CHAPTER 12

Cisco Unified SIP Proxy Security Commands

Last Updated: November 25, 2019

crypto key certreq

To generate a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate, use the **crypto key certreq** command in module configuration mode. This command does not have a **no** or **default** form.

crypto key certreq label *label-name* **url** {**ftp:** | **http:**}

Syntax Description

label *label-name*	Requests a CSR for the specified certificate-private key pair.
url {**ftp:** | **http:**}	Specifies a remote server as the source of the certificate and key. The system prompts you for more information.

Command Default

This command has no defaults.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The certificate sign request is only valid after the key is generated. Note that the **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

Examples

The following example generates a certificate sign request XXXX.

```
se-10-1-0-0(config)# crypto key certreq label XXXX url ftp:
se-10-1-0-0(config)#
```

Related Commands

Command	Description
crypto key default	Designates a certificate-private key pair as the system default.
crypto key delete	Deletes a certificate-private key pair.
crypto key generate	Generates a certificate-private key pair.
show crypto key	Displays configured certificate-private key pairs.

crypto key label default

To set a certificate and private key pair as the system default, use the **crypto key default** command in module configuration mode. To remove the system default designation from the certificate-key pair, use the **no** form of this command.

crypto key label *label-name* **default**

no crypto key label *label-name* **default**

Syntax Description

label *label-name*	The name of the certificate-private key pair to be set as the system default.

Command Default

This command has no defaults.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Note that the **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

Setting the certificate-key pair allows applications such as integrated messaging to use the default certificate for SSL security without knowing the specific label name of the pair.

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.

To change the designation from one pair to another, remove the designation from the original pair using the **no** form of this command. Then assign the designation to the new pair.

The **no** form of this command does not delete the certificate or private key. The pair remains on the system and is no longer designated as the system default pair.

The system displays an error message if either of the certificate-key pairs does not exist.

Examples

The following example designates the certificate-private key pair with the label mainkey.ourcompany as the system default.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key label mainkey.ourcompany default
se-10-1-0-0(config)#
```

The following example changes the system default designation from certificate-key pair alphakey.myoffice to betakey.myoffice:

```
se-10-1-0-0# configure terminal
```

```
se-10-1-0-0(config)# no crypto key label alphakey.myoffice default
se-10-1-0-0(config)# crypto key label betakey.myoffice default
se-10-1-0-0(config)# end
```

Related Commands

Command	Description
crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
crypto key delete	Deletes a certificate-private key pair.
crypto key generate	Generates a certificate-private key pair.
show crypto key	Displays configured certificate-private key pairs.

crypto key delete

To delete a certificate and private key pair from the system, use the **crypto key delete** command in module configuration mode. This command does not have a **no** or **default** form.

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

Syntax Description

all	Deletes all certificate-private key pairs on the system.
label *label-name*	Deletes the specified certificate-private key pair.

Command Default

This command has no defaults.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

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

Examples

The following example deletes the certificate and private key with the name mainkey.ourcompany.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key delete label mainkey.ourcompany
se-10-1-0-0(config)#
```

Related Commands

Command	Description
crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
crypto key default	Designates a certificate-private key pair as the system default.
crypto key generate	Generates a certificate-private key pair.
show crypto key	Displays configured certificate-private key pairs.

crypto key generate

To generate a self-signed certificate and private key, use the **crypto key generate** command in module configuration mode. This command does not have a **no** or **default** form.

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

Syntax Description

rsa	(Optional) Specifies the algorithm for public key encryption.
label *label-name*	(Optional) Assigns a name to the certificate-key pair.
modulus *modulus-size*	(Optional) Specifies the size of the modulus, which is the base number for generating a key. Valid values are 512 to 1024 and must be a multiple of 8.
default	(Optional) Assigns the generated certificate-key pair as the system default.

Command Default

The default encryption algorithm is ras.
The default label has the form *hostname***.***domainname*.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

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*.

