



RSA and Certificate Commands

This chapter contains the following sections:

- [crypto key generate dsa, on page 2](#)
- [crypto key generate rsa, on page 3](#)
- [crypto key import, on page 4](#)
- [show crypto key, on page 6](#)
- [crypto certificate generate, on page 7](#)
- [crypto certificate request, on page 9](#)
- [crypto certificate import, on page 11](#)
- [show crypto certificate, on page 15](#)
- [show crypto certificate chain, on page 17](#)

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates a DSA key pair for SSH Public-Key authentication.

Syntax

crypto key generate dsa

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

The size of the created DSA key is 1024 bits

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

Example

The following example generates a DSA key pair.

```
switchxxxxx(config)# crypto key generate dsa  
The SSH service is generating a private DSA key.  
This may take a few minutes, depending on the key size.  
.....
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs for SSH Public-Key Authentication.

Syntax

crypto key generate rsa

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

The size of the created RSA key is 2048 bits

RSA keys are generated in pairs - one public RSA key and one private RSA key.

If the device already has RSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

Example

The following example generates RSA key pairs where a RSA key already exists.

```
switchxxxxxx(config)# crypto key generate rsa  
Replace Existing RSA Key [y/n]? N  
switchxxxxxx(config)#
```

crypto key import

The **crypto key import** Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

crypto key import {dsa|rsa}

encrypted crypto key import {dsa|rsa}

no crypto key {dsa|rsa}

Default Configuration

DSA and RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

The imported key must follow the format defined in RFC 4716

DSA key size for import is between 512 bits and 1024 bits

RSA key size for import is between 1024 bits and 2048 bits

DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

If the device already has DSA/RSA key keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is saved in the Running Configuration file.

When using the **encrypted** key-word, the private key is imported in its encrypted form.

Example

```
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
84et9C2XUfcrLpemUGINAYgnLwfkKJcDM6m2OReALHScqgLhi0wMSSYN1T1IWFZP1kEVHH
Fpt1aECZi7HfGLcp1pMZwjnl+HaXBtQjPdIEtbpScXqrg6ml1/OEnwpFK2TrmUy0Iifwk8
E/mMfX3i/2rRZLkEBea5jra6Q62gl5naRw1ZkOges+GNeibtvZYsk1jzr56LUR6ft7Xu5i
KMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrsId2MmjbExUdz
+RQRhzjzcGMBYp6HzkD66z8HmShOU+hKd7M1K9U4Sr+Pr1vyWUJ1EkOgz9O6aZoIGp4tgm4
VDy/K/G/sI5nVL0+bR8LFUXUO/U5hohBcyRUFO2fHYKZrhTiPT5Rw+PHt6/+EXKG9E+TRs
1UADmltCRvs+lsB33IBdvoRdd198YaA2htZay1TkbMqCUBdf10+74UOqa/b+bp67wCYKe9
yen418MaYktcHJBQmF7sUQZQP34VPmOMyZzon68S/ZoT77cy0ihRZx9wcIlyYhJnDiYxP
dgXHYhW6kCTcTj6LrUSQuxCJ9su89ZIWnN5OwdgonLSpvfnabv2GHmme1aveL7JJ/7UcfO
61q5D4PJ67Vvk2xL7PqyHXN931rseTzPuJplkSLCFZ5uqTMbWwYQEKmHD1Ox35v1Gou5tky
9LgIwG4d+9edctZzaggeq5cgjnsZWJgUoB4Bn4hIreyOdHdiFUPPRxkoYhGOGnJuvxC9T9
K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53WOT0Q1bHMTMLPppn2nXzvfGxWL/bu
QhZsSqrOnG6MX1cP7KT7i4TPq2w2k3TGtNBnVYHx6OoNcaTHmg1N2s5OgRsyXD9tF++6nY
```

```
RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr032HY+IpzZ4ujkK+/X5oawZL5NnkaEQTQKX
RSL55S4O5NPOjS/pC9hg7GaVjoY2mQ7HDpSUBeTIDTlvOwC2kskA9C6aF/Axj2dXLweQd5
lxk7m0/mMNaiJsNk6y33LcuKjIxpNNjK9n9KzRPkGNMFobprfenWKteDftjQ==
---- END SSH2 PRIVATE KEY ----
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMkymb+yWEp9042vupLvYVq3ngt1sB9JH
OcdK/2nw7lCQguylmLsX8/bKMXYSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8jLD+7
7t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRye9ifxT7otE=
---- END SSH2 PUBLIC KEY ----
```

show crypto key

The **show crypto key** Privileged EXEC mode command displays the device's SSH private and public keys for both default and user-defined keys.

Syntax

```
show crypto key [mypubkey] [dsa|rsa]
```

Parameters

- *mypubkey*—Displays only the public key.
- **rsa**—Displays the RSA key.
- **dsa**—Displays the DSA key.

Command Mode

Privileged EXEC mode

User Guidelines

See **Keys and Certificates** for information on how to display and copy this key pair.

Example

The following example displays the SSH public DSA keys on the device.

