MDS 9000 스위치에 신뢰 지점 구성 및 인증서 설치

목차

소개

이 문서에서는 MDS 스위치의 신뢰 지점 및 인증서 컨피그레이션에 대한 컨피그레이션 단계에 대해 설명합니다.

배경 정보

PKI(Public Key Infrastructure) 지원은 Cisco MDS(Multilayer Director Switch) 9000 제품군 스위치에서 네트워크의 보안 통신을 위해 디지털 인증서를 얻고 사용할 수 있는 수단을 제공합니다. PKI 지원은 IPsec(IP Security), IKE(Internet Key Exchange) 및 SSH(Secure Shell)를 위한 관리 편의성과 확장성을 제공합니다.

사전 요구 사항

스위치의 호스트 이름 및 IP 도메인 이름이 아직 구성되지 않은 경우 이를 구성해야 합니다.

```
switch# configuration terminal
switch(config)# switchname <switchName>
SwitchName(config)# ip domain-name example.com
```
참고: 인증서를 생성한 후 IP 호스트 이름 또는 IP 도메인 이름을 변경하면 인증서가 무효화될 수 있습니다.

관련 키워드가 거의 없음

신뢰 지점 : 로컬 RSA 키 쌍, CA 공용 인증서, CA에서 스위치에 발급한 ID 인증서 등 신뢰할 수 있는 CA(Certificate Authority)에 대한 정보를 포함하는 로컬로 구성된 개체입니다. 여러 신뢰 지점을 구성하여 여러 CA의 스위치 ID 인증서를 등록할 수 있습니다. 신뢰 지점의 전체 ID 정보를 암호로 보호된 PKCS12 표준 형식의 파일로 내보낼 수 있습니다. 나중에 동일한 스위치(예: 시스템 충돌 후) 또는 교체 스위치로 가져올 수 있습니다. PKCS12 파일의 정보는 RSA 키 쌍, ID 인증서 및 CA 인증서(또는 체인)로 구성됩니다.

CA 인증서: 이 인증서는 CA(Certification Authority)에서 자체와 관련하여 발급한 인증서입니다. 설정에 중간 또는 하위 CA가 있을 수 있습니다. 이 경우 중간 또는 하위 CA 공용 인증서도 참조할 수 있습니다.

CA(Certificate Authorities): 인증서 요청을 관리하고 호스트, 네트워크 디바이스 또는 사용자와 같은 엔터티에 ID 인증서를 발급하는 디바이스입니다. CA는 이러한 엔터티에 대한 중앙 집중식 키 관리를 제공합니다.

RSA 키 쌍 : 스위치에서 cli로 생성되고 신뢰 지점과 연결됩니다. 스위치에 구성된 각 신뢰 지점에 대해 고유한 RSA 키 쌍을 생성하여 신뢰 지점과 연결해야 합니다.

CSR(Certification Signing request) 스위치에서 생성되어 CA로 전송되어 서명되는 요청입니다. 이 CSR에 대해 CA는 ID 인증서를 다시 보냅니다.

ID 인증서: CSR이 생성되는 스위치에 대해 인증 기관에서 서명하고 발급하는 인증서입니다. CSR이 CA에 제출되면 CA 또는 관리자가 이메일 또는 웹 브라우저를 통해 ID 인증서를 제공합니다. ID 인증서를 MDS 신뢰 지점에 붙여넣으려면 표준 PEM(base64) 형식이어야 합니다.

요구 사항

루트 CA .

하위 CA 인증서(ID 인증서가 하위 CA에 의해 서명된 경우) 이 경우 하위 CA의 CA 인증서도 스위치에 추가해야 합니다.

ID 인증서

구성

1단계

RSA 키 쌍 생성

```
switchName# configure terminal
```

```
switchName(config)# crypto key generate rsa label <rsaKeyPairName> exportable modulus xxx
```
(유효한 모듈러스 값은 (기본값) 512, 768, 1024, 1536, 2048 및 4096입니다.)

2단계

CA 신뢰 지점을 생성하고 RSA 키 쌍을 신뢰 지점과 연결

키 쌍 생성 중에 지정된 항목이 없는 경우 스위치 FQDN이 기본 키 레이블로 사용됩니다.