Use the **crypto key generate** command or the **crypto key label default** command to set a certificate-key pair as the system default.

Examples

The following example generates a certificate and private key with the name mainkey.ourcompany, size 750, and assigns the generated pair as the system default.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key generate label mainkey.ourcompany modulus 750 default
se-10-1-0-0(config)#
```

Related Commands

Command	Description
crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
crypto key default	Designates a certificate-private key pair as the system default.
crypto key delete	Deletes a certificate-private key pair.
show crypto key	Displays configured certificate-private key pairs.

show crypto key

To display configured certificate-private key pairs, use the **show crypto key** command in module EXEC mode.

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

Syntax Description

all	Displays all configured certificate-private key pairs.
label *label-name*	Displays characteristics of the specified certificate-private key pair. An error message appears if *label-name* does not exist.

Command Modes

Module EXEC

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

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

```
se-10-1-0-0# show crypto key label mainkey.ourcompany

Label name: mainkey.ourcompany [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
```

Table 1 describes the significant fields shown in the display.

Table 1 show crypto key Field Descriptions

Field	Description
Label name	Name of the certificate-key pair.
Entry type	Method of providing the certificate-key pair.
Creation date	Date the certificate-key pair was created.
Owner	Owner of the certificate-key pair.
Issuer	Issuer of the certificate-key pair.
Valid from	Dates for which the certificate-key pair is valid.

Related Commands

Command	Description
crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
crypto key default	Designates a certificate-private key pair as the system default.

Command	Description
crypto key delete	Deletes a certificate-private key pair.
crypto key generate	Generates a certificate-private key pair.

web session security

To associate a security key for accessing the Cisco Unified SIP Proxy GUI using HTTPS, use the **web session security** command in Cisco Unified SIP Proxy configuration mode. To disable HTTPS access to the Cisco Unified SIP Proxy GUI session, use the **no** or **default** form of this command.

web session security keylabel *labelname*

no web session security keylabel *labelname*

default web session security keylabel

Syntax Description

keylabel *label-name*	Associates the certificate-key pair to the HTTPS connection.

Command Modes

Cisco Unified SIP Proxy configuration

Command History

Cisco Unified SIP Proxy Version	Modification
8.5	This command was introduced.
10.1	HTTPS is enabled by default. The command **no web session security keylabel** *labelname* is disabled.

Usage Guidelines

Before configuring the connection type, the system must have a default security certificate and private key. Use the **crypto key generate** command to generate the pair of values. Once the crypto key is generated and associated with HTTPS, you use the web session security command to enable HTTPS access to the Cisco Unified SIP Proxy GUI.

From Cisco Unified SIP Proxy Release 10.1 onwards, HTTPS is enabled by default. You need not manually generate a crypto key and pass it to the web session security to enable HTTPS. Cisco Unified SIP Proxy Release 10.1 supports only TLS v1.2 for HTTPS. The command **no web session security keylabel** *labelname* is disabled. Therefore all the HTTP requests will be redirected to HTTPS. Only the latest connection is retained and the remaining connections are logged out.

Examples

The following example generates a crypto key, and then associates it to HTTPS to enable HTTPS access to the Cisco Unified SIP Proxy GUI:

```
se-10-1-0-0#config t
se-10-1-0-0(config)# crypto key generate
Key generation in progress. Please wait
The label name for the key is mainkey.ourcompany
se-10-1-0-0(config)# web session security keylabel mainkey.ourcompany
```

The following example disables HTTPS on the session:

```
se-10-1-0-0(config)# no web session security keylabel mainkey.ourcompany
```

The following sample output indicates the behavior of Cisco Unified SIP Proxy 10.1, when trying to run the command **no web session security keylabel** *labelname*:

```
se-10-1-0-1(config)#no web session security keylabel mainkey.ourcompany
!!! INFO: HTTPS is the only web interface option for this version of vCUSP.
Hence, no web session security is disabled.
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.