Configure Trustpoints and Install Certificates on MDS 9000 Switches

Contents

Introduction

This document describes the configuration steps for the configuration of Trustpoint and Certificates in the MDS switches.

Background Information

Public Key Infrastructure (PKI) support provides the means for the Cisco Multilayer Director Switch (MDS) 9000 Family switches to obtain and use digital certificates for secure communication in the network. PKI support provides manageability and scalability for IP Security (IPsec), Internet Key Exchange (IKE), and Secure Shell (SSH).

Prerequisites

You must configure the host name and IP domain name of the switch if they are not already configured.

```
switch# configuration terminal
switch(config)# switchname <switchName>
SwitchName(config)# ip domain-name example.com
```

Note: Changing the IP host name or IP domain name after generating the certificate can invalidate the certificate.

Understanding of few related keywords

Trustpoint : A locally configured object that contains informtion about a trusted Certificate Authority (CA), including the local RSA keypair, the CA public certificate(s), and the identity certificate issued to the switch by a CA. Mutiple trustpoints can be configured to enroll switch identity certificates from multiple CAs. The complete identity information in a trust point can be exported to a file in the password-protected PKCS12 standard format. It can be later imported to the same switch (for example, after a system crash) or to a replacement switch. The information in a PKCS12 file consists of the RSA key-pair, the identity certificate, and the CA certificate (or chain).

CA Certificate : This is the certificate that is issued by the Certification Authority (CA) in respect to itself. There could be an Intermeidate or Subordinate CA in the setup. In that case, this could also refer to the Intermediate or Subordinate CA public certificate.

Certificate Authorities (CAs) : Devices that manage certificate requests and issue identity certificates to entities such as hosts, network devices, or users. CAs provide centralized key management for such entities.

RSA keypair : Generated with cli in the switch and associated with the the trustpoint. For each trustpoint configured on the switch, you must generate a unique RSA keypair and associate it with the trustpoint.

Certification Signing request (CSR) This is request that is generated from the switch and sent to CA to be signed. Against this CSR the CA sends back the Identity Certificate.

Identity Certificate : This is the certificate that is signed and issued by the Certification Authority for the switch from which the CSR is generated. Once a CSR is submitted to a CA, the CA or an administrator provides the Identity Certificate by e-mail or through a web browser. In order to paste an Identity Certificate into an MDS trustpoint, it must be in standard PEM (base64) format.

Requirements

Root CA .

Sub CA Certificates (If the Identity Certificates are signed by the Sub CA) In this case CA certificates of Sub CA are also required to be added in the switch.

Identity Certificate

Configure

Step 1

Generate an RSA key-pair

```
switchName# configure terminal
switchName(config)# crypto key generate rsa label <rsaKeyPairName> exportable modulus xxx
```

(Valid modulus values are (default) 512, 768, 1024, 1536, 2048, and 4096)

Step 2

Create a CA Trust Point and Associate the RSA keypair with the Trustpoint

The switch FQDN is used as a default key label when none is specified during key-pair generation.

```
switchName(config)# crypto ca trustpoint <trustpointName>
switchName(config-trustpoint)# enroll terminal
switchName(config-trustpoint)# rsakeypair <rsaKeyPairName>
```

Step 3

Authenticating a Trust Point Certificate Authority

If the CA being authenticated is not a self-signed CA, then the full list of the CA certificates of all the CAs in the certification chain needs to be input during the CA authentication step. This is called the CA certificate chain of the CA being authenticated. The maximum number of certificates in a CA certificate chain is 10.

When Only there is Root CA

```
switchName# configure terminal

switchName(config)# crypto ca authenticate <trustpointName>

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIDmjCCAoKgAwIBAgIGAVTGvpxRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNVBAYT
AkFVMSUwIwYDVQQKDBxDaXNjbyBTeXN0ZW1zIEluYy4gQXVzdHJhbGlhMRIwEAYD
VQQLDAlDaXNjbyBUQUMxEzARBgNVBAMMCk5pa29sYXkgQ0EwHhcNMTYwNTE5MDIw
MTAxWhcNMjYwNTIwMDIwMTE0WjBdMQswCQYDVQQGEwJBVTElMCMGA1UECgwcQ2lz
Y28gU3lzdGVtcyBJbmMuIEF1c3RyYWxpYTESMBAGA1UECwwJQ2lzY28gVEFDMRMw
EQYDVQQDDApOaWtvbGF5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAm6onXi3JRfIe2NpQ53CDBCUTn8cHGU67XSyqgL7MlYBhH032QaVrT3b98KcW
55UoqQW15kAnJhNTIQ+f0f8oj9A5UbwcQwIXQuHGkDZvJULjidM37tGF90ZVLJs7
sMxsnVSPIe05w71B9Zuvgh3b7QEdW0DMevNwhuYgaZ0TWrkRR0SoG+6l60DWVzfT
GX0I7MCpLE8JevHZmwfutkQcbVlozcu9sueemvL3v/nEmKP+GlxboR9EqFhXQeyy
/qkhr7Oj/pPHJbvTSuf09VgVRi5c03u7R1Xcc0taNZxSENWovyy/EXkEYjbWaFr7
u+Npt5/6H3XNQKJ0PCSuoOdWPwIDAQABo2AwXjAfBgNVHSMEGDAWgBSE/uqXmcfx
DeH/OVLB6G3ARtAvYzAdBgNVHQ4EFgQUhP7ql5nH8Q3h/zlSwehtwEbQL2MwDgYD
VR0PAQH/BAQDAgGGMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH9J
a89CFrIUIGGQFg6L2CrYmuOE0bv69UnuodvzG/qEy4GwWUNkUCNu8wNfx3RAgJ8R
KHUbeQY0HjGRaThY8z7Qx8ugA6pDEiwf/BMKPNBPkfhMEGL2Ik02uRThXruA82Wi
OdLY0E3+fx0KULVKS5VvO9Iu5sGXa8t4riDwGWLkfQo2AMLzc+SP4T3udEpG/9BD
nwGOseiz5a/kTAsMircoN2TcqoMBf5LQoA52DJf6MAHd2QZxcnm9ez8igKhzvMG1
OiopI3jTQ38Y9fqCK8E30wUwCozaY3jT0G3F57BfPCfBkkdz1a/Lw7en991xtBcp
0iptGTDJSt7TruaTvDs=
-----END CERTIFICATE-----
```

```
END OF INPUT ---> press Enter
```

When there are Internmediate or Subordinate CAs

The certificates are to be provided as shown:

```
switchName# configure terminal
switchName(config)# crypto ca authenticate <trustpointName>

Input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIDmjCCAoKgAwIBAgIGAVTGvpxRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNVBAYT
AkFVMSUwIwYDVQQKDBxDaXNjbyBTeXN0ZW1zIEluYy4gQXVzdHJhbGlhMRIwEAYD
VQQLDAlDaXNjbyBUQUMxEzARBgNVBAMMCk5pa29sYXkgQ0EwHhcNMTYwNTE5MDIw
MTAxWhcNMjYwNTIwMDIwMTE0WjBdMQswCQYDVQQGEwJBVTElMCMGA1UECgwcQ2lz
Y28gU3lzdGVtcyBJbmMuIEF1c3RyYWxpYTESMBAGA1UECwwJQ2lzY28gVEFDMRMw
EQYDVQQDDApOaWtvbGF5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAm6onXi3JRfIe2NpQ53CDBCUTn8cHGU67XSyqgL7MlYBhH032QaVrT3b98KcW
55UoqQW15kAnJhNTIQ+f0f8oj9A5UbwcQwIXQuHGkDZvJULjidM37tGF90ZVLJs7
sMxsnVSPIe05w71B9Zuvgh3b7QEdW0DMevNwhuYgaZ0TWrkRR0SoG+6l60DWVzfT
GX0I7MCpLE8JevHZmwfutkQcbVlozcu9sueemvL3v/nEmKP+GlxboR9EqFhXQeyy
/qkhr7Oj/pPHJbvTSuf09VgVRi5c03u7R1Xcc0taNZxSENWovyy/EXkEYjbWaFr7
u+Npt5/6H3XNQKJ0PCSuoOdWPwIDAQABo2AwXjAfBgNVHSMEGDAWgBSE/uqXmcfx
DeH/OVLB6G3ARtAvYzAdBgNVHQ4EFgQUhP7ql5nH8Q3h/zlSwehtwEbQL2MwDgYD
VR0PAQH/BAQDAgGGMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH9J
a89CFrIUIGGQFg6L2CrYmuOE0bv69UnuodvzG/qEy4GwWUNkUCNu8wNfx3RAgJ8R
KHUbeQY0HjGRaThY8z7Qx8ugA6pDEiwf/BMKPNBPkfhMEGL2Ik02uRThXruA82Wi
OdLY0E3+fx0KULVKS5VvO9Iu5sGXa8t4riDwGWLkfQo2AMLzc+SP4T3udEpG/9BD
nwGOseiz5a/kTAsMircoN2TcqoMBf5LQoA52DJf6MAHd2QZxcnm9ez8igKhzvMG1
OiopI3jTQ38Y9fqCK8E30wUwCozaY3jT0G3F57BfPCfBkkdz1a/Lw7en991xtBcp
0iptGTDJSt7TruaTvDs=
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT ---> press Enter
```

Blue color Text -> This is copied from the CA certificate (open in any text editor) and pasted when prompted in the switch CLI.

Red Color Text -> This is to be entered to end the certifcate.

Any Error in in the the certificate results in this

```
failed to load or parse certificate
```

```
could not perform CA authentication
```

If you try to authenticate from a Sub CA certificate without adding the Root CA certificate you get

```
incomplete chain (no selfsigned or intermediate cert)
could not perform CA authentication
```

If everything is good

```
Fingerprint(s): SHA1 Fingerprint=E1:37:5F:23:FA:82:0C:63:40:9C:AD:C7:7A:83:C9:6A:EA:54:9A:7A
Do you accept this certificate? [yes/no]:yes
```

Step 4

Generating Certificate Signing Requests

NX-OS 8.4(1x) and earlier

```
switchName# configure terminal
switchName(config)# crytpo ca enroll <trustpointName>
Create the certificate request.. Create a challenge password. You need to verbally provide this
password to the CA Administrator in order to revoke your certificate. For security reasons your
password not be saved in the configuration. Please make a note of it. Password: abcdef1234 -----
>(Keep a note of this password that you are entering) The subject name in the certificate be the
name of the switch. Include the switch serial number in the subject name? [yes/no]: no Include
an IP address in the subject name [yes/no]: yes ip address: 192.168.x.x The certificate request
be displayed... -----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST---
--
```

The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Note: Do not use the '$' character for your password. It causes the CSR to fail.

Copy this starting from

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

Untill

```
-----END CERTIFICATE REQUEST-----
```

Save this outside the switch. This needs to be forwarded to the Root CA or Sub CA (whichever one signs) via email or another method. The CA returns a signed Identity Certificate.

NX-OS 8.4(1) and later.

As a fix for Cisco bug ID CSCvo43832 , the enrollment prompts were changed in NX-OS 8.4(1).

By default, the Subject Name is the same as the switch name.

The enrollment prompts also allow an Alternate Subject Name and multiple DN fields.

Note: The DN field prompts with numbers as examples can accept any string with that range of characters. For example, the State DN prompt says:

Enter State[1-128]:

It takes any string from 1 to 128 characters.

```
switchName# configure terminal
switchName(config)# crypto ca enroll <trustpointName>
Create the certificate request ..
Create a challenge password. You need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password not be saved in the configuration.
Please make a note of it.
Password:abcdef1234
The subject name in the certificate is the name of the switch.
Change default subject name? [yes/no]:yes
Enter Subject Name:customSubjectName
Include the switch serial number in the subject name? [yes/no]:yes
The serial number in the certificate is: XXXXXXXXXXX
Include an IP address in the subject name [yes/no]:yes
ip address:192.168.x.x
Include the Alternate Subject Name ? [yes/no]:yes
Enter Alternate Subject Name:AltName
Include DN fields? [yes/no]:yes
Include Country Name ? [yes/no]:yes
Enter Country Code [XX]:US
Include State ? [yes/no]:yes
Enter State[1-128]:NC
Include Locality ? [yes/no]:yes
Enter Locality[1-128]:RTP
Include the Organization? [yes/no]:yes
Enter Organization[1-64]:TAC
Include Organizational Unit ? [yes/no]:yes
Enter Organizational Unit[1-64]:sanTeam
The certificate request is displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIDEjCCAfoCAQAwbzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDDAKBgNVBAoMA1RBQzEQMA4GA1UECwwHc2FuVGVhbTElMCMGA1UEAwwc
RjI0MS0xNS0xMC05MTQ4VC0yLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJxGBpaX7j1S5rtLfZhttgvcvDPeXrtFCwOwrSSshPnJfzKN
ZFxzqTtyTSZpTUApfhd2QEDu+rdz+5RB4LF6cP5YNJeiYwQattf65QFfxWffFEuk
BSSvkBwx7y0Bna0fW7rMhDgVF5c9Cj2qNItwkO4Wxx56Guzn/iQGbGQ8Ak3YA/mZ
6lwl4x8Xj15jHwPrg57HB0IJoVFta0SV7DRsCwguq7Vq3CxViQSgdlOn4op699fn
7mENvOFHUfZhPF+YgsUakGeTcJpebu524kg4nZH1eiu9mlrs9VrU0d2qG7Ez+Goi
+GFD0NrauCQSvREpk7dv7l8jMk+tYR6u3ETFYYUCAwEAAaBeMBkGCSqGSIb3DQEJ
BzEMDAphYmNkZWYxMjM0MEEGCSqGSIb3DQEJDjE0MDIwMHYDVR0RAQH/BCYwJIIc
RjI0MS0xNS0xMC05MTQ4VC0yLmNpc2NvLmNvbYcEwKgBCjANBgkqhkiG9w0BAQsF
AAOCAQEAcBrh5xObTI/SOJ7DLm9sf5rfYFaJ0/1BafKqi2Dp3QPLMIa1jydZwz4q
NdNj7Igb4vZPVv/KBrJCibdjEJUn/YiGMST9PFQLys/Qm0fhQmsWcDxDX5xkE+/x
jZ+/8o5W/p6fPV4xT6sGDydjhA5McYr1o3grj0iPWloP+BaDpZgLpIoUHQygk8RB
SJbRR48QKl6pOVwcLPMXWy4w9Yp24hoJ8LI4Ll10D+urpyeEu0IpXywQdOJShQ3S
LWDEgVQSOhFQ+L7c+GGhnrXNXBD37K5hQ2mwrSIqI0FjDQMfzsBDe8bnDqx/HlLa
EP0sjBxo5AxmGon3ZEdlj6ivoyCA/A==
```

```
-----END CERTIFICATE REQUEST-----
```