```
switchxxxxx# show crypto key mypubkey dsa
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAEAAzN31fu56KSEozdrGVPIJHpAs8G8NDIkB
dqZ2q0QPikCnLPw0Xsk9tTVKaHZQ5jJbXn81QZpolaPLJIH3B1cc96D7IFf
VkbPbMRbz24dpuWmFVVLULQy5nCKdDCui5KKVD6zj3gguhLhMJor7AjAAu5e
BrIi2IuwMVJuak5M098=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 6f:93:ca:01:89:6a:de:6e:ee:c5:18:82:b2:10:bc:1e
```

crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax

crypto certificate *number* **generate** [**key-generate** [*length*]] [**cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **key-generate** *rsa length*—Regenerates SSL RSA key and specifies the key length. (Supported lengths: 2048 (bits) or 3092 (bits))

The following elements can be associated with the key. When the key is displayed, they are also displayed.

cn *common- name*—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).

ou *organization-unit*—Specifies the organization-unit or department name. (Length: 1–64 characters)

or *organization*—Specifies the organization name. (Length: 1–64 characters)

loc *location*—Specifies the location or city name. (Length: 1–64 characters)

st *state*—Specifies the state or province name. (Length: 1–64 characters)

cu *country*—Specifies the country name. (Length: 2 characters)

duration *days*—Specifies the number of days a certification is valid. (Range: 30–1095)

Default Configuration

If the **key-generate** parameter is not used the certificate is generated using the existing key.

The default SSL's RSA key length is 2048.

The default SSL's EC key length is 256.

If **cn** *common- name* is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If **duration** *days* is not specified, it defaults to 730 days.

Command Mode

Global Configuration mode

User Guidelines

If the specific certificate key does not exist, you must use the parameter **key-generate**.

If both certificates 1 and 2 have been generated, use the **ip https certificate** command to activate one of them.

See **Keys and Certificates** for information on how to display and copy this key pair.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

Example

The following example generates a self-signed certificate for HTTPS whose key length is 2048 bytes.

```
switchxxxxx(config)# crypto certificate 1 generate key-generate 2048
```


crypto certificate request

The **crypto certificate request** Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax

crypto certificate *number* **request** [**cn** *common-name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*]

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
 - cn** *common-name*—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
 - ou** *organization-unit*—Specifies the organization-unit or department name. (Length: 1–64 characters)
 - or** *organization*—Specifies the organization name. (Length: 1–64 characters)
 - loc** *location*—Specifies the location or city name. (Length: 1–64 characters)
 - st** *state*—Specifies the state or province name. (Length: 1–64 characters)
 - cu** *country*—Specifies the country name. (Length: 2 characters)

Default Configuration

If **cn common-name** is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the **crypto certificate generate** command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example

The following example displays the certificate request for HTTPS.

```
switchxxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXCzAJBgNVBAGTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDeKb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAQIMA0GCSqGSIb3DQEBAQUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIw18ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
```

crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the relevant key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

Syntax

crypto certificate *number* **import**

encrypted crypto certificate *number* **import**

no crypto certificate *number*

Parameters

- *number*—Specifies the certificate number. (Range: 1–2).

Command Mode

Global Configuration mode

User Guidelines

Certificate needs to be imported from PEM encoding/file extension

To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** command.

If only the certificate is imported, and the public key found in the certificate does not match the device's SSL key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported key, the command fails.

This command is saved in the Running configuration file.

When using the encrypted form of the command, only the private key must be in encrypted format.

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input, and press
Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEWlgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MjQwCAQYDVQQKEWVQowCAQYDVQQLEWVg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
Oog9XMlAxfOiqLlQJHd4xP+BHGZWwfKjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5s041v0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQinJst6hI
XFDxe7I8Od3Uyt3DmF7KE/AmUV0Pif2yU1uy/RuxRwKhDp/1GrKl2tzLQz+s50x7
Klft/IcjzBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
.
-----END CERTIFICATE-----
```

```
Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

Example 2: The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input, and press
Enter.

-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGLXkwxBuZU1AO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLULJujM9p1IXFpMk8qR3NS7Jz1InYAWjHKkBEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvMq6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tgUoOAgL0b/C
11EoqzPcQ5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFOAa0N+y+2NwoGp0pxOvDA9ENY17qsZ
MwMcFXu52/Ix7FD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIU56uTzhhW
dKWwC0e/vwMgPtLlWyxWynnaP0fAJ+PawOadsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhpqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYmewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOUiQaMnhYf+RyPXhPOqs01PpIPhKBGTi6pj39XMvixRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnrUJAYXSLhjApf5iIQR1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpCbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYSK70ps8u7BtgpRfSRUr7g0LfhzhMuswoDSnB65pkc
ql7yZnBeRS0zrUDgHLRFzjwmXjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHA0GBAMVuFgfJYlBuzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitsfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFbYNmbzHc7a+7043wfVmh+QOXf
TbnRDhIMVrZJGbz1lc9IzGky1l21XmicY0/nwsXDAgEj
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIqIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBBQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
O0g9XM1Axf0iQLlQJHd4xP+BHGZwWfKjKjUDbPzn52LxdDulKrpE/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/halpYxp7EWat5iDBzSw5s04lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABAAAwDQYJKoZIhvcNAQEEBQADgYEAAuqYQINJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvIh45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0nlfXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

Example 3 - Import certificate with encrypted key

