



Cisco Unified SIP Proxy Security Commands

Last Updated: November 1, 2020

- [crypto key certreq](#)
- [crypto key label default](#)
- [crypto key delete](#)
- [crypto key generate](#)
- [show crypto key](#)

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 <i>label-name</i>	url {ftp: http:}
	Requests a CSR for the specified certificate-private key pair.	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-10-0-0-0(config)# crypto key certreq label XXXX url ftp:
se-10-0-0-0(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 <i>label-name</i>	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-10-0-0-0# configure terminal
se-10-0-0-0(config)# crypto key label mainkey.ourcompany default
se-10-0-0-0(config)#
```

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

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

■ crypto key label default

```
se-10-0-0-0(config)# no crypto key label alphakey.myoffice default
se-10-0-0-0(config)# crypto key label betakey.myoffice default
se-10-0-0-0(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 <i>label-name</i>	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-10-0-0-0# configure terminal
se-10-0-0-0(config)# crypto key delete label mainkey.ourcompany
se-10-0-0-0(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 <i>label-name</i>		(Optional) Assigns a name to the certificate-key pair.
modulus <i>modulus-size</i>		(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-10-0-0-0# configure terminal
se-10-0-0-0(config)# crypto key generate label mainkey.ourcompany modulus 750 default
se-10-0-0-0(config)#
```

Related Commands	Command	Description
	<code>crypto key certreq</code>	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
	<code>crypto key default</code>	Designates a certificate-private key pair as the system default.
	<code>crypto key delete</code>	Deletes a certificate-private key pair.
	<code>show crypto key</code>	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-10-0-0-0# 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.

■ show crypto key

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

■ show crypto key