 用に IMAP サーバを設定し、SSL 接続を許可するためには、Cisco Unity Express にデフォルトの証明書とプライベート キーが必要です。証明書とキーのペアを入手するには、次の 2 つの手順があります。

- **証明書とキーのペアの生成**：コマンドでペアを自動的に生成します。
- **証明書とキーのペアのインポート**：コマンドで、コンソールまたはリモート サーバからペアをインポートします。

証明書とキーのペアの生成

Cisco Unity Express 設定モードで開始し、次のコマンドを使用して、Cisco Unity Express システムに証明書とキーのペアを生成します。

```
crypto key generate [rsa {label label-name | modulus modulus-size} | default]
```

ここで、**rsa** はサポートされる暗号化アルゴリズム、**label-name** は証明書とキーのペアに割り当てられる名前、**modulus-size** はキーを生成するために使用する 512 と 2048 の間の数値で、**default** はシステムのデフォルトとして生成される証明書とキーのペアを指定します。キーワードを選択しない場合、またはラベルを指定しない場合は、形式 *hostname.domainname* の名前で証明書とキーのペアが自動的に生成されます。

次の例では、ラベル `alphakey.myoffice` を持つデフォルトの証明書とキーのペアが生成されます。

```
se-10-0-0-0# config t
se-10-0-0-0(config)# crypto key generate label alphakey.myoffice modulus 600 default
se-10-0-0-0(config)# end
```

証明書とキーのペアのインポート

Cisco Unity Express 設定モードで開始し、次のコマンドを使用して、証明書とキーのペアをインポートします。

```
crypto key import rsa label label-name {der url {ftp: | http:} | pem {terminal | url {ftp: | http:}} [default]
```

ここで、パラメータは次のように定義されています。

- **rsa** は、サポートされる暗号化アルゴリズムです。
- **label label-name** は、証明書とキーのペアに割り当てられる名前です。
- **der** および **pem** は、インポートされる証明書の符号化形式です。
- **terminal** は、コンソールからインポートすることを示します。
- **url {ftp: | http:}** は、指定した URL のリモート サーバからインポートすることを示します。
- **default** は、システムのデフォルトとしてインポートした証明書とキーのペアを指定します。

このコマンドでは、証明書とプライベート キーの情報を要求されます。

次の例では、ラベル `alphakey.myoffice` を持つデフォルトの証明書とキーのペアがインポートされます。

```
se-10-0-0-0# config t
se-10-0-0-0(config)# crypto key import rsa label alphakey.myoffice pem terminal

Enter certificate...
End with a blank line or "quit" on a line by itself
```

```
Enter private key...
Private key passphrase?
End with a blank line or "quit" on a line by itself

quit

Import succeeded.
```

証明書とキーのペアの表示

Cisco Unity Express EXEC モードで開始し、次のコマンドを使用すると、システム上のすべての証明書とキーのペアのリストを表示したり、特定の証明書とキーのペアを表示できます。

```
show crypto key {all | label label-name}
```

ここで、**all** でシステム上のすべての証明書とキーのペアが表示され、**label label-name** では指定した証明書とキーのペアの情報が表示されます。

次の例は、**show crypto key** コマンドのサンプル出力を示しています。

```
se-10-0-0-0# show crypto key label alphakey.myoffice

Label name: alphakey.myoffice [default]
Entry type:Key Entry
Creation date: Mon Jun 10 14:23:09 PDT 2002
Owner: CN=se-1-100-6-10.localdomain, OU='', O='', L='', ST='', C=''
Issuer: CN=se-1-100-6-10.localdomain, OU='', O='', L='', ST='', C=''
Valid from: Mon Jun 10 14:23:06 PDT 2002 until: Sun Sep 08 14:23:06 PDT 2002
```

デフォルトの証明書とキーのペアの変更

Cisco Unity Express 設定モードで次のコマンドを使用して、証明書とキーのペアをシステムのデフォルトとして指定します。

```
[no] crypto key label label-name default
```

ここで **label label-name** は、新しいシステムのデフォルトとして指定する証明書とキーのペアです。

システムに複数の証明書とキーのペアが存在し、どれもシステムのデフォルトではない場合は、このコマンドを使用していずれかのペアをシステムのデフォルトとして指定します。

デフォルトの証明書とキーのペアが存在する場合、別のペアをデフォルトとして指定すると、最初のペアからデフォルト ステータスが自動的に削除されます。

このコマンドの **no** 形式は、証明書とキーのペアを削除せず、システム デフォルトの指定だけを削除します。

証明書とキーのペアが存在しない場合は、エラー メッセージが表示されます。

証明書とキーのペアの削除

Cisco Unity Express 設定モードで開始し、次のコマンドを使用して、証明書とキーのペアを削除します。

```
crypto key delete {all | label label-name}
```

ここで、**all** でシステム上のすべての証明書とキーのペアが削除され、**label label-name** では指定した証明書とキーのペアの情報が削除されます。

次の例は、**alphakey.myoffice** というラベルの付いた証明書とキーのペアを削除します。

```
se-10-0-0-0# config t  
se-10-0-0-0(config)# crypto key delete label alphakey.myoffice  
se-10-0-0-0(config)# end
```

証明書とキーのペアが存在しない場合は、エラーメッセージが表示されます。