



Configuring Security

Last Updated: July 25, 2006

This chapter describes the procedures for configuring and managing security certificates and includes the following sections:

- [Overview of Security, page 133](#)
- [Obtaining a Certificate and Private Key, page 134](#)
- [Displaying the Certificate-Key Pairs, page 135](#)
- [Changing the Default Certificate-Key Pair, page 135](#)
- [Deleting a Certificate-Key Pair, page 135](#)

Overview of Security

Cisco Unity Express provides the infrastructure for configuring and managing security certificates.

You can obtain these certificates using either of the following methods:

- Generate self-signed certificates using the RSA encryption algorithm with a modulus size from 512 to 2048.



Note For self-signed certificates, certain clients display a warning message and require subscribers to accept the certificate.

- Obtain the certificates from the Certificate Authority (CA). Import these certificates from the Cisco Unity Express console or upload them from an FTP or HTTP server.

The certificates use either the Distinguished Encoding Rules (DER) or Privacy Enhanced Mail (PEM) encoding formats.

Configure the Integrated Messaging Access Protocol (IMAP) feature to use this infrastructure to provide a secure connection between an e-mail client and a Cisco Unity Express module.



Note This configuration and infrastructure apply only to Cisco Unity Express devices. For other devices, see their respective device documentation.

Obtaining a Certificate and Private Key

Cisco Unity Express requires a default certificate and private key before the IMAP server is configured for SSL and can accept SSL connections. Two procedures are available to obtain a certificate-key pair:

- [Generating a Certificate-Key Pair](#)—A command automatically generates the pair.
- [Importing a Certificate-Key Pair](#)—A command imports a pair from the console or a remote server.

Generating a Certificate-Key Pair

Starting in Cisco Unity Express configuration mode, use the following command to have the Cisco Unity Express system generate a certificate-key pair:

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

where **rsa** is the supported encryption algorithm, *label-name* is the name assigned to the certificate-key pair, *modulus-size* is a number between 512 and 2048 used for generating a key, and **default** designates the generated certificate-key pair as the system default. If you do not select any keywords or do not specify a label, the system automatically generates a certificate-key pair with a name in the format *hostname.domainname*.

The following example generates a default certificate-key pair with the label `alphakey.myoffice`.

```
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
```

Importing a Certificate-Key Pair

Starting in Cisco Unity Express configuration mode, use the following command to import a certificate-key pair:

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

where the parameters are defined as follows:

- **rsa** is the supported encryption algorithm.
- **label** *label-name* is the name assigned to the certificate-key pair.
- **der** and **pem** are the encoding formats of the imported certificate.
- **terminal** indicates that the import is coming from the console.
- **url {ftp: | http:}** indicates that the import is coming from a remote server at the specified URL.
- **default** designates the imported certificate-key pair as the system default.

The command prompts you for the certificate and private key information.

The following example imports a default certificate-key pair with the label `alphakey.myoffice`.

```
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.
```

Displaying the Certificate-Key Pairs

Starting in Cisco Unity Express EXEC mode, use the following command to display a list of all certificate-key pairs on the system or to display a specific certificate-key pair.

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

where **all** displays all certificate-key pairs on the system and **label label-name** displays information for the specified certificate-key pair.

The following is sample output for the **show crypto key** command:

```
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
```

Changing the Default Certificate-Key Pair

Use the following command in Cisco Unity Express configuration mode to designate a certificate-key pair as the system default.

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

where **label label-name** is the certificate-key pair that is designated as the new system default.

If several certificate-key pairs exist on the system and none of them are the system default, use this command to designate one of them as the system default.

If a certificate-key pair exists as the default, designating another pair as the default automatically removes the default status from the first pair.

The **no** form of the command does not delete the certificate-key pair; it only removes the system default designation.

The system displays an error message if the certificate-key pair does not exist.

Deleting a Certificate-Key Pair

Starting in Cisco Unity Express configuration mode, use the following command to delete a certificate-key pair.

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

where **all** deletes all certificate-key pairs on the system and **label** *label-name* deletes information for the specified certificate-key pair.

The following deletes the certificate-key pair labeled `alphakey.myoffice`:

```
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
```

An error message appears if the certificate-key pair does not exist.