

CA Certificate Commands

This chapter contains the following sections:

- ca-certificate install, on page 2
- ca-certificate revoke, on page 4
- show ca-certificate, on page 5
- show ca-certificate revocation, on page 7

ca-certificate install

To manually install a CA certificate, use the **ca-certificate install** command in Global Configuration mode. To remove a static CA certificate, use the **no** form of this command.

Syntax

ca-certificate install name *name* [**owner** owner]

no ca-certificate install {**name** *name* | **owner** *owner*}

Parameters

- **intermediate** (optional) - install and validate the certificate as an intermediatecertificate.
- ***name***—Specifies the certificate name. The range is from 1 to 160 characters.
- ***owner***—specifies the owner of the certificate. This is a string of 1 to 32 characters. If an owner is not specified, the default owner is "Static".

When adding a certificate, the certificate itself should follow the command on the command line.

Default Configuration

There are no installed certificates.

Command Mode

Global Configuration mode

User Guidelines

Use the **ca-certificate install** *name* command to install a CA certificate.

Installing a certificate without the optional intermediate keyword, indicates that the installed certificate is a root CA certificate. Certificate will be installed only after validating the certificate as a root CA certificate.

Installing a certificate including the optional intermediate keyword, indicates that the installed certificate is an intermediate CA certificate. Certificate will be installed only after validating the certificate as an intermediate CA certificate.

The name parameter - cannot include the "/" (forward slash) character. the owner parameter cannot include the "/" (forward slash) and the "_" (underscore) characters.

Following the command, the user will be prompted to enter the certificate in the command line.

The user will need to enter or paste the certificate. Entering a period on a separate line indicates that the certificate input is complete.

The entered certificate must use the pem format.

A certificate will not be valid if the system clock was not set by user or synchronized with

SNTP, or based on hardware based Real Time Clock (RTC).

Up to 256 certificates can be installed.

When using the no form of the command to remove certificates, a specific certificate can be removed by name. Alternatively, the owner keyword can be used to remove all static certificates belonging to a specific owner.

Example 1. The following example installs a CA certificate from the command line:

```
switchxxxxxx(config)# ca-certificate install root1
Please paste the input now, add a period (.) on a separate line after the
input,and press Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE-----
switchxxxxxx(config)#
```

ca-certificate revoke

To add a certificate to the revocation list, use the **ca-certificate revoke** command in Global Configuration mode. To remove a certificate from the revocation list, use the **no** form of this command.

Syntax

ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

no ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

Parameters

- ***issuer***—The issuer string as it appears in the revoked certificate - including all parameters (Range: 1-160 characters).
- ***serial-number***—The serial number of the revoked certificate. This is a string in hexadecimal format (Range: 1-32 pairs of characters).

Default Configuration

There are no revoked certificates.

Command Mode

Global Configuration mode

User Guidelines

Use the **ca-certificate revoke** command to add a certificate to the revocation list.

When entering the issuer information, the full issuer string should be entered as it appears in the certificate. If the string contains spaces, it must be contained in quotation marks.

Adding a certificate to this list will change the status of this certificate to "revoked" if it is installed. If the certificate is not installed, it will receive the revoked status if it is installed at a later date.

Up to 512 certificates can be added to the revocation list.

Example 1. The following example adds a CA certificate to the revocation list:

```
switchxxxxxx(config)# ca-certificate revoke issuer "C=US, O=GlobalSign nv-sa, CN=GlobalSign
 Organization Validation" serial-number 10ad0044a8418ad5005e45b6
switchxxxxxx(config)#
```

show ca-certificate

To display the CA certificates installed on the device and their status, use the **show ca-certificate** command in Privileged EXEC mode.

Syntax

show ca-certificate [name *name*][type *type*][owner *owner-name*][detailed]

Parameters

- **name** *name* - Specifies the certificate name. (Range: 1-160 characters).
- **type** *type*—Specifies the certificate type. The possible values are static, dynamic or signer.
- **owner** *owner-name*—Specifies the name of the certificate owner - this is the application that installed a dynamic certificate. (Range: 1-32 characters).
- **detailed** - This optional parameter shows detailed information of the displayed certificates. If this parameter is not used, only limited information will be displayed for each certificate.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show ca-certificate** command to display all installed CA certificates.

Use the optional **name, type** and **owner** parameters to display the information of a subset of certificates.

Example 1 The following example displays brief information for all static CA certificates.

```
switchxxxxxx# show ca-certificate type static
Name           Type    Owner     Valid From   Valid To     Status
-------------  ------  --------  -----------  -----------  ----------
local.cert     static  rnd       03-Aug-2019  03-Aug-2020  Valid
app1.cert1     static  app1      16-Jan-2021  16-Jul-2023  Premature
app1.cert2     static  app1      15-Mar-2017  14-Mar-2018  Expired
trusted-cert1  static  app2      27-Jun-2019  26-Jun-2024  Valid
certif3        static  app3      08-Feb-2018  08-Feb-2020  Revoked
```

Example 2 The following example displays detailed information for all CA certificates:

```
switchxxxxxx# show ca-certificate detailed
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
cert1
  Type: Signer
  Owner: N/A
  Version: 3 (0x2)
  Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Status: Valid
  Validity
    Not Before: Nov 21 08:00:00 2015 GMT
    Not After : Nov 22 07:59:59 2020 GMT
  Subject: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
```

```
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
   Signature Algorithm: sha256RSA
certA
 Type: Static
 Owner: Static
 Parent: cert1
 Version: 3 (0x2)
 Serial Number: 10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
 Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
 Status: Not Valid (expired)
 Validity
   Not Before: Nov 21 08:00:00 2016 GMT
   Not After : Nov 22 07:59:59 2017 GMT
 Subject: C=US, ST=California, L=San Francisco, O=AKB Foundation, Inc.,
          CN=*.wikipedia.org
 Finger print: DC72343 DC88A988 127897BC BB789788
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
   Signature Algorithm: sha256RSA
 certB
 Type: Dynamic
 Owner: PnP
 Parent: cert1
 Version: 3 (0x2)
 Serial Number: 88:cc:55:ae:a8:41:8a:d5:00:5e:45:b6
 Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
 Status: Not Valid (revoked)
 Validity
   Not Before: Sep 21 08:00:00 2019 GMT
   Not After : Sep 22 07:59:59 2020 GMT
 Subject: C=US, S=California, L=Mountain View O=Google LLC, CN=*.google.com
 Finger print: DC789788 DC88A988 127897BC BB789788
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
 Signature Algorithm: sha256RSA
```

show ca-certificate revocation

To display the CA certificate revocation list, use the **show ca-certificate revocation** command in Privileged EXEC mode.

Syntax

show ca-certificate revocation

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show ca-certificate revocation** command to display the CA certificate revocation list.

Example. The following displays the revocation list:

```
switchxxxxxx# show ca-certificate revocation
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
-------------------------------------------------------------------------
  Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
  Serial Number: 00:9e:44:1b:49:08:8d:75:bb:02:00:00:00:00:40:a5:b4
```