

Contents

PKI commands	1
attribute.....	1
ca identifier	2
certificate request entity.....	3
certificate request from	4
certificate request mode.....	4
certificate request polling	6
certificate request url.....	7
common-name.....	7
country.....	8
crl check.....	9
crl url	9
display pki certificate access-control-policy	10
display pki certificate attribute-group.....	11
display pki certificate domain	12
display pki certificate renew-status	17
display pki certificate request-status	18
display pki crl domain.....	20
fqdn.....	22
ip	22
ldap-server.....	23
locality	24
organization	24
organization-unit	25
pki abort-certificate-request	25
pki certificate access-control-policy	26
pki certificate attribute-group.....	27
pki delete-certificate.....	28
pki domain	29
pki entity.....	30
pki export.....	31
pki import.....	37
pki request-certificate	42
pki retrieve-certificate	43
pki retrieve-crl.....	44
pki storage.....	45
pki validate-certificate.....	46
public-key dsa	48
public-key ecdsa	49
public-key rsa	50
root-certificate fingerprint	52
rule.....	53
source.....	54
state	55
subject-dn.....	55
usage	56

PKI commands

attribute

Use **attribute** to configure a rule to filter certificates based on an attribute in the certificate issuer name, subject name, or alternative subject name field.

Use **undo attribute** to remove an attribute rule.

Syntax

```
attribute id { alt-subject-name { fqdn | ip } | { issuer-name | subject-name } { dn | fqdn | ip } } { ctn | equ | nctn | nequ } attribute-value
```

```
undo attribute id
```

Default

No attribute rules exist.

Views

Certificate attribute group view

Predefined user roles

network-admin

Parameters

id: Specifies a rule ID in the range of 1 to 16.

alt-subject-name: Specifies the alternative subject name.

fqdn: Specifies an FQDN of the PKI entity.

ip: Specifies an IP address of the PKI entity.

dn: Specifies the DN of the PKI entity.

issuer-name: Specifies the issuer name.

subject-name: Specifies the subject name.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Sets an attribute value, a case-insensitive string of 1 to 128 characters.

Usage guidelines

The issuer name, subject name, and alternative subject name field can contain the following attributes in a certificate:

- Each subject name and the issuer name can contain a single DN, multiple FQDNs, and multiple IP addresses.
- The alternative subject name can contain multiple FQDNs and IP addresses but zero DNs.

An attribute rule is a combination of an attribute-value pair with an operation keyword, as listed in [Table 1](#).

Table 1 Combinations of attribute-value pairs and operation keywords

Operation	DN	FQDN/IP
ctn	The DN contains the specified attribute value.	Any FQDN or IP address contains the specified attribute value.
nctn	The DN does not contain the specified attribute value.	None of the FQDNs or IP addresses contain the specified attribute value.
equ	The DN is the same as the specified attribute value.	Any FQDN or IP address is the same as the specified attribute value.
nequ	The DN is not the same as the specified attribute value.	None of the FQDNs or IP addresses are the same as the specified attribute value.

A certificate matches an attribute rule only if it contains an attribute that matches the criterion defined in the rule. For example, an attribute rule defines a criterion that the DN of the subject name contains the **abc** string. All certificates that have the DN in the subject name containing the **abc** string match the rule.

A certificate matches an attribute group if it matches all attribute rules in the group.

Examples

Create a certificate attribute group and enter its view.

```
<Sysname> system-view
```

```
[Sysname] pki certificate attribute-group mygroup
```

Specify an attribute rule to match certificates that contain the **abc** string in the subject DN.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

Specify an attribute rule to match certificates that do not contain FQDN **abc** in the issuer name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

Specify an attribute rule to match certificates that do not contain IP address **10.0.0.1** in the alternative subject name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

Related commands

- **display pki certificate attribute-group**
- **rule**

ca identifier

Use **ca identifier** to specify the trusted CA.

Use **undo ca identifier** to restore the default.

Syntax

ca identifier *name*

undo ca identifier

Default

No trusted CA is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name: Specifies the trusted CA by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To obtain a CA certificate, you must specify the trusted CA name. The trusted CA name uniquely identifies the CA to be used if multiple CAs exist on the same CA server. The CA server's URL is specified by using the **certificate request url** command.

When you use this command, make sure the specified CA name is consistent with the name of the CA that owns the CA certificate to be obtained.

Examples

```
# Specify the name of the trusted CA as new-ca.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

certificate request entity

Use **certificate request entity** to specify the PKI entity for certificate request.

Use **undo certificate request entity** to restore the default.

Syntax

certificate request entity *entity-name*

undo certificate request entity

Default

No PKI entity is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a PKI entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity describes the identity attributes of an entity for certificate request, including the following information:

- Common name.
- Organization.
- Unit in the organization.
- Locality.
- State and country where the entity resides.
- FQDN.
- IP address.

You can specify only one PKI entity for a PKI domain. If you configure this command for a PKI domain multiple times, the most recent configuration takes effect.

Examples

```
# Specify PKI entity en1 for certificate request in PKI domain aaa.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request entity en1
```

Related commands

pki entity

certificate request from

Use **certificate request from** to specify the type of certificate request reception authority.

Use **undo certificate request from** to restore the default.

Syntax

```
certificate request from { ca | ra }
undo certificate request from
```

Default

The type of certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ca: Specifies the CA to accept certificate requests.

ra: Specifies the RA to accept certificate requests.

Usage guidelines

The CA server determines whether CA or RA accepts certificate requests. This authority setting must be consistent with the setting on the CA server.

Examples

```
# Specify the RA to accept certificate requests.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request from ra
```

certificate request mode

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

Syntax

```
certificate request mode { auto [ password { cipher | simple } string | renew-before-expire days ] reuse-public-key ] [ automatic-append common-name ] ] * | manual }
```

undo certificate request mode

Default

The certificate request mode is manual.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto certificate request mode.

password: Specifies a password for certificate revocation as required by the CA policy.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

renew-before-expire days: Configures the system to automatically request a new certificate the specified number of days before the current certificate expires. The value range for the *days* argument is 0 to 365. Value 0 indicates that the request for a new certificate is made when the old certificate expires, which might cause service interruptions.

reuse-public-key: Reuses the key pair in the old certificate for the new certificate. If you do not specify this keyword, the system generates a new key pair for the new certificate. The old key pair is replaced with the new one when the new certificate is received from the CA.

automatic-append common-name: Automatically appends random data to the common name of the PKI entity for the new certificate. If you do not specify this keyword, the common name of the PKI entity will be unchanged in the new certificate.

manual: Specifies the manual certificate request mode.

Usage guidelines

A certificate request can be submitted to a CA in offline or online mode. In online mode, a certificate request can be automatically or manually submitted:

- **Auto request mode**—A PKI entity automatically obtains the CA certificate and submits a certificate request to the CA when both of the following conditions exist:
 - An associated application (IKE, for example) performs identity authentication.
 - No certificate is available for the application on the device.
- **Manual request mode**—You must manually obtain the CA certificate and submit certificate requests.

To avoid service interruptions caused by certificate expiration, specify the **renew-before-expire days** option to enable certificate auto-renewal in auto certificate request mode. Certificate auto-renewal allows the system to automatically request a new certificate the specified number of days before the old certificate expires. The old certificate is replaced immediately when the new certificate is received.

Some CAs require a new PKI entity common name for certificate auto-renewal to work. Specify the **automatic-append common-name** keyword to ensure successful certificate auto-renewal.

Examples

```
# Set the certificate request mode to auto.
```

```
<Sysname> system-view
```

```

[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto

# Set the certificate request mode to auto, and set the certificate revocation password in plain text to
123456.

<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456

# Set the certificate request mode to auto, and set the certificate revocation password in plain text to
123456. Configure the system to automatically request a new certificate by using a new key pair 60
days before the old certificate expires.