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

3단계

신뢰 지점 인증 기관 인증

인증 중인 CA가 자체 서명된 CA가 아닌 경우 CA 인증 단계 중에 인증 체인에 있는 모든 CA의 CA 인증서 전체 목록을 입력해야 합니다. 이를 인증 중인 CA의 CA 인증서 체인이라고 합니다. CA 인증서 체인의 최대 인증서 수는 10입니다.

루트 CA만 있는 경우

```
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
```
내부 또는 하위 CA가 있는 경우

다음과 같이 인증서가 제공됩니다.

```
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(파란색 텍스트) -> CA 인증서에서 복사한 다음(텍스트 편집기에서 열림) 스위치 CLI에서 프롬프트가 표시되면 붙여넣습니다.

빨간색 텍스트 -> 인증서를 종료하기 위해 입력해야 합니다.

인증서에 오류가 있으면 이 오류가 발생합니다

```
failed to load or parse certificate
could not perform CA authentication
```

루트 CA 인증서를 추가하지 않고 하위 CA 인증서에서 인증을 시도하는 경우

```
incomplete chain (no selfsigned or intermediate cert)
```

```
could not perform CA authentication
```
모든 것이 좋다면

```
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
```

4단계

CSR (Certificate Signing Request) 생성

NX-OS 8.4(1x) 이전

```
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---
--
```
챌린지 비밀번호는 컨피그레이션과 함께 저장되지 않습니다. 이 비밀번호는 인증서를 폐기해야 하는 경우에 필요하므로 이 비밀번호를 기억해야 합니다.

참고: 암호에는 '$' 문자를 사용하지 마십시오. 이로 인해 CSR에 오류가 발생합니다.

다음부터 복사

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

```
-----END CERTIFICATE REQUEST-----
```
이것을 스위치 외부에 저장하십시오. 이메일 또는 다른 방법을 통해 루트 CA 또는 하위 CA(서명된 것 중 하나)에 전달해야 합니다. CA는 서명된 ID 인증서를 반환합니다.

NX-OS 8.4(1) 이상

Cisco 버그 ID CSCvo43832의 수정 사항으로 NX-OS 8.4(1)에서 등록 프롬프트가 변경되었습니다.

기본적으로 Subject Name(주체 이름)은 스위치 이름과 동일합니다.

등록 프롬프트는 대체 주체 이름 및 여러 DN 필드도 허용합니다.

참고: 예를 들어 DN 필드는 해당 문자 범위의 문자열을 수락할 수 있으므로 숫자로 프롬프트를 표시합니다. 예를 들어, State DN 프롬프트는 다음과 같이 말합니다.

State[1-128] 입력:

1~128자의 문자열을 사용합니다.

```
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-----
```

5단계

ID 인증서 설치

참고: 스위치에서 구성할 수 있는 ID 인증서의 최대 개수는 16개입니다.

```
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-----
```

6단계

설정 저장

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

다음을 확인합니다.

```
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>
================================================================================
========================
```

제한 사항 및 주의 사항

CA 및 디지털 인증서에 대한 최대 제한

기능	최대 한도
스위치에 선언된 신뢰 지점	16
스위치에서 생성된 RSA 키 쌍	16
RSA 키 쌍 크기	4096비트
스위치에 구성된 ID 인증서	16
CA 인증서 체인의 인증서	10
특정 CA에 인증된 신뢰 지점	10

기본 설정

매개변수	기본값
신뢰 지점	없음
RSA 키 쌍	없음
RSA 키 쌍 레이블	스위치 FQDN
RSA 키 쌍 모듈러스	512
내보낼 수 있는 RSA 키 쌍	예
신뢰 지점의 해지 확인 방법	CRL

경고

Cisco 버그 ID CSCvo43832 - MDS 9000 CSR(Certificate Signing Request)에 모든 DN(Distinguished Name) 필드가 포함되지 않음

Cisco 버그 ID CSCvt46531 - PKI 'trustpool' 명령을 문서화해야 함

Cisco 버그 ID CSCwa77156 - Cisco MDS 9000 Series 보안 컨피그레이션 가이드, 릴리스 8.x Needs Update on Password Character

Cisco 버그 ID CSCwa54084 - NX-OS에 의해 생성된 CSR에서 '주체 대체 이름'이 잘못되었습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.