Step 5

Installing Identity Certificates

Note: The maximum number of identify certificates that you can configure on a switch are 16.

```
switch# configure terminal
switch(config)# crypto ca import <trustpointName> certificate
input (cut & paste) certificate in PEM format: -----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= --
---END CERTIFICATE-----
```

Step 6

Save the configuration

```
switch# copy running-config startup-config
```

Verify

```
switchName# show crypto ca certificates

Trustpoint: <trustpointName>

certificate: ---> Identity Certificate
subject= /CN=CP-SAND-MDS-A.example.com
issuer= /C=GB/O=England/CN=Utility CA1
serial=16D34BA800004441C69D
notBefore=Nov 15 08:11:47 2021 GMT
notAfter=Nov 14 08:11:47 2023 GMT
SHA1 Fingerprint=03:E0:73:FE:31:C5:4A:84:C0:77:21:0F:3A:A0:05:29:55:FF:9B:7E
purposes: sslserver sslclient ike

CA certificate 0: ---> CA Certificate of Sub CA
subject= /C=GB/O=England/CN=Eng Utility CA1
issuer= /C=GB/O= England/CN=EngRoot CA
```

```
serial=616F2990AB000078776000002
notBefore=Aug 14 11:22:48 2012 GMT
notAfter=Aug 14 11:32:48 2022 GMT
SHA1 Fingerprint=DF:41:1D:E7:B7:AD:6F:3G:05:F4:E9:99:B2:9F:9C:80:73:83:1D:B4
purposes: sslserver sslclient ike

CA certificate 1: ---> CA Certificate of Root CA
subject= /C=GB/O=England/CN=Eng Root CA
issuer= /C=GB/O=Bank of England/CN=Eng Root CA
serial=435218BABA57D57774BFA7A37A4E54D52
notBefore=Aug 14 10:08:30 2012 GMT
notAfter=Aug 14 10:18:09 2032 GMT
SHA1 Fingerprint=E3:F9:85:AC:1F:66:22:7C:G5:36:2D:89:5A:B4:3C:06:0E:2A:DB:13
purposes: sslserver sslclient ike

switchName# show crypto key mypubkey rsa
key label: <rsaKeyPairName>
key size: 2048
exportable: yes
key-pair already generated

switchName# show crypto ca crl <trustpointName>
Trustpoint: <trustpointName>
================================================================================
========================
```

Limitations and Caveats

Maximum Limits for CA and Digital Certificate

Feature	Maximum Limit
Trust points declared on a switch	16
RSA key-pairs generated on a switch	16
RSA key-pair size	4096 bits
Identity certificates configured on a switch	16
Certificates in a CA certificate chain	10
Trust points authenticated to a specific CA	10

Default Settings

Parameters	Default
Trust point	None
RSA key-pair	None
RSA key-pair label	Switch FQDN
RSA key-pair modulus	512
RSA key-pair exportable	Yes
Revocation check method of trust point	CRL

Caveats

Cisco bug ID CSCvo43832 - MDS 9000 Certificate Signing Request (CSR) does not include all Distinguished Name (DN) fields

Cisco bug ID CSCvt46531 - Need to document PKI 'trustpool' commands

Cisco bug ID CSCwa77156 - Cisco MDS 9000 Series Security Configuration Guide, Release 8.x Needs Update on Password Character

Cisco bug ID CSCwa54084 - 'Subject Alternate Name' is incorrect in CSR generated by NX-OS