<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
renew-before-expire 60

```

Related commands

pki request-certificate

certificate request polling

Use **certificate request polling** to set the polling interval and the maximum number of attempts to query certificate request status.

Use **undo certificate request polling** to restore the defaults.

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

Default

The polling interval is 20 minutes, and the maximum number of attempts is 50.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

count *count*: Specifies the maximum number of attempts to query certificate request status. The value range is 1 to 100.

interval *interval*: Specifies a polling interval in minutes. The value range is 5 to 168..

Usage guidelines

After a PKI entity submits a certificate request, it might take the CA server a while to issue the certificate if the CA administrator manually approves the certificate request. During this period, the PKI entity periodically queries the CA server for the certificate request status. The periodic query operation stops until the PKI entity obtains the certificate or the maximum number of query attempts is reached. If the maximum number of query attempts is reached, the certificate request fails.

If the CA server automatically approves a certificate request, the PKI entity can obtain the certificate immediately after it submits a certificate request. In this case, the PKI entity does not send queries to the CA server.

Examples

```
# Set the polling interval to 15 minutes, and the maximum number of query attempts to 40.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request polling interval 15
[Sysname-pki-domain-aaa] certificate request polling count 40
```

Related commands

display pki certificate request-status

certificate request url

Use **certificate request url** to specify the URL of the certificate request reception authority (CA or RA) to which the device should send SCEP certificate requests.

Use **undo certificate request url** to restore the default.

Syntax

certificate request url *url-string*

undo certificate request url

Default

The URL of the certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the certificate request reception authority, a case-sensitive string of 1 to 511 characters. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

The URL is in the format `http://server_location/ca_script_location`, where:

- The *server_location* argument is the IPv4 address, IPv6 address, or domain name of the certificate request reception authority (CA or RA) server.
- The *cgi_script_location* argument is the path of the application script on the server.

Examples

```
# Set the certificate request URL to http://169.254.0.1/certsrv/mscep/mscep.dll.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request url
http://169.254.0.1/certsrv/mscep/mscep.dll
```

common-name

Use **common-name** to set the common name for a PKI entity.

Use **undo common-name** to restore the default.

Syntax

common-name *common-name-string*

undo common-name

Default

No common name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

common-name-string: Specifies a common name, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set the username of the PKI entity as the common name.

Examples

Set the common name to **test** for the PKI entity **en**.

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] common-name test
```

country

Use **country** to set the country code of a PKI entity.

Use **undo country** to remove the configuration.

Syntax

country *country-code-string*

undo country

Default

No country code is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

country-code-string: Specifies a country code, a case-sensitive string of two characters. For example, CN is the country code for China.

Examples

Set the country code to **CN** for PKI entity **en**.

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] country CN
```

crl check

Use **crl check enable** to enable CRL checking.

Use **undo crl check enable** to disable CRL checking.

Syntax

crl check enable

undo crl check enable

Default

CRL checking is enabled.

Views

PKI domain view

Predefined user roles

network-admin

Usage guidelines

A CRL is a list of revoked certificates signed and published by a CA. Revoked certificates should no longer be trusted.

CRL checking is designed to check whether a certificate has been revoked.

Examples

```
# Disable CRL checking.  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] undo crl check enable
```

Related commands

- **pki import**
- **pki retrieve-certificate**
- **pki validate-certificate**

crl url

Use **crl url** to specify the URL of the CRL repository.

Use **undo crl url** to restore the default.

Syntax

crl url *url-string*

undo crl url

Default

The URL of the CRL repository is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the CRL repository, a case-sensitive string of 1 to 511 characters. The URL format is `ldap://server_location` or `http://server_location`, where *server_location* can be an IP address or a domain name. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

To use CRL checking, a CRL must be obtained from a CRL repository.

The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

After the previous selection process, if the CRL repository is not found, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

If an LDAP URL is specified, the device must connect to the LDAP server to obtain the CRL. If the LDAP server's host name is not included in the URL, the device can get the complete URL information based on the LDAP server address specified in the PKI domain.

Examples

```
# Set the URL of the CRL repository to http://169.254.0.30.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

Related commands

- **ldap-server**
- **pki retrieve-crl**

display pki certificate access-control-policy

Use **display pki certificate access-control-policy** to display information about certificate-based access control policies.

Syntax

```
display pki certificate access-control-policy [ policy-name ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a policy name, this command displays information about all certificate-based access control policies.

Examples

Display information about the certificate-based access control policy **mypolicy**.

```
<Sysname> display pki certificate access-control-policy mypolicy
Access control policy name: mypolicy
  Rule 1 deny    mygroup1
  Rule 2 permit  mygroup2
```

Display information about all certificate-based access control policies.

```
<Sysname> display pki certificate access-control-policy
Total PKI certificate access control policies: 2
Access control policy name: mypolicy1
  Rule 1 deny    mygroup1
  Rule 2 permit  mygroup2
Access control policy name: mypolicy2
  Rule 1 deny    mygroup3
  Rule 2 permit  mygroup4
```

Table 2 Command output

Field	Description
Total PKI certificate access control policies	Total number of certificate-based access control policies.
permit	Permit certificates that match the attribute group in the access control rule.
deny	Deny certificates that match the attribute group in the access control rule.

Related commands

- **pki certificate access-control-policy**
- **rule**

display pki certificate attribute-group

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Syntax

```
display pki certificate attribute-group [ group-name ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a certificate attribute group, this command displays information about all certificate attribute groups.

Examples

Display information about the certificate attribute group **mygroup**.

```
<Sysname> display pki certificate attribute-group mygroup
Attribute group name: mygroup
  Attribute 1 subject-name    dn    ctn    abc
  Attribute 2 issuer-name    fqdn  nctn  app
```

Display information about all certificate attribute groups.

```
<Sysname> display pki certificate attribute-group
Total PKI certificate attribute groups: 2.
Attribute group name: mygroup1
  Attribute 1 subject-name    dn    ctn    abc
  Attribute 2 issuer-name    fqdn  nctn  app
Attribute group name: mygroup2
  Attribute 1 subject-name    dn    ctn    def
  Attribute 2 issuer-name    fqdn  nctn  fqd
```

Table 3 Command output

Field	Description
Total PKI certificate attribute groups	Total number of certificate attribute groups.
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.
Attribute 1 subject-name dn ctn abc	Attribute rule contents: <ul style="list-style-type: none">• alt-subject-name—Alternative subject name.• issuer-name—Certificate issuer name.• subject-name—Certificate subject name.• fqdn—FQDN of the PKI entity.• ip—IP address of the PKI entity.• dn—DN of the PKI entity.• ctn—Indicates the contain operation.• equ—Indicates the equal operation.• nctn—Indicates the not-contain operation.• nequ—Indicates the not-equal operation.

Related commands

- **attribute**
- **pki certificate attribute-group**

display pki certificate domain

Use **display pki certificate domain** to display information about certificates.

Syntax

```
display pki certificate domain domain-name { ca | local | peer [ serial serial-num ] }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 4](#).

Table 4 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies the serial number of a peer certificate.

Usage guidelines

If you specify the **CA** keyword, this command displays information about all CA certificates in the domain. If the domain has RA certificates, the RA certificates are also displayed.

If you specify the **local** keyword, this command displays information about all local certificates in the domain.

If you specify the **peer** keyword without a serial number, this command displays brief information about all peer certificates. If you specify a serial number, this command displays detailed information about the specified peer certificate.

Examples

Display information about the CA certificate in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa ca
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=cn, O=docm, OU=rnd, CN=rootca
    Validity
      Not Before: Jan  6 02:51:41 2011 GMT
      Not After : Dec  7 03:12:05 2013 GMT
    Subject: C=cn, O=ccc, OU=ppp, CN=rootca
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
```

```
00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
52:db:7b:cd:5d:2b:66:5a:fb
```

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

```
6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
88:a6
```

Display information about local certificates in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa local
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

```
bc:05:70:1f:0e:da:0d:10:16:1e
```

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=CN, O=sec, OU=software, CN=ipsec

Validity

Not Before: Jan 7 20:05:44 2011 GMT

Not After : Jan 7 20:05:44 2012 GMT

Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

```
00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
8a:f0:ea:02:fd:2d:44:7a:67
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

```

CA:FALSE
Netscape Cert Type:
  SSL Client, S/MIME
X509v3 Key Usage:
  Digital Signature, Non Repudiation, Key Encipherment
X509v3 Extended Key Usage:
  TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
Netscape Comment:
  User Certificate of OpenCA Labs
X509v3 Subject Key Identifier:
  91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
X509v3 Authority Key Identifier:
  keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

X509v3 Subject Alternative Name:
  email:fips@ccc.com
X509v3 Issuer Alternative Name:
  email:pki@openca.org
Authority Information Access:
  CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
  OCSP - URI:http://titan:2560/
  1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

X509v3 CRL Distribution Points:

  Full Name:
    URI:http://titan/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption
94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1

```

Display brief information about all peer certificates in the PKI domain aaa.

```

<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1

```

Serial Number: 9a0337eb2156balf5476e4d754a5a9f7

Subject Name: CN=sldsslserver

Display detailed information about a peer certificate in the PKI domain aaa.

<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156balf5476e4d754a5a9f7

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=ccc, OU=sec, CN=ssl

Validity

Not Before: Oct 15 01:23:06 2010 GMT

Not After : Jul 26 06:30:54 2012 GMT

Subject: CN=sldsslserver

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:

a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:

68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:

04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:

97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:

39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:

29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:

ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:

8b:a3:4d:b2:17:08:8d:dd:81

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment,

Key Agreement

Netscape Cert Type:

SSL Server

X509v3 Subject Alternative Name:

DNS:docm.com

X509v3 Subject Key Identifier:

3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26

X509v3 CRL Distribution Points:

Full Name:

URI:http://s03130.ccc.sec.com:447/ssl.crl

```
Signature Algorithm: sha1WithRSAEncryption
61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
f0:a5
```

Related commands

- **pki domain**
- **pki retrieve-certificate**

display pki certificate renew-status

Use **display pki certificate renew-status** to display the certificate renewal status for a PKI domain.

Syntax

```
display pki certificate renew-status [ domain domain-name ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 5](#). If you do not specify a domain name, this command displays the certificate renewal status for all PKI domains.

Table 5 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Examples

```
# Display the certificate renewal status for all PKI domains.
<Sysname> display pki certificate renew-status
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
Key type: RSA
```

```

Time when key pair created: 15:40:48 2015/05/12
Key code:
 30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
 667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
 C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
 FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
 2DA4C04EF5AE0835090203010001

```

The command output indicates that the **reuse-public-key** keyword was not configured for PKI domain **domain1** and a new key pair was created for the new certificate.

Display the certificate renewal status for PKI domain **domain1**.

```

<Sysname> display pki certificate renew-status domain domain1
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2016-06-13
  Key code:
 30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
 667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
 C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
 FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
 2DA4C04EF5AE0835090203010001

```

Table 6 Command output

Field	Description
Renew Time	Time when a new certificate will be requested.
Renew public key	Information about the new key pair created for the certificate. The renew public key information is displayed only if the certificate renewal process is slow or has failed.
Key type	Key pair type, which can be RSA, DSA, or ECDSA.
Time when key pair created	Time when the key pair was created.
Key code	Public key data.

Related commands

certificate request mode
pki domain

display pki certificate request-status

Use **display pki certificate request-status** to display certificate request status.

Syntax

display pki certificate request-status [domain *domain-name*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 7](#).

Table 7 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

If you do not specify a PKI domain, this command displays the status of all certificate requests.

Examples

Display certificate request status for the PKI domain **aaa**.

```
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
  Domain name: aaa
  Status: Pending
  Key usage: General
  Remain polling attempts: 10
  Next polling attempt after : 1191 seconds
```

Display certificate request statuses for all PKI domains.

```
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
  Domain name: domain1
  Status: Pending
  Key usage: General
  Remain polling attempts: 10
  Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
  Domain name: domain2
  Status: Pending
  Key usage: Signature
  Remain polling attempts: 10
  Next polling attempt after : 188 seconds
```

Table 8 Command output

Field	Description
Certificate Request Transaction <i>number</i>	Certificate request transaction number, starting from 1.

Field	Description
Status	Certificate request status, including only the pending status.
Key usage	Certificate purposes: <ul style="list-style-type: none"> • General—Signature and encryption. • Signature—Signature only. • Encryption—Encryption only.
Remain polling attempts	Remaining number of attempts to query certificate request status.
Next polling attempt after	Remaining seconds before the next request status polling.

Related commands

- **certificate request polling**
- **pki domain**
- **pki retrieve-certificate**

display pki crl domain

Use **display pki crl domain** to display information about the locally saved CRLs.

Syntax

display pki crl domain *domain-name*

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 9](#).

Table 9 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

Use this command to check whether a certificate has been revoked.

Examples

Display information about the CRL saved at the local for PKI domain **aaa**.

```

<Sysname> display pki crl domain aaa
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /C=cn/O=docm/OU=sec/CN=therootca
  Last Update: Apr 28 01:42:13 2011 GMT
  Next Update: NONE
  CRL extensions:
    X509v3 CRL Number:
      6
    X509v3 Authority Key Identifier:
      keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
  Serial Number: CDE626BF7A44A727B25F9CD81475C004
  Revocation Date: Apr 28 01:37:52 2011 GMT
  CRL entry extensions:
    Invalidation Date:
      Apr 28 01:37:49 2011 GMT
  Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
  Revocation Date: Apr 28 01:33:28 2011 GMT
  CRL entry extensions:
    Invalidation Date:
      Apr 28 01:33:09 2011 GMT
  Signature Algorithm: sha1WithRSAEncryption
  57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
  5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
  36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
  99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
  8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
  4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
  52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
  ba:aa

```

Table 10 Command output

Field	Description
Version	CRL version number.
Signature Algorithm	Signature algorithm used by the CA to sign the CRL.
Issuer	Name of the CA that issued the CRL.
Last Update	Most recent CRL update time.
Next Update	Next CRL update time.
X509v3 Authority Key Identifier	X509v3 ID of the CA that issues the CRL.
keyid	Key ID. This field identifies the key pair used to sign the CRL.
Signature Algorithm:	Signature algorithm and signature data.

Related commands

pki retrieve-crl

fqdn

Use **fqdn** to set the FQDN of an entity.

Use **undo fqdn** to restore the default.

Syntax

fqdn *fqdn-name-string*

undo fqdn

Default

No FQDN is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

fqdn-name-string: Specifies an FQDN, a case-sensitive string of 1 to 255 characters in the format *hostname@domainname*.

Usage guidelines

An FQDN uniquely identifies a PKI entity on a network.

Examples

Set the FQDN to **pki.domain-name.com** for PKI entity **en**.

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

ip

Use **ip** to assign an IP address to a PKI entity.

Use **undo ip** to restore the default.

Syntax

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

Default

No IP address is assigned to the PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The primary IPv4 address of the interface will be used as the IP address of the PKI entity.

Usage guidelines

Use this command to assign an IP address to a PKI entity or specify an interface whose primary IP address will be used as the IP address for the PKI entity. If you specify an interface, make sure the interface has an IP address before the PKI entity requests a certificate.

Examples

Assign IP address **192.168.0.2** to PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

ldap-server

Use **ldap-server** to specify an LDAP server for a PKI domain.

Use **undo ldap-server** to restore the default.

Syntax

ldap-server host *hostname* [**port** *port-number*]

undo ldap-server

Default

No LDAP server is specified for a domain.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

host *hostname*: Specifies an LDAP server by its IPv4 address, IPv6 address, or domain name. The domain name is a case-sensitive string of 1 to 255 characters.

port *port-number*: Specifies the port number of the LDAP server. The value range is 1 to 65535, and the default is 389.

Usage guidelines

You must specify an LDAP server for a PKI domain in the following situations:

- An LDAP URL is specified in the PKI domain (by using the **url** command).
- The specified LDAP URL does not contain the IP address or host name of the LDAP server.

You can specify only one LDAP server for a PKI domain. If you configure this command multiple times, the most recent configuration takes effect.

Examples

Specify LDAP server **10.0.0.1** for PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

```
# Specify LDAP server 10.0.0.11 and set the port number to 333.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.11 port 333
```

Related commands

- **pki retrieve-certificate**
- **pki retrieve-crl**

locality

Use **locality** to set the locality of a PKI entity.

Use **undo locality** to restore the default.

Syntax

locality *locality-name*

undo locality

Default

No locality is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

locality-name: Specifies a locality, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set a city name as the locality.

Examples

```
# Set the locality to pukras for PKI entity en.
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] locality pukras
```

organization

Use **organization** to set an organization name for a PKI entity.

Use **undo organization** to restore the default.

Syntax

organization *org-name*

undo organization

Default

No organization name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-name: Specifies an organization name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

```
# Set the organization name to abc for PKI entity en.
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization abc
```

organization-unit

Use **organization-unit** to set an organization unit name for a PKI entity.

Use **undo organization-unit** to restore the default.

Syntax

```
organization-unit org-unit-name
undo organization-unit
```

Default

No organization unit name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-unit-name: Specifies an organization unit name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

```
# Set the organization unit name to rdtest for PKI entity en.
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization-unit rdtest
```

pki abort-certificate-request

Use **pki abort-certificate-request** to abort the certificate request for a PKI domain.

Syntax

```
pki abort-certificate-request domain domain-name
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 11](#).

Table 11 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

You can abort a certificate request and change some parameters, such as common name, country code, or FQDN, in the certificate request before the CA issues the certificate. Use the **display pki certificate request-status** command to display the certificate request status.

Examples

```
# Abort the certificate request for the PKI domain 1.
<Sysname> system-view
[Sysname] pki abort-certificate- request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

Related commands

- **display pki certificate request-status**
- **pki request-certificate domain**

pki certificate access-control-policy

Use **pki certificate access-control-policy** to create a certificate-based access control policy and enter its view.

Use **undo pki certificate access-control-policy** to remove a certificate-based access control policy.

Syntax

```
pki certificate access-control-policy policy-name
undo pki certificate access-control-policy policy-name
```

Default

No certificate-based access control policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Certificate-based access control policies allow you to authorize access to a device (for example, an HTTPS server) based on the attributes of an authenticated client's certificate.

A certificate-based access control policy is a set of access control rules (permit or deny statements), each associated with a certificate attribute group. A certificate attribute group contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field.

If a certificate matches all attribute rules in a certificate attribute group associated with an access control rule, the system determines that the certificate matches the access control rule. In this scenario, the match process stops, and the system performs the access control action defined in the access control rule.

Examples

Create a certificate-based access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

Related commands

- **display pki certificate access-control-policy**
- **rule**

pki certificate attribute-group

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view.

Use **undo pki certificate attribute-group** to remove a certificate attribute group.

Syntax

```
pki certificate attribute-group group-name
undo pki certificate attribute-group group-name
```

Default

No certificate attribute groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate attribute group is a set of attribute rules configured by using the **attribute** command. Each attribute rule defines a matching criterion for an attribute in the issuer name, subject name, or alternative subject name field of certificates.

A certificate attribute group must be associated with an access control rule (a permit or deny statement configured by using the **rule** command). If a certificate attribute group does not have any attribute rules, the system determines that the all certificates match the associated access control rule.

Examples

```
# Create a certificate attribute group named mygroup and enter its view.
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

Related commands

- **attribute**
- **display pki certificate attribute-group**
- **rule**

pki delete-certificate

Use **pki delete-certificate** to remove certificates from a PKI domain.

Syntax

```
pki delete-certificate domain domain-name { ca | local | peer [ serial serial-num ] }
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 12](#).

Table 12 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies a peer certificate by its serial number, a case-insensitive string of 1 to 127 characters. If you do not specify a serial number, this command removes all peer certificates in the PKI domain.

Usage guidelines

When you remove the CA certificate in a PKI domain, the system also removes the local certificates, peer certificates, and the CRL in the PKI domain.

Examples

```
# Remove the CA certificate in PKI domain aaa.
<Sysname> system-view
```

```

[Sysname] pki delete-certificate domain aaa ca
Local certificates, peer certificates and CRL will also be deleted while deleting the CA
certificate.
Confirm to delete the CA certificate? [Y/N]:y
[Sysname]

# Remove the local certificates in PKI domain aaa.
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa local
[Sysname]

# Remove all peer certificates in PKI domain aaa.
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa peer
[Sysname]

# Display information about all peer certificates in PKI domain aaa, and remove a peer certificate
with the specified serial number.
<Sysname> system-view
[Sysname] display pki certificate domain aaa peer
Total peer certificates: 1

Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject Name: CN=abc
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7

```

Related commands

display pki certificate

pki domain

Use **pki domain** to create a PKI domain and enter its view.

Use **undo pki domain** to remove a PKI domain.

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

Default

No PKI domain exists.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 13](#).

Table 13 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

When you remove a PKI domain, the certificates and the CRL in the domain are also removed.

Examples

Create a PKI domain named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa]
```

pki entity

Use **pki entity** to create a PKI entity and enter its view.

Use **undo pki entity** to remove a PKI entity.

Syntax

```
pki entity entity-name
undo pki entity entity-name
```

Default

No PKI entities exist.

Views

System view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a name for a PKI entity, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity includes the identity information that can be used by a CA to identify a certificate applicant. You can configure multiple attributes for a PKI entity, such as common name, organization, organization unit, locality, state, country, FQDN, and IP address. The information will be included as subject contents in the certificate issued by the CA.

Examples

Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

Related commands

`pki domain`

pki export

Use `pki export` to export the CA certificate and the local certificates in a PKI domain to local files or a terminal.

Syntax

```
pki export domain domain-name der { all | ca | local } filename filename
```

```
pki export domain domain-name p12 { all | local } passphrase p12-key filename filename
```

```
pki export domain domain-name pem { { all | local } [ { 3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc } pem-key ] | ca } [ filename filename ]
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 14](#).

Table 14 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the certificate file format as DER, which includes PKCS#7.

p12: Specifies the certificate file format as PKCS#12.

pem: Specifies the certificate file format as PEM.

all: Specifies both CA and local certificates. The RA certificate is excluded.

ca: Specifies the CA certificate.

local: Specifies the local certificates or the local certificates and their private keys.

passphrase *p12-key*: Specifies a password for encrypting the private key of a local PKCS12 certificate.

3des-cbc: Specifies 3DES_CBC for encrypting the private key of a local certificate.

aes-128-cbc: Specifies 128-bit AES_CBC for encrypting the private key of a local certificate.

aes-192-cbc: Specifies 192-bit AES_CBC for encrypting the private key of a local certificate.

aes-256-cbc: Specifies 256-bit AES_CBC for encrypting the private key of a local certificate.

des-cbc: Specifies DES_CBC for encrypting the private key of a local certificate.

pem-key: Specifies a password for encrypting the private key of a local certificate in PEM format.

filename *filename*: Specifies a file name for storing a certificate. The file name is a case-insensitive string. If you do not specify a file name for the certificates in PEM format, this command displays the certificates on the terminal.

Usage guidelines

When you export the CA certificate, the following conditions might exist:

- If the PKI domain has only one CA certificate, this command exports the CA certificate to a file or displays it on the terminal.
- If the PKI domain has a CA certificate chain, this command exports the certificate chain to a file or displays it on the terminal.

When you export the local certificates, the local file names might not be the same as specified in the command. The file names depend on the usage of the key pairs in the certificates. In the following description, the *filename* is the specified file name in the command.

- If the key pair of the local certificate is for signing, the local file name is *filename-sign*.
- If the key pair of the local certificate is for encryption, the local file name is *filename-encr*.
- If the key pair of the local certificate is for general use (RSA, ECDSA, or DSA), the local file name is *filename*.

If the PKI domain has two local certificates, one of the following results occurs:

- If you specify a file name, the local certificates are exported to two different files.
- If you do not specify a file name, the local certificates are displayed on the terminal, separated by the system prompts.

When you export all certificates, the following conditions might exist:

- If the PKI domain has only the CA certificate or local certificates, the result is the same as when you export the CA certificate or local certificates separately.
- If the PKI domain has both the CA certificate and the local certificates, you get the following results:
 - If you specify a file name, each local certificate with its associated CA certificate chain is exported to a separate file.
 - If you do not specify a file name, all local certificates and the CA certificate or the CA certificate chain are displayed on the terminal, separated by system prompts.

When you export all certificates in PKCS12 format, the PKI domain must have a local certificate. Otherwise, the export operation fails.

When you export the local certificates or all certificates in PEM format, you must specify the cryptographic algorithm and the challenge password for the private key. Otherwise, this command does not export the private keys of the local certificates. If you specify the cryptographic algorithm and the password, and the local certificates have their private keys, this command can export the local certificates with their private keys. If the local certificates do not have their private keys, the export operation fails.

When you export the local certificates, if the key pair in the PKI domain is changed and no longer matches the key in the local certificates, the export operation fails.

When you export the local certificates or all certificates, if the PKI domain has two local certificates, failure of exporting one local certificate does not affect export of the other.

The specified file name can contain an absolute path. If the specified path does not exist, the export operation fails.

Examples

```
# Export the CA certificate in the PKI domain to a file named cert-ca.der in DER format.
```

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 der ca filename cert-ca.der
```



```
L2NhY3JsLmNybdANBgkqhkiG9w0BAQsFAAOCQAQEAGcMeSpBjiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGyLMqaZ8pKUKv
UDS8c+HgIbRhmXvXztI08N1imYHq27WY9j6NpSS60mFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
```

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

Key Attributes: <No Attributes>

-----BEGIN ENCRYPTED PRIVATE KEY-----

```
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIAbfCE+KoYYoCAGgA
MBEGBSSoAwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzXHU0rExgn+6cQsK5uK99FPBmy4q9/nnYrooTX8BVlXAJenvgyii
WQLwnIglIuM8j2aPkQ3wbael+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvUOCc
/gxdgk97XZSW/0qnOSZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFTToixROTxWtTf8SEsKGPdfrEKq3fSTWlxokB8nM
bkRtU+fUiY27V/mr1RH06+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yxkSi
JdL+X3uEjHnQ/rvnPSKB EU/URwXHxMX9CdCTSqh/SajnrGuB/E4Jh0EnS/H9dIM+
DN6iz1IwPFk1bcK9KMGwV1bosymXmuEbyCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeEIHGEMcQU+g0EtfpOLTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BE1DVjJq3ioyHSJca8C+3lzcueuAF+107Y4Zluq3dqWuJjE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsV+9IYRYasjzoXE5dhZ5sIPod
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKym3Yg+Bgg8Df4bBrFrsh1U0ifmmp
ir2+OuhlC+GbHOxWNeBCa8iAq91k6FGFJ0OLA2oIvhCnh45tm7BjjKTHk+RZdMiA
0TKSWuOyihrwxduEWh999GKUpkwDHLZJFd21z/kWspqThodEx8ea
-----END ENCRYPTED PRIVATE KEY-----
```

Display all certificates in the PKI domain in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

<Sysname> system-view

[Sysname] pki export domain domain1 pem all des-cbc 111

%The signature usage local certificate:

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest

issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd

-----BEGIN CERTIFICATE-----

```
MIIEEjCCA5KgAwIBAgILAOhID4rI04kBFYgwdQYJKoZIhvcNAQELBQAwRTELMakG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLEDAhzb2Z0d2Fy
ZTENMAsGA1UEAwEYVWJjZDAeFw0xMjA0MjYxMzYxMjYxMjYxMjYxMjYxMjYxMjYx
ME0xMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
VXN1cnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwGykCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovHS5eJKZyky8fhMoTHHe
jE2KfBQizOZSgo2mdgpkccjr9Ek6IUC03ed11Pn0IG/YaA14Tjgkiv+w1Nr1SvAy
cnPaSuko2Qb09sg3ycye1zqpbqqj775ulGpcXyXYD90Y63/Cp5+DRQ92zGsCAwEA
```

AaOcahUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgmDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljbMEGECWCGSAGG+EIBAQQEAWIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQqh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBbTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9 jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFu0jgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDUuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybdANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhpWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ00t6hGylMqaZ8pKUKv
UDS8c+HgIBrhmXvXztI08N1imYHq27WY9j6NpSS60mFmI5whzCWfTSHzq1T2Dnd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----

Bag Attributes: <No Attributes>

subject=/C=CN/O=OpenCA Labs/OU=software/CN=abcd

issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd

-----BEGIN CERTIFICATE-----

MIIEYTTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFAADBFMQswCQYDVOQQGEWJDTjEU
MBIGA1UECgwLT3BlbkNBIExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTEyMDQxODU0NDQ0N1oXDTEyMDQxODU0NDQ0N1owRTELMAKGA1UE
BhMCQ04xFDASBgNVBAoMCM09wZW5DQSBMYWJzMRERDwYDVQLDAhzb2Z0d2FyZTEN
MASGA1UEAwwEYWJjZDCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51b0wjkFUBwxyvOy4D897LmOSedaCyDt6Lvp+PBEHfwWBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2V1cctsYKYvAQapuaThy1tuOcpHAB+ jQQL9dPoqdk0xp
jvmPdLw+k832Konn9U4dIivS0n+/KMgh0g5UyzHGqU0o7s9qFuQf5EjQon40TZg
BwUnFYRlvGe7bSQPxjwi8LTyxHPy+dDVj05CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7Z1udNus5vKWTihgx2Qalgb+sqUMwI/WUET7gh02dRxPUDUbgIYF0saTndKPYd
4oBg16M0SMsHhe9nF5UCAwEAAoCAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBbQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAWgBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEEjAQgQ5wa21Ab3B1bmNh
Lm9yZzAZBgNVHRIEEjAQgQ5wa21Ab3B1bmNhLm9yZzCBGQYIKwYBBQUHAQEEdTBz
MDIGCCsGAQUFBzAchiZodHRwOi8mdcG10YW4vcGtpL3B1Yi9jYWNlcnQvY2FjZXJ0
LmNyDAAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFu0ji1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcG10YW46ODMwLzA8BgNVHR8ENTAzMDGgG6AthitodHRwOi8vMTky
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcmwvY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0q0SSmVQnfa5ELtRKYF62C/Y8QTLbk61ZDTZuIzN15SGKQcbNM970ffCD
LklzosityEVE7PLnii3bZ5kchGO3byyXfluAqRyOGVJcudaw7uIQqgv0AJQ+zaQShi
d4kQf5QWgYkQ55/C5puOmcMRgCbMpr21YkqXLDjTIAZiHRZ/sTp6c+ie2bFxi/YT
3xYb00wDMuGOKJjpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bMfBduwhQWKSoyE
6vZsPGAEisCmAl3dIp49jPgVkiXoShraYF1jLsWzJG1zem8QvWYzOqKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAm1kAPX

-----END CERTIFICATE-----

Bag Attributes

```

friendlyName:
localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIcUSKSW9GVmICAggA
MBEGBSSoAwIHBAi5QZM+lsYWPASCAoBKDYule5f2BXL9ZhI9zWAJpx2cShz/9PsW
5Qm106D+xSj1eAzkx/m4Xb4xRU8oOAuzu1DlWfSHKXoaa0OoRSiOEXleg0eo/2vv
CHCvKHfTJr4gVSSa7i4I+aQ6AitrI6q99Wlkn/e/IE5U1UE4ZhcsIiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP7O2SdLV1Ub5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nm114EwPtPMMbHefcuQ6b82y1M+dWfVxBN9K031N4tZNfPWWLSRrPvJUZBG
dKtj3/IFdV7/tUmy9JJSpt4iFtlh7SZPcOoGplZW+YUR30I7YnFE+9Yp/46KWT8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXralLMYt/4jg4M0jUvoi3GS2Kbo+czsUn
gKgqYnxVfRSvt8d6GBYrpf2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhvyLkH0UuQE95emXBD/K0H1D73cMrtmogL8F4y5B2hPIr/v5/
eW35+1QMnJ9FtHFVnVsLx9w191X8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzxPVfEhO8
5ajQxWlidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsVmr5sk+fRaELD/cwL6VjtXO6x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uif
RLCfFAwaJMBdIQ6jDQHnpWT67uNDwdEzaPmuTVMme5Woc5zsqE5DY3hWu4oqFdDz
kPLnbX74IZ0GLki9eIJkVswNF5HkBCK50ejlW6TgbMNZ+Jpk2w
-----END ENCRYPTED PRIVATE KEY-----

```

Display the CA certificate in the PKI domain in PEM format.

```

<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB+TCCAWICEQDMbgjRKYgg3vpGFVY6pa3ZMA0GCSqGSib3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMzB4XDTEuMDMyMjA0NDQyNFoXDTE0MDMyMzA0MzUyNFowPTELMAkG
A1UEBHMcy24xDDAKBgNVBAoTA2gzYzERMA8GA1UECXMiaDNjLXRlc3QxD0TALBgNV
BAMTBDBgVNDMwz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOvDAYQhyc++G7h5
eNDzJs220QjCn/4JqnNKIdKz1BbaJT8/+IueSn9JISg64Ex2WBeCd/tcmnSW57ag
dCvNIUYXXVOGca2iaSOElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqwIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAE1m7
W2Lp9Xk4nZVIpVV76CkNe8/C+Id00GCRUUVQFSMvo7Pded76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTF080aKJGe6NapsfhJHKS+Q7mL0XpXeMONGK+e3dX7rsDxsY7hF+j
0gwsHrjV7kWvwJvDlhzGW6xbpr4DRmdca019Cr6o=
-----END CERTIFICATE-----

```

Export the CA certificate in the PKI domain to a file named **cacert in PEM format.**

```

<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert

```

Display the CA certificate or the CA certificate chain in the PKI domain on the terminal.

```

<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB7jCCAVcCEQCdSvShJFEMifvG8zRRoSsWMA0GCSqGSib3DQEBBQUAMDcxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTEuMDUwNTc0NFoXDTEuMTAzMTMyMzA0MzUyNFowODELMAkGA1UEBHMCM
Y24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECXMdaDNjMQ0wCwYDVQQDEwRhYWNhMIGf
MA0GCSqGSib3DQEBQUAA4GNADCBiQKBgQDcuJsWhAJXEDmowGb5z7VDVms54TKi

```

```
xnaNJCWvBOrU64ftvpVB7xQekbkjgAS9FjDyXlLQ8IyIsYIp5ebJr8P+n9i9P17j
lBx5mi4XeIldyv2OjfnX5oSQ+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPP6GQIDAQABMA0GCSqGSIb3DQEEBQUAA4GBAJrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeyiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJs0lhAqMpsCW6G2zh
5mus7FTHhyXpJ22/fnHg61m
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8DCCAVkCEQD2PBux/rvs1Nw9uTrZB3DlMA0GCSqGSIb3DQEEBQUAMDoxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEPMA0GAlUEAxMG
cm9mdcGNhMB4XDTEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
BhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGAlUECXMdaDNjMQwwCgYDVQQDEwNhY2Ew
gz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOeklR7DpeEV72N1OLz+dydIDTx0
zVZDdPxFlgQYWSfIBwwFKJEyQ/4y8VIfDIIm0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKrB82WZ2mah5Nuekus3LSZzBoZKTAOY5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVvGYBPwVpYglhJDOuIZxKdR2pfQOA4f35wM
Vz6kAujLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iROhJjc1NMV3pvIs
CuFiCLxRQcMGhCNHlOn4wuydssc=
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8jCCAAsCEfxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwwjELMAkG
AlUEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGAlUECXMdaDNjMQ8wDQYDVQQDEwZy
b290Y2EwHhcNMTEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
EwJjbjEMMAoGAlUEChMDaDNjMQwwCgYDVQQLEwNoM2MxMDEwMDEwMDEwMDEwMDEw
YTcBnzANBggkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAxP2XLFE230zq6MhwZvAomOxa
7tclr4bESXZu3UBKno3Ay9kQm2HrDOAizvZXfLu7Gx22ga2Qdz01IeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHfOG8nS+P7n83Bkrj/Fu7Yz4zjTKMbCF2EfhEyXxr4NSXA
fhC9qg9S23vNXStmWvsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBtsU7X77sdZ1Nn
0I981h0qA5g7SEEIpI+pwZjJrH0FVHw01e4JWhHjyHqrOyfXYqe7vH4Sxp5MHEqf
14nKIEbexbPONspebtznxv4/xTjd1aM2rfQ95jJ/SN8H8KIyiyZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pC2ZNiIpg==
```

-----END CERTIFICATE-----

Export the local certificates and their private keys in the PKI domain to a file named **cert-lo.der** in PKCS12 format. The password for the private keys is 123.

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
```

Export all certificates in the PKI domain to a file named **cert-all.p7b** in PKCS12 format.

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

Related commands

pki domain

pki import

Use **pki import** to import the CA certificate, local certificates, or peer certificates for a PKI domain.

Syntax

```
pki import domain domain-name { der { ca | local | peer } filename filename | p12 local filename filename | pem { ca | local | peer } [ filename filename ] }
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 15](#).

Table 15 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

filename *filename*: Specifies a certificate file name, a case-insensitive string. For a certificate in PEM format, you can also choose to copy and paste the certificate contents on the terminal instead of importing from a file.

Usage guidelines

Use this command to import a certificate in the following situations:

- The CRL repository is not specified or the CA server does not support SCEP.
- The certificate is packed with the server generated key pair in a single file. Only certificate files in PKCS12 or PEM format might contain key pairs.

Before you import the certificates, complete the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, you can import the certificates by copying and pasting the certificate contents through the terminal. In this case, make sure the certificate is in PEM format because only certificates in PEM format can be imported by this means.
- For the local certificates or peer certificates to be imported, the correct CA certificate chain must exist. The CA certificate chain can be stored on the device, or carried in the local certificates or peer certificates. If the PKI domain, the local certificates, or the peer certificates do not have the CA certificate chain, you must import the CA certificate first. To import a local or peer certificate, a CA certificate chain must exist in the PKI domain, or be carried in the local or peer certificate. If not, obtain it first.

When you import the local certificates or peer certificates:

- If the local certificates or peer certificates to be imported contain the CA certificate chain, you can import the CA certificate and the local certificates or peer certificates at the same time. If the certificate of the CA that issues the local certificates or peer certificates already exists in a PKI domain, the system displays a prompt to ask you whether to overwrite the existing CA certificate.
- If the local certificates or peer certificates to be imported do not contain the CA certificate chain, but the certificate of the CA that issues the local certificate or peer certificate already exists in a PKI domain, you can directly import the local certificates or peer certificates.

When you import the CA certificate:

- If the CA certificate to be imported is the CA root certificate or contains the certificate chain with the root certificate, you can import the CA certificate.
- If the CA certificate to be imported contains a certificate chain without the root certificate, but can form a complete certificate chain with the CA certificate on the device, you can import the CA certificate. Otherwise, you cannot import it.

Contact the CA server administrator to get the correct information in the following scenarios:

- If the certificate file to be imported contains the root certificate, but the root certificate and its fingerprint are not specified on the device, the system asks you to confirm the fingerprint.
- If the local certificate to be imported contains a key pair, the system asks you to enter the challenge password used for encrypting the private key.

When you import a local certificate file that contains a key pair, you can choose to update the domain with the key pair. Depending on the purpose of the key pair, the following conditions apply:

- If the purpose of the key pair is general, the device uses the key pair to replace the local key pair that is found in this order: general-purpose key pair, signature key pair, and encryption key pair.
- If the purpose of the key pair is signature, the device uses the key pair to replace the local key pair that is found in this order: general-purpose key pair and signature key pair.
- If the purpose of the key pair is encryption, the device searches the domain for an encryption key pair.

If a matching key pair is found, the device asks whether you want to overwrite the existing key pair on the device. If no match is found, the device asks you to enter a key pair name (defaulting to the PKI domain name). Then, it generates the key pair according to the key algorithm and the purpose defined in the certificate file.

The import operation automatically updates or generates the correct key pair. When you perform the import operation, be sure to save the configuration file to avoid data loss.

Examples

Import the CA certificate file **rootca_pem.cer** in PEM format to the PKI domain **aaa**. The certificate file contains the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Sysname]
```

Import the CA certificate file **aca_pem.cer** in PEM format to the PKI domain **bbb**. The certificate file does not contain the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem ca filename aca_pem.cer
[Sysname]
```

Import the local certificate file **local-ca.p12** in PKCS12 format to the PKI domain **bbb**. The certificate file contains a key pair.

```
<Sysname> system-view
[Sysname] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
*****
[Sysname]
```

Import the local certificate in PEM format to the PKI domain **bbb** by copying and pasting the contents of the certificate. The certificate contains the key pair and the CA certificate chain.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem local
Enter PEM-formatted certificate.
End with a Ctrl+c on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 8DCE37F0A61A4B8C
```

```
k9C3KHY5S3EtnF5iQymvHYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApYbW
EclTDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfHhpQp
GdmMqnFpp59ZzB210GlbgZlPcsjot+EGpZg6BlKrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50Jz1QYIzMbcrw+S5W1PxACTIONz1cld1Blblkpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JpP720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHath4BiT9v7zetnQqf4q8plfd/
Xqd9zEF1BPpoJftJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOpia+Pm
GbrqSyy55c1Vde5GocGN1DZ94DW7AypazgLPBbrkIYAdjFPRmq+zModyqsGMTNj
jnheI51784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/S19d9x
Q00ru0lpsxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+d0925GoAcHO40
cCl6jA/HsGAU9HkpWkHL35lmBDRLEzQeBFcaGwSmlJvrfE4tkJM7+Uz2QHJOFP10
0VLqMgxMlPk3TvBwgZHGJDe7TdzFCDPMPHod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
```

```
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTAA2gzYzEMMAoGA1UECXMDC2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxbGRzc2xzZXJ2ZXIwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLp
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO5521oGiPy10wmFMK12TSL7sHvrxr00drFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPuytP185JUhbOrVaUDlisZi6NNshcIjd2BAGMBAAGjgbowgbcwHwYDVR0j
```

```

BBgwFoAUmoMPEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCg
SAGG+EIBAQQEAWIGQDASBgNVHREECzAJggdoM2MuY29tMB0GAlUdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzAlMDOgMaAvhilodHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5t19ZNI THFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWwx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwnZELMAkG
AlUEBhMCY24xDdAKBgNVBAoTA2gzYzEMMAoGAlUECXMdc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwnZMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEWJj
bjEMMAoGAlUEChMDaDNjMQwwCgYDVQQLEwNzZWmxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAt8QSMetQ70GONiFh7iJkvGQ8n15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAWEAATANBgkqhkiG9w0BAQUFAAOBgQBwsaMgRbBmtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCx19l+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXMlo4DQ==
-----END CERTIFICATE-----

```

Please input the password:*****

Local certificate already exist, confirm to overwrite it? [Y/N]:y

The PKI domain already has a CA certificate. If it is overwritten, local certificates, peer certificates and CRL of this domain will also be deleted.

Overwrite it? [Y/N]:y

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name [default name: bbb]:

The key pair already exists.

Please enter the key pair name:

import-key

Related commands

- **display pki certificate**
- **public-key dsa**
- **public-key ecdsa**
- **public-key rsa**

pki request-certificate

Use **pki request-certificate** to submit a local certificate request or generate a certificate request in PKCS#10 format.

Syntax

```
pki request-certificate domain domain-name [ password password ] [ pkcs10 [ filename filename ] ]
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 16](#).

Table 16 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

password *password*: Sets the password for certificate revocation, a case-sensitive string of 1 to 31 characters. The password is contained in the certificate request and must be provided if the certificate is revoked.

pkcs10: Displays BASE64-encoded PKCS#10 certificate request information, which can be used to request a certificate by an out-of-band means, like phone, disk, or email.

filename *filename*: Specifies a local file for saving the certificate request in PKCS#10 format. The *filename* argument is case-insensitive.

Usage guidelines

If SCEP fails, you can perform one of the following tasks:

- Use the **pkcs10** keyword to print the BASE64-encoded request information.
- Use the **pkcs10 filename** *filename* option to save the request information to a local file and send the file to the CA by an out-of-band means. The specified file name can contain an absolute path. If the specified path does exist, the request information cannot be saved.

This command is not saved in the configuration file.

Examples

```
# Display information about the certificate request in the PKCS#10 format.
```

```
<Sysname> system-view
```

```
[Sysname] pki request-certificate domain aaa pkcs10
```

```
*** Request for general certificate ***
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

```

MIIBTDCBtgIBADANMQswCQYDVQQDEwJqa jCBnzANBgkqhkiG9w0BAQEFAAOB jQAw
gYkCgYEAw5Dr j8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJi jB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3o12z7Nmdu5TED6iN8
4m+hfp1QWoV61ty3o9pxAXuQ18peUDcfN6WV3LBXYy11WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa11QOHS7YMvno6hXAQ1kM4c
-----END NEW CERTIFICATE REQUEST-----

```

```

# Request the local certificates.
[Sysname] pki request-certificate domain openca
Start to request the general certificate ...
...
Request certificate of domain openca successfully

```

Related commands

display pki certificate

pki retrieve-certificate

Use **pki retrieve-certificate** to obtain a certificate from the certificate distribution server.

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** | **peer** *entity-name* }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 17](#).

Table 17 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer *entity-name*: Specifies a peer entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In online mode:

- You can obtain the CA certificate through the SCEP protocol. If a CA certificate already exists locally, do not obtain the CA certificate again. To obtain a new one, use the **pki**

delete-certificate command to remove the CA certificate and local certificates, and then obtain the CA certificate again.

- You can obtain local certificates or peer certificates through the LDAP protocol. If a PKI domain already has local certificates or peer certificates, you can still perform the obtain operation and the obtained local certificates or peer certificates overwrite the existing ones. If RSA is used, a PKI domain can have two local certificates, one for signing and the other for encryption. Certificates for different purposes do not overwrite each other.

The obtained CA certificate, local certificates, and peer certificates are automatically verified before they are saved locally. If the verification fails, they are not saved.

This command is not saved in the configuration file.

Examples

Obtain the CA certificate from the certificate distribution server. (This operation requires the user to confirm the fingerprint of the CA root certificate.)

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5 fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

Obtain the local certificates from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa local
```

Obtain the certificate of the peer entity **en1** from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa peer en1
```

Related commands

- **display pki certificate**
- **pki delete-certificate**

pki retrieve-crl

Use **pki retrieve-crl** to obtain CRLs and save them locally.

Syntax

```
pki retrieve-crl domain domain-name
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 18](#).

Table 18 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.

Character name	Symbol	Character name	Symbol
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

CRLs are used to verify the validity of the local certificates and the peer certificates in a PKI domain. To obtain CRLs, a PKI domain must have the correct CA certificate.

The URL of the CRL repository is specified by using the **crl url** command.

The device can obtain CRLs from the CRL repository through the HTTP, LDAP, or SCEP protocol. Which protocol is used depends on the configuration of the CRL repository in the PKI domain:

- If the specified URL of the CRL repository is in HTTP format, the device obtains CRLs through the HTTP protocol.
- If the specified URL of the CRL repository is in LDAP format, the device obtains CRLs through the LDAP protocol. If the specified URL does not have a host name, for example, `ldap:///CN=8088,OU=test,U=rd,C=cn`, you must specify the LDAP server's URL for the PKI domain by using the **ldap server** command. The device can obtain the complete URL of the LDAP repository by combining the URLs of the LDAP server and of the CRL repository.
- If the PKI domain is not configured with the CRL repository, the device looks up the local certificates and then the CA certificate for the CRL repository. If a CRL repository is found, the device obtains CRLs from the point. Otherwise, the device obtains CRLs through the SCEP protocol.

Examples

```
# Obtain CRLs from the CRL repository.
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
```

Related commands

- **crl url**
- **ldap server**

pki storage

Use **pki storage** to specify the storage path for the certificates or CRLs.

Use **undo pki storage** to restore the default.

Syntax

```
pki storage { certificates | crls } dir-path
```

```
undo pki storage { certificates | crls }
```

Default

Certificates and CRLs are stored in the **PKI** directory on the storage media of the device. The **PKI** directory is automatically created when a certificate is successfully requested, obtained, or imported for the first time.

Views

System view

Predefined user roles

network-admin

Parameters

certificates: Specifies a storage path for the certificates.

crls: Specifies a storage path for the CRLs.

dir-path: Specifies a storage path, a case-sensitive string, which cannot start with a slash (/) or contains two dots plus a slash (./). The *dir-path* argument specifies an absolute path or a relative path, and the path must exist.

Usage guidelines

The specified storage path is a path on the active MPU rather than on other MPUs.

If the path to be specified does not exist, use the **mkdir** command to create the path before using this command. After you change the storage path for certificates or CRLs, the certificate files (with the .cer or .p12 extension) and CRL files (with the .crl extension) in the original path are moved to the new path.

Examples

Specifies **flash:/pki-new** as the storage path for the certificates.

```
<Sysname> system-view
[Sysname] pki storage certificates flash:/pki-new
```

Specifies **pki-new** as the storage path for the CRLs.

```
<Sysname> system-view
[Sysname] pki storage crls pki-new
```

pki validate-certificate

Use **pki validate-certificate** to verify the validity of certificates.

Syntax

```
pki validate-certificate domain domain-name { ca | local }
```

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in [Table 19](#).

Table 19 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

Generally, certificates are automatically verified when you request, obtain, or import them, or when an application uses PKI.

You can also use this command to manually verify a certificate in the following aspects:

- Whether the certificate is issued by a trusted CA.
- Whether the certificate expires.
- Whether the certificate is revoked if CRL checking is enabled.

When CRL checking is enabled:

- To verify the local certificates, if the PKI domain has no CRLs, the device looks up the locally save CRLs. If a correct CRL is found, the device loads the CRL to the PKI domain. Otherwise, the device obtains the correct CRL from the CA server and saves it locally.
- To verify the CA certificate, CRL checking is performed for the CA certificate chain from the current CA to the root CA.

Examples

Verify the validity of the CA certificate in PKI domain **aaa**.

```
<Sysname> system-view
```

```
[Sysname] pki validate-certificate domain aaa ca
```

```
Verifying certificates.....
```

```
Serial Number:
```

```
f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
```

```
Issuer:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```
Subject:
```

```
C=cn
```

```
O=abc
```

```
OU=test
```

```
CN=aca
```

```
Verify result: OK
```

```
Verifying certificates.....
```

```
Serial Number:
```

```
5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
```

```
Issuer:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```
Subject:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```

Verify result: OK

# Verify the local certificates in PKI domain aaa.
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa local
Verifying certificates.....
    Serial Number:
        bc:05:70:1f:0e:da:0d:10:16:1e
    Issuer:
        C=CN
        O=sec
        OU=software
        CN=bca
    Subject:
        O=OpenCA Labs
        OU=Users
        CN=fips fips-sec

Verify result: OK

```

Related commands

- **crl check**
- **pki domain**

public-key dsa

Use **public-key dsa** to specify a DSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

Default

No key pair is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

- If DSA or ECDSA is used, a PKI domain can have only one key pair.
- If RSA is used, a PKI domain can have two key pairs: one is the signing key pair, and the other is the encryption key pair.
- In a PKI domain, key pairs for different purposes (RSA signing and RSA encryption) do not overwrite each other.
- For DSA or ECDSA, the most recent configuration takes effect.

The **length key-length** option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length key-length** option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

```
# Specify the DSA key pair abc with the key length of 2048 bits for certificate request.
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

Related commands

- **pki import**
- **public-key local create** (see *Security Command Reference*)

public-key ecdsa

Use **public-key ecdsa** to specify an ECDSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

```
public-key ecdsa name key-name [ secp192r1 | secp256r1 | secp384r1 ]
undo public-key
```

Default

No key pair is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name key-name: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

secp192r1: Uses the secp192r1 curve to generate the key pair. The secp192r1 curve is used by default.

secp256r1: Uses the secp256r1 curve to generate the key pair.

Secp384r1: Uses the secp384r1 curve to generate the key pair.

Usage guidelines

You can specify a nonexistent key pair in this command. A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

- If DSA or ECDSA is used, a PKI domain can have only one key pair.
- If RSA is used, a PKI domain can have two key pairs: one is the signing key pair, and the other is the encryption key pair.
- In a PKI domain, key pairs for different purposes (RSA signing and RSA encryption) do not overwrite each other.
- For DSA or ECDSA, the most recent configuration takes effect.

The specified elliptic curve takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and curve before submitting a certificate request. The curve parameter is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify the ECDSA key pair **abc** generated by using the secp384r1 curve for certificate request in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

Related commands

- **pki import**
- **public-key local create** (see *Security Command Reference*)

public-key rsa

Use **public-key rsa** to specify an RSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

```
public-key rsa { { encryption name encryption-key-name [ length key-length ] | signature name signature-key-name [ length key-length ] } * | general name key-name [ length key-length ] }
```

```
undo public-key
```

Default

No key pair is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

encryption: Specifies a key pair for encryption.

name *encryption-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

signature: Specifies a key pair for signing.

name *signature-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

general: Specifies a key pair for both signing and encryption.

name *key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. You can get a key pair in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

- If DSA or ECDSA is used, a PKI domain can have only one key pair.
- If RSA is used, a PKI domain can have two key pairs: one is the signing key pair, and the other is the encryption one.
- In a PKI domain, key pairs for different purposes (RSA signing and RSA encryption) do not overwrite each other.
- For DSA or ECDSA, the most recent configuration takes effect.

If you specify a signing key pair and an encryption key pair separately, their key length can be different.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify a general purpose RSA key pair named **abc** with a key length of 2048 bits for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

Specify the RSA encryption key pair **rsa1** with the key length 2048 bits. Specify the RSA signing key pair **sig1** with the key length 2048 bits for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

Related commands

- **pki import**
- **public-key local create** (see *Security Command Reference*)

root-certificate fingerprint

Use **root-certificate fingerprint** to set the fingerprint for verifying the validity of the root CA certificate.

Use **undo root-certificate fingerprint** to restore the default.

Syntax

```
root-certificate fingerprint { md5 | sha1 } string
```

```
undo root-certificate fingerprint
```

Default

No fingerprint is set.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

md5: Sets an MD5 fingerprint.

sha1: Sets a SHA1 fingerprint.

string: Sets the fingerprint information in hexadecimal notation. If you specify the **MD5** keyword, the fingerprint is a string of 32 characters. If you specify the **SHA1** keyword, the fingerprint is a string of 40 characters.

Usage guidelines

If you set the certificate request mode to auto for a PKI domain that does not have a CA certificate, you must configure the fingerprint for CA certificate verification. When an application, like IKE, triggers the device to request local certificates, the device automatically performs the following operations:

1. Obtains the CA certificate from the CA server.
2. Verifies the fingerprint contained in the CA certificate with the one configured in the PKI domain.

If the PKI domain is not configured with a fingerprint or if the configured fingerprint does not match the fingerprint contained in the CA certificate, the device rejects the CA certificate and the local certificate request fails.

You can choose whether to set the fingerprint of the root CA certificate when performing the following tasks:

- Import the CA certificate by using the **pki import** command.
- Obtain the CA certificate by using the **pki retrieve** command.

If you specify the fingerprint in the PKI domain, the device automatically verifies the fingerprint of the CA certificate to be imported or obtained against that configured in the domain. If the two fingerprints do not match, the device rejects the CA certificate. If no fingerprint is specified in the domain, the device asks you to manually verify the fingerprint of the CA certificate.

Examples

```
# Specify an MD5 fingerprint for verifying the validity of the root CA certificate.
```

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

Specify an SHA1 fingerprint for verifying the validity of root CA certificate.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDAD93
```

Related commands

- **certificate request mode**
- **pki import**
- **pki retrieve-certificate**

rule

Use **rule** to create an access control rule (or statement).

Use **undo rule** to remove an access control rule (or statement).

Syntax

```
rule [ id ] { deny | permit } group-name
```

```
undo rule id
```

Default

No statement exists.

Views

PKI certificate-based access control policy view

Predefined user roles

network-admin

Parameters

id: Assigns an ID to the access control rule, in the range of 1 to 16. The default setting is the smallest unused ID in this range.

deny: Denies the certificates that match the associated attribute group.

permit: Permits the certificates that match the associated attribute group.

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

When you create an access control rule, you can associate it with a nonexistent certificate attribute group.

The system determines that a certificate matches an access control rule when either of the following conditions exists:

- The associated certificate attribute group does not exist.
- The associated certificate attribute group does not contain any attribute rules.
- The certificate matches all attribute rules in the associated certificated attribute group.

You can create multiple access control rules for an access control policy. A certificate matches the rules one by one, starting with the rule with the smallest ID. When a match is found, the match process stops, and the system performs the access control action defined in the access control rule.

Examples

```
# Create rule 1 to permit all certificates that match certificate attribute group mygroup.
```

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

Related commands

- **attribute**
- **display pki certificate access-control-policy**
- **pki certificate attribute-group**

SOURCE

Use **source** to specify the source IP address for PKI protocol packets.

Use **undo source** to restore the default.

Syntax

```
source { ip | ipv6 } { ip-address | interface interface-type interface-number }
undo source
```

Default

The source IP address of PKI protocol packets is the IP address of their outgoing interface.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies a source IPv4 address.

ipv6 *ip-address*: Specifies a source IPv6 address

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface's primary IP address will be used as the source IP address for PKI protocol packets.

Usage guidelines

Use this command to specify the source IP address for PKI protocol packets. You can also specify a source interface if the IP address is dynamically obtained.

Make sure there is a route between the source IP address and the CA server.

You can specify only one source IP address in a PKI domain. If you configure this command multiple times, the most recent configuration takes effect.

Examples

```
# Set the source IP address to 111.1.1.8 for PKI protocol packets.
```

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip 111.1.1.8
```

Set the source IPv6 address to 1::8 for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 1::8
```

Set the source IP address to the IPv4 address of VLAN-interface 100 for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface vlan-interface 100
```

Set the source IP address to the IPv6 address of VLAN-interface 100 for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface vlan-interface 100
```

state

Use **state** to set the state or province name for a PKI entity.

Use **undo state** to restore the default.

Syntax

state *state-name*

undo state

Default

No state name or province name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

state-name: Specifies a state or province by its name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the state name to **countryA** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA
```

subject-dn

Use **subject-dn** to configure the DN for a PKI entity.

Use **undo subject-dn** to restore the default.

Syntax

subject-dn *dn-string*

undo subject-dn

Default

No DN is configured for a PKI entity.

Views

PKI entity view

Default command level

network-admin

Parameters

dn-string: Specifies the DN for the PKI entity, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The subject DN string is a sequence of *attribute=value* pairs separated by commas. Each attribute can be specified multiple times with different values. Supported DN attributes are:

- **CN**—Common-name.
- **C**—Country code.
- **L**—Locality.
- **O**—Organization.
- **OU**—Organization unit.
- **ST**—State or province.

After this command is configured, the following commands do not take effect:

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Configure the DN for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] subject-dn
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

Related commands

common-name
country
locality
organization
organization-unit
state

usage

Use **usage** to specify the extensions for certificates.

Use **undo usage** to remove certificate extensions.

Syntax

usage { **ike** | **ssl-client** | **ssl-server** } *

undo usage [**ike** | **ssl-client** | **ssl-server**] *

Default

No extensions are specified. A certificate can be used for all applications, including IKE, SSL clients, and SSL servers.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ike: Specifies the IKE certificate extension so IKE peers can use the certificates.

ssl-client: Specifies the SSL client certificate extension so the SSL client ends can use the certificates.

ssl-server: Specifies the SSL server certificate extension so the SSL server ends can use the certificates.

Usage guidelines

If you do not specify any keywords for the **undo usage** command, this command removes all certificate extensions.

The extension options contained in a certificate depends on the CA policy, and might be different from those specified in the PKI domain.

Examples

```
# Specify the IKE certificate extension.  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] usage ike
```