```
switchxxxxxx(config)# encrypted crypto certificate 1 import
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWm5mnjUhUaJlMM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6PxlV6cKvYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgovQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRUwEQoapMo0Py2Cvy+sqLlv4ZKck1FP1sVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDncqTyvUpffFEJYrdGKGyBqd0o3tD/ioUQ3UJgxDbGyW
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4Hda6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqThyETxgQKNERl07gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYQww2R0nAqnZsZPgrDzj0zTDL8qvykurfw4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAkvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBxa2VmbInutuP
```

```

CZM927oxkb41g+U5oYQxGhMK70EzTmfS1FdLomfqv0DHZNR41t4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvePljWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwpjHPbJkiCmDjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0srxvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgyWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABzdTPqz017FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jptLMWFgVf9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRXLahkiF7DZhrE7udOmtiP9
W3PqtJzbtjvMjm5/C+hoC6oLNP6qp0TE78EdfaHpmMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdZ55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPGWeDhw3q5QkaqInzzlh7j2+A++mwCsHui1BhpFNfY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMT0eO+Qsbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCAYUCEFCcI4/dhLsUhtWxOwbzngMwDQYJKoZIhvcNAQEEBQAwtzELMAkG
AlUEBhMCIcAxCjAIBgNVBAGTASAxCjAIBgNVBACjAIBgNVBACjAIBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQGEwIgdEKMAGGA1UECBMBIDEKMAgGA1UEBxBM
IDEQMA4GA1UEAxMHMC4wLjAxUmMDEKMAgGA1UEChMBIDEKMAgGA1UECzMBIDCBzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyGJor5v2FOCVMR5a3PnkWhbBXyZniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoiF
PWHuPb4D76bAKwe6LUGGkUOVj+CYQ2Iar1+m66Ryeh08E2/PvPdU7G/qHDVQcxM5
475BJt7tbUCAwEAATANBgkqhkiG9w0BAQQFAAOBQOktZas7HniIHMPeC5yC0
2rd7c+zqOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfasYe
dkB/761PpeKkUtgyPHfTzFSMcJdBOPpnpQcqbxCfH9QSN4ENSXqC5pND02RHXFx
wS1XJGrhMUoNgz1BY5DJWw==
-----END CERTIFICATE-----

```

```

Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788

```

```

Example 3 - Import certificate with encrypted key
encrypted crypto certificate 1 import

```

```

-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkT15C+SFOeSyTnxSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
aDQwgWM5mnjUhUaJlMM3WfrApY7HaBL3iSXS9jDvrf++Q/KKhVH6Pxlv6cKvYyzHg43Unm
CNl2n5zf9oisMH0U6gsIDs4yswVD1zNgovQwD7RqKpL9wo3+YVfV86XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuWQoapMo0Py2Cvy+sqLiv4ZKck1FP1svFV7X7sh+zVa3
We84pmzYjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJYrdGKGybgD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMyiWkdPjfcbn5MVRdu5iApCQJXWv3MYC8GQ4Hda6UDN6aoUBalUhgqT+RwW0
DXpJmvmX4T/u5W4DPvELqThyETxgQKNERl07gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6YOQwW2R0nAqnZsZPgRdzj0zTDL8qvykurfw4jWa4cv1Sc1hDEfTHH7NdLjQ
FkPFNAkvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK70EzTmfS1FdLomfqv0DHZNR41t4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvePljWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwpjHPbJkiCmDjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0srxvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgyWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABzdTPqz017FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jptLMWFgVf9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRXLahkiF7DZhrE7udOmtiP9
W3PqtJzbtjvMjm5/C+hoC6oLNP6qp0TE78EdfaHpmMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdZ55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPGWeDhw3q5QkaqInzzlh7j2+A++mwCsHui1BhpFNfY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMT0eO+Qsbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCAYUCEFCcI4/dhLsUhtWxOwbzngMwDQYJKoZIhvcNAQEEBQAwtzELMAkG
AlUEBhMCIcAxCjAIBgNVBAGTASAxCjAIBgNVBACjAIBgNVBACjAIBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQGEwIgdEKMAGGA1UECBMBIDEKMAgGA1UEBxBM
IDEQMA4GA1UEAxMHMC4wLjAxUmMDEKMAgGA1UEChMBIDEKMAgGA1UECzMBIDCBzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyGJor5v2FOCVMR5a3PnkWhbBXyZniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoiF
PWHuPb4D76bAKwe6LUGGkUOVj+CYQ2Iar1+m66Ryeh08E2/PvPdU7G/qHDVQcxM5
475BJt7tbUCAwEAATANBgkqhkiG9w0BAQQFAAOBQOktZas7HniIHMPeC5yC0
2rd7c+zqOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfasYe
dkB/761PpeKkUtgyPHfTzFSMcJdBOPpnpQcqbxCfH9QSN4ENSXqC5pND02RHXFx
wS1XJGrhMUoNgz1BY5DJWw==
-----END CERTIFICATE-----

```

```
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BggkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAYgJor5v2FOCvMR5aN3PnkWhbBXyZniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTonlySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iarl+m66Ryeh08E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQB0knTzas7HniIHMpEC5yC0
2rd7c+zqQOe1e4CpEvVlOC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPpnpQcqbxCfh9QSN44ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

show crypto certificate

The **show crypto certificate** Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

Syntax

```
show crypto certificate [mycertificate] [number]
```

Parameters

- **number**—Specifies the certificate number. (Range: 1,2)
- **mycertificate**—Specifies that only the certificate will be displayed

Default Configuration

displays both keys.

Command Mode

Privileged EXEC mode

Examples

The following example displays SSL certificate # 1 present on the device and the key-pair.

```
switchxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t1a1GaqchfMqqe0kmfhcoHSWr
yflFpDOMWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEWEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASKwgdkGgc+ggcyGgclsZGFwOi8v
L0VByb3h5JTJwU29mdHdhcmU1MjBSb290JTJwQ2VydG1maWVyLENOPXNlcnZl
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGLXkwxBuZU1AO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLULJujM9p1IXFpMk8qr3NS7Jz1InYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11Eoqzpcq5mT7+vOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENY17qsZ
MwMcfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWwC0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGK1jhPqLHuzXHUon7Zx15CUTp3sbH1+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34a1VJaN+2AMCb0hpI3IkreYo
A8Lk6UMOUiQaMnhYf+RyPXhPOqs01PpIPhKBGTi6pj39XMviyRXvSpn5+eIYPhe5jYaEn
UeOnVZRhNCVnrUJAYXSLhjApf5iIQR1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
q17yZnBeRS0zrUDgHLLRfzjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLBuzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFbYNmbzHc7a+7043wfVmH+QOXf
TbnRdHIMVrZJGbz11c9IzGky1121XmicY0/nwsXDAgEj
```

```
-----END RSA PUBLIC KEY-----  
Issued by: www.verisign.com  
Valid from: 8/9/2003 to 8/9/2004  
Subject: CN= router.gm.com, O= General Motors, C= US  
Finger print: DC789788 DC88A988 127897BC BB789788
```


show crypto certificate chain

The show crypto certificate chain Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

Syntax

show crypto certificate chain [*number*]

Parameters

- *number* (optional)—Specifies the certificate number. (Range: 1,2)

Default Configuration

Displays both keys.

Command Mode

Privileged EXEC mode

Examples

The following example displays certificate 1 chain:

```
switchxxxxx# show crypto certificate chain 1
```

```
Certificate Chain - server certificate 1 (Active)
```

```
=====
Sever Certificate
Status: valid
Serial Number:
00:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:11
Issuer: cn=Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US
Subject: cn= momo.company.com, ou=Depd, o=myCompany, st=NA, c=US
Validity:
Not Before: Nov 14 21:06:28 2023 EST
Not After: Nov 09 21:06:28 2043 SET
Intermediate CA Certificate – Inter2
Status: valid
Serial Number: 55:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:55
Issuer: cn= My Root CA, ou=RootIss, o=MyRootCA, st=NA, c=US
Subject: cn= Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US
```

show crypto certificate chain

Validity:

Not Before: Nov 14 21:06:28 2023 EST

Not After: Nov 09 21:06:28 2043 EST