Ascertain ASA Smart Licensing Failures Due to Certificate Issues

Contents

Introduction

This document describes how to ascertain ASA Smart Licensing failures that are due to a certificate handshake failure.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes how to address a change that occurred on March 2016 and October 2018, in which webservers that host tools.cisco.com were migrated to a different root Certificate Authority (CA) certificate. After that migration, some ASA (Adaptive Security Appliance) devices fail to connect to the Smart Software Licensing Portal (which is hosted on tools.cisco.com) when they register an ID token or while they attempt to renew current authorizations. This was determined to be a certificate-related issue. Specifically, the new certificate that is presented to the ASA is signed by a different Intermediate CA than the ASA expects and has preloaded.

Problem

When an attempt is made to register an ASAv to the Smart Software Licensing Portal, the registration fails with a connection or communication failure. The **show license registration** and **call-home test profile license** commands show these outputs.

```
<#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)
```

However, the ASAv can resolve tools.cisco.com and connect on TCP port 443 with a TCP ping.

Syslogs and Debug Output

Syