

# 인증서 문제로 인한 ASA Smart Licensing 실패 확인

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[Syslogs 및 디버그 출력](#)

[솔루션](#)

[다음을 확인합니다.](#)

[루트 CA 인증서 변경 - 2018년 10월](#)

[ASA를 실행하는 4100/9300 플랫폼](#)

[해결 단계](#)

[FIPS\(Federal Information Processing Standards\) 준수가 필요한 ASA 소프트웨어 설치](#)

[관련 정보](#)

---

## 소개

이 문서에서는 인증서 핸드셰이크 실패로 인한 ASA Smart Licensing 실패를 확인하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

이 문서에서는 tools.cisco.com을 호스트하는 웹 서버가 다른 루트 CA(Certificate Authority) 인증서로 마이그레이션되는 2016년 3월과 2018년 10월에 발생한 변경 사항을 해결하는 방법에 대해 설명합니다. 마이그레이션 후 일부 ASA(Adaptive Security Appliance) 디바이스는 ID 토큰을 등록하거나 현재 권한 부여를 갱신하려고 시도할 때 Smart Software Licensing Portal(tools.cisco.com에서 호스팅됨)에 연결하지 못합니다. 이는 인증서 관련 문제로 확인되었습니다. 특히 ASA에 제공되는 새 인증서는 ASA에서 예상한 것과 다른 중간 CA에서 서명하고 미리 로드되어 있습니다.

## 문제

ASAv를 Smart Software Licensing Portal에 등록하려고 시도하면 연결 또는 통신 실패와 함께 등록이 실패합니다. show license registration 및 call-home test profile license 명령은 이러한 출력을 보여줍니다.

```
<#root>
```

```
ASAv#
```

```
show license registration
```

```
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Last Retry Start Time: Mar 22 13:26:32 2016 UTC.  
Next Scheduled Retry Time: Mar 22 13:45:31 2016 UTC.  
Number of Retries: 1.  
Last License Server response time: Mar 22 13:26:32 2016 UTC.  
Last License Server response message:
```

```
Communication message send response error
```

```
<#root>
```

```
ASAv#
```

```
call-home test profile License
```

```
INFO: Sending test message to DDCEService  
ERROR: Failed:
```

```
CONNECT_FAILED(35)
```

그러나 ASAv는 tools.cisco.com을 확인하고 TCP ping을 사용하여 TCP 포트 443에 연결할 수 있습니다.

## Syslogs 및 디버그 출력

등록을 시도한 후 ASAv의 Syslog 출력에서는 다음을 표시할 수 있습니다.

```
<#root>
```

[%ASA-3-717009](#): Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name: cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name: ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .

[%ASA-3-717009](#): Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 513FB9743870B73440418699FF, subject name:

cn=Symantec Class 3 Secure Server CA - G4

,ou=Symantec Trust Network,o=Symantec Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network, o=VeriSign\, Inc.,c=US .

자세한 내용을 보려면 다른 등록을 시도하는 동안 다음 debug 명령을 실행하십시오. SSL(Secure Socket Layer) 오류가 표시됩니다.

```
debug license 255
debug license agent all
debug call-home all
debug ssl 255
```

특히 이 메시지는 해당 출력의 일부로 표시됩니다.

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
failed@s3_clnt.c:1492
```

기본 ASA v 컨피그레이션에는 주체 이름 "cn=Verisign Class 3 Secure Server CA - G3"에 인증서가 로드되고 발급된 \_SmartCallHome\_ServerCA라는 신뢰 지점이 있습니다.

<#root>

ASAv#

```
show crypto ca certificate
```

CA Certificate

Status: Available

Certificate Serial Number: 6ecc7aa5a7032009b8cebc2d491

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA1 with RSA Encryption

Issuer Name:

cn=VeriSign Class 3 Public Primary Certification Authority - G5

ou=(c) 2006 VeriSign\, Inc. - For authorized use only

ou=VeriSign Trust Network

o=VeriSign\, Inc.


c=US

Subject Name:

```
cn=VeriSign Class 3 Secure Server CA - G3
ou=Terms of use at https:// verisign /rpa (c)10
ou=VeriSign Trust Network
o=VeriSign\, Inc.
c=US
OCSP AIA:
  URL: http://ocsp verisign
CRL Distribution Points:
  [1] http://crl verisign/pca3-g5.crl
Validity Date:
  start date: 00:00:00 UTC Feb 8 2010
  end   date: 23:59:59 UTC Feb 7 2020
Associated Trustpoints: _SmartCallHome_ServerCA
```

그러나 이전 syslog에서 ASA는 "cn=Symantec Class 3 Secure Server CA - G4"라는 중간 관리자가 서명한 Smart Software Licensing 포털에서 인증서를 받는다는 것을 나타냅니다.

---

 참고: 제목 이름은 유사하지만 두 가지 차이점이 있습니다. 첫째는 Verisign과 Symantec이고, 둘째는 G3과 G4입니다.

---

## 솔루션

ASAv에서 체인을 검증하려면 적절한 중간 및/또는 루트 인증서가 포함된 신뢰 풀을 다운로드해야 합니다.

버전 9.5.2 이상에서는 ASAv에 오후 10시(디바이스 로컬 시간 기준) 자동으로 가져오도록 구성된 신뢰 풀이 있습니다.

```
<#root>
```

```
ASAv#
```

```
sh run crypto ca trustpool
```

```
crypto ca trustpool policy
  auto-import
```

```
ASAv#
```

```
sh run all crypto ca trustpool
```

```
crypto ca trustpool policy
  revocation-check none
  crl cache-time 60
  crl enforcenextupdate
  auto-import
  auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
  auto-import time 22:00:00
```

초기 설치이고 DNS(Domain Name System) 조회 및 인터넷 연결이 아직 설정되지 않은 경우 자동

가져오기가 성공하지 못하므로 수동으로 완료해야 합니다.

9.4.x와 같은 이전 버전에서는 신뢰 풀 자동 가져오기가 디바이스에 구성되지 않으며 수동으로 가져와야 합니다.

모든 버전에서 이 명령은 신뢰 풀 및 관련 인증서를 가져옵니다.

```
<#root>
```

```
ASAv#
```

```
crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Root file signature verified.
```

```
You are about to update the current trusted certificate pool
```

```
with the 17145 byte file at http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Do you want to continue? (y/n)
```

```
Trustpool import:
```

```
  attempted: 14
```

```
  installed: 14
```

```
  duplicates: 0
```

```
  expired: 0
```

```
  failed: 0
```

## 다음을 확인합니다.

manual 명령으로 신뢰 풀을 가져오거나 현지 시간으로 오후 10시 이후에 신뢰 풀을 가져오면 이 명령은 신뢰 풀에 설치된 인증서가 있는지 확인합니다.

```
<#root>
```

```
ASAv#
```

```
show crypto ca trustpool policy
```

```
14 trustpool certificates installed
```

```
Trustpool auto import statistics:
```

```
  Last import result: FAILED
```

```
  Next scheduled import at 22:00:00 UTC Wed Mar 23 2016
```

```
Trustpool Policy
```

```
  Trustpool revocation checking is disabled
```

```
  CRL cache time: 60 seconds
```

```
  CRL next update field: required and enforced
```

```
  Automatic import of trustpool certificates is enabled
```


```
  Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
  Download time: 22:00:00
```


```
  Policy Overrides:
```

```
    None configured
```

---

 참고: 이전 출력에서 마지막으로 자동으로 시도했을 때 DNS가 작동하지 않아 마지막 자동 업데이트 가져오기가 실패했으므로 마지막 자동 가져오기 결과가 실패한 것으로 표시됩니다. 그

---

 러나 수동 신뢰 풀 업데이트가 실행되고 신뢰 풀을 성공적으로 업데이트했습니다. 따라서 설치된 인증서가 14개 표시됩니다.

신뢰 풀이 설치된 후 ASA를 Smart Software Licensing 포털에 등록하기 위해 token registration 명령을 다시 실행할 수 있습니다.

```
<#root>
```

```
ASAv#
```

```
license smart register idtoken id_token force
```

ASAv가 Smart Software Licensing 포털에 이미 등록되었지만 권한 부여 갱신이 실패한 경우 이를 수동으로 시도할 수도 있습니다.

```
<#root>
```

```
ASAv#
```

```
license smart renew auth
```

## 루트 CA 인증서 변경 - 2018년 10월

tools.cisco.com에 대한 루트 CA 인증서가 2018년 10월 5일 금요일에 변경되었습니다.

[http://www.cisco.com/security/pki/trs/ios\\_core.p7b](http://www.cisco.com/security/pki/trs/ios_core.p7b)에 대한 통신이 허용되지 않을 경우 현재 구축된 ASA 버전 9.6(2) 이상 및 ASA를 실행 중인 Firepower 2100의 경우 이 변경의 영향을 받을 수 없습니다. 앞에서 언급한 모든 ASA 스마트 라이선스 플랫폼에서 기본적으로 활성화되는 인증서 자동 가져오기 기능이 있습니다. 'show crypto ca trustpool'의 출력에는 'QuoVadis Root CA 2' 인증서가 포함됩니다.

```
CA Certificate
```

```
Fingerprint: 5e397bddf8baec82e9ac62ba0c54002b
```

```
Issuer Name:
```

```
cn=QuoVadis Root CA 2
```

```
o=QuoVadis Limited
```

```
c=BM
```

```
Subject Name:
```

```
cn=QuoVadis Root CA 2
```

```
o=QuoVadis Limited
```

```
c=BM
```

신규 구축의 경우 'crypto ca trustpool import default' 명령을 실행하고 QuoVadis 인증서가 포함된 기본 Cisco 인증서 번들을 다운로드할 수 있습니다. 이 방법이 작동하지 않을 경우 인증서를 수동

으로 설치할 수 있습니다.

```
asa(config)# crypto ca trustpoint QuoVadisRootCA2
asa(config-ca-trustpoint)# enrollment terminal
asa(config-ca-trustpoint)# crl configure
asav(config-ca-crl)# crypto ca authenticate QuoVadisRootCA2
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTElMAkGA1UEBhMCQ0x
GTAXBgNVBAoTEFF1b1ZlZG1zIEExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZlZG1zIFJv
b3QgQ0EgMjAeFw0wNjExMjM0ODIzMDBaFw0zMTExMjQxODIzMDZNaMEUxCzAJBgNV
BAYTAKJNMRRkwFwYDVQKExBRdW9WYWRpcyBMAw1pdGVkMRswGQYDVQQDEXJRdW9W
YWRpcyBSb290IENBIDwggIiMAOGCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpL1A0ALa8DKYrwD4HIrkwZHR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKiFvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yk1vc/ulsrHHo1wtZn/qtmUIttKGA79dgw8eTvI02kfn/+NsRE8Scd3bB
rrcCaoF6qUWD4jXmuVbB1DePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9X0va7R+zdRcAitMOeGylZUtQofX1b0QQ7dsE/He3fbE+Ik/OXX1
ksOR1YqI0JDs3G3eicJlCzALDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUR5R/7mp/i
Ucw6UwxI5g69ybR2B1LmEROFcmMBOAENisgGQLodKcfts1WZvB1JdxnWQ5hYIiz
PtGo/KPaHbDRsSNU3OR2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/z0hD7osFRXq17PSorW+8oyWHhQPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyBNkr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc90tb+fVuI
yV77zGHciZn300QyNQ1iBJIWIENieJ0f70yHj+OsdWwIDAQABO4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAF8wCwYDVROPAQAQAgEGMBOGA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMZzB1gBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQ0xGTAXBgNVBAoTEFF1b1ZlZG1zIEExpbWl0ZWQxGzAZBgNVBAMT
E1F1b1ZlZG1zIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4Kfk2f
B1uornFdLwUvZ+YTRYPENvbzwcYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae4219NlmeYhP3ZRPx3UIHmFLTJJDQTYU/h2BwdBR5YM++CCJpNVjP4iH2B1
ff/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WPKjaJW1acvvFYfzbnB4vsKqBUSfU16Y8Zs10Q80m/DShcK+JDSV6IZUaUt10Ha
B0+pUNQqjZRG4T7w1POQADj10+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIoZc
hLsib9D45MY56QSIpM0661V6bYCZJPVsAfv417CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQ1fe6yJvmjqIBxdZmv31h8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkgoi3XZZenMfvJ2II4pEZXLxId26F0KCl3GBUzGpn/Z9Yr9y
4a0THcyKJlOJOND01w2AFrR4pTqHTI2KpdVG1/IsELm8VCLAABpQ570su9t+Oza
8e0x79+Rj1QqCyXBjhnEUhAFZdwCEOrCMc0u
-----END CERTIFICATE-----
```

quit

INFO: Certificate has the following attributes:  
Fingerprint: 5e397bdd f8baec82 e9ac62ba 0c54002b  
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

## ASA를 실행하는 4100/9300 플랫폼

이 문제는 FXOS(Firepower eXtensible Operating System)를 통해 스마트 라이선싱 정보를 제공하는 ASA를 실행 중인 필드의 일부 4100/9300에 영향을 미쳤습니다.

영향을 받는 장치:

<#root>

```
FP9300-1-A-A-A /license # show license all
```

Smart Licensing Status

=====

Smart Licensing is ENABLED

Registration:

Status: REGISTERED

Smart Account: TAC Cisco Systems, Inc.

Virtual Account: CALO

Export-Controlled Functionality: Allowed

Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC

Last Renewal Attempt: FAILED on Oct 09 17:32:59 2018 UTC

Failure reason: Failed to authenticate server

## 해결 단계

문제를 해결하려면 새 신뢰 지점을 만들고 FXOS에 인증서 데이터를 입력해야 합니다.

<#root>

```
FPR-2-A /license # scope security
```

```
FPR-2-A /security # enter trustpoint QuoVadisRootCA2
```

```
FPR-2-A /security/trustpoint* # set certchain
```

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.

Trustpoint Certificate Chain: (THIS PART NEEDS TO BE COPY/PASTED)

>

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

```
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZlZG1zIEExpbW10ZWQxGzAZBgNVBAMTE1F1b1ZlZG1zIFJv
b3QgQ0EgMjAeFw0wNjExMjM0ODIzMDBaFw0zMTExMjM0ODIzMDZNaMEUxCzAJBgNV
BAYTAKJNMkRwFwYDVQQKEwBRdW9WYWRpcyBMAw1pdGVkMRswGQYDVQQDEwJRdW9W
YWRpcyBSb290IENBIDwggIiMAOGCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpL1A0ALa8DKYrWd4HIrkwZhr0In6spRIZL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKiFvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yk1vc/u1srHHo1wtZn/qtmUIttKGA79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbB1DePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9X0va7R+zdRcAi tMOeGylZUtQofX1b0QQ7dsE/He3fbE+Ik/OXX1
ksOR1YqI0JDs3G3eicJ1cZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUR5R/7mp/i
Ucw6UwI5g69ybR2B1LmEROfcmMDBOENisgGQLodKcfts1WZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU3OR2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/z0hD7osFRXq17PSorW+8oyWHhQPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNkr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc90tb+fVuI
yV77zGHciZn300QyNQ1iBJIWENieJ0f70yHj+0sdWwIDAQABO4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMBOGA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMZezB1gBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEwRTEL
```



```
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZG1zIEExpbW10ZWQxGzAZBgNVBAMT
E1F1b1ZhZG1zIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KfK2f
B1uornFdLwUvZ+YTRYPENvbzWCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae4219NlmeYhP3ZRPx3UIHmFLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2B1
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WPKjaJW1acvvFYfzZnB4vsKqBUsfU16Y8Zs10Q80m/DSHck+JDSV6IZUaUt10Ha
B0+pUnQjZRG4T7w1POQADj10+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIoZc
hLsib9D45MY56QSIPM0661V6bYCZJPVsAfV417CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQ1fe6yJvmjqIBxdZmv31h8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3GoI3XZZenMfvJ2II4pEZXNLxId26F0KC13GBuzGpn/Z9Yr9y
4a0THcyKJ1oJONDO1w2AFrR4pTqHTI2KpdVG1/IsELm8VCLAABpQ570su9t+0za
8e0x79+Rj1QqCyXBjHnEUhAFZdwCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF
```

<---manually type this on a new line after the ----END OF CERTIFICATE---- line and press ENTER

다음으로, 변경 사항을 커밋한 다음 라이선스를 갱신합니다.

```
FPR-2-A /security/trustpoint* # comm
FPR-2-A /security/trustpoint # scope license
FPR-2-A /license # scope licdebug
FPR-2-A /license/licdebug # renew
```

이제 라이선스가 갱신되었는지 확인해야 합니다.

```
<#root>
```

```
FP9300-1-A-A-A /license/licdebug # show license all
```

```
Smart Licensing Status
```

```
=====
```

```
Smart Licensing is ENABLED
```

```
Registration:
```

```
Status: REGISTERED
```

```
Smart Account: TAC Cisco Systems, Inc.
```

```
Virtual Account: CALO
```

```
Export-Controlled Functionality: Allowed
```

```
Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
```

```
Last Renewal Attempt: SUCCEEDED on Oct 09 17:39:07 2018 UTC
```

```
Next Renewal Attempt: Apr 07 17:39:08 2019 UTC
```

```
Registration Expires: Oct 09 17:33:07 2019 UTC
```

```
License Authorization:
```

```
Status: AUTHORIZED on Oct 09 17:39:12 2018 UTC
```

```
Last Communication Attempt: SUCCESS on Oct 09 17:39:12 2018 UTC
```

```
Next Communication Attempt: Nov 08 17:39:12 2018 UTC
```

# FIPS(Federal Information Processing Standards) 준수가 필요한 ASA 소프트웨어 설치

FIPS 규정준수가 필요한 ASA 기반 플랫폼의 경우, QuoVadis Root CA 2 인증서를 가져오면 서명 암호화 요구 사항을 준수하지 못할 수 있으며 이 메시지가 표시될 수 있습니다.

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate is not FIPS compliant.  
% Error in saving certificate: status = FAIL

FIPS 호환 ASA 설치의 해결 방법으로 HydrantID SSL ICA G2 중간 인증서를 가져옵니다. HydrantID SSL ICA G2 인증서는 다음에 표시되며 sha256WithRSAEncryption 서명 알고리즘 요구 사항을 준수합니다. 플랫폼을 기반으로 인증서를 로드하려면 이 문서에 나온 설명서를 참조하십시오.

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

```
MIIGxDCCBKyGAWIBAgIUdRcWd4PQQ361VsNX1G5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTElMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZlZG1zIEExpbW10ZWQxGzAZ
BgNVBAMTE1F1b1ZlZG1zIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xZzA1bG90BAQFAAOCAg8AMIICGKCAgEA9p1ZOA9+
H+tgdlN+STF7bd0xvnOERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rhn0+
Jt0NVJM41jVctf9qwacVduR7CEi0qJgpAUJyZUuB9IpfWF1Kz1403Leh6URuRZ43
RzHaRmNtzkxttGBu0tAg+i10uwiGAo9VQLgd0N1qQFcrbp97/f08ZiQiPrbhLxCZ
fXkYi3mktZVRFKXG62FHAuH1sLDXCKba3avDcUR7ykG4ZXcmp6k114UKa8JHOHPE
NYyr0R6oHELOGZMox1nQcFwuYMX9sJdAUU/9SQVXYA6u6Ytx1pZiC8qhXM1IE00T
Q9+q5ppffSUDMC4V/5If5A6snKVP78M8qd/RMVswcjMUMEnov+wykwCbDLD+IREM
A57XX+HojN+8XFTL9Jwge3z3Z1MwL7E54W3cI7f6cx05DVwoKxkdk2jRIg37oqS1
SU3z/bA9UXjHcT1/6BoLho2p9rWm6o1jANPeQuLHyGJ3hc19N8nDo2IATp70k1GP
kd1qhIgrdkki7gBpanMOK98hKMpdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jZoj4b+g+l+XU1SQ+9DWiuZtvfDW++k0BMCAwEAAaOCAZEwggGNMBIGA1UdEwEB
/wQIMAYBAf8CAQAwEAYDVR0gBHEwBzAIBgZngQwBAgEwCAYGZ4EMAQICMA4GDCsG
AQQBv1gAAmQBAjBJBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oewRyYW50aWQuY29tL3N1cHBvcnQvcmluL3NpdG9yeTB5BggrBgEFBQcB
AQRmMGQwKgYIKwYBBQUHMAAGHmhOdHA6Ly9vY3NwLnF1b1ZlZG1zZ2xvYmFsLmNv
bTA2BggrBgEFBQcCwAoYqAHR0cDovL3RydXN0LnF1b1ZlZG1zZ2xvYmFsLmNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAfbG90BAQFAAOCAgEAlraik8EDDUkpAnIOaj09/r4dpj/Zry76
6SH1oYPo7eTGzpdDanPMeGmSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqf1mx9qA1Fe9XcV1ZrUu
9hph+/MfwMrUju+VPL5U7hZvUpp66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9w1YDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
```

83Hic/2Xgwksf1DKS3/z5nTzhsUIpCpwkN6nHp6gmA8JBXoU1KQz4eYHJCq/ZyC+  
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtfwJPqdf+/9RgLriXeFTqwe  
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEqgm1WG5mWW1PxHstu  
Ew9jBMcJ6wjQc8He9rSUMrhBr0HyhckdC99RgEvpCZpV2XL4nPPrTI2ki/c9xQb9  
kmhVGonSXY5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUSTRxOsRfJozU0R9ysyP  
EZAHFZ3Zivg2BaD4t0IS08/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c  
9vkaKoPvX4w=  
-----END CERTIFICATE-----

## 관련 정보

- [Cisco 기술 지원 및 다운로드](#)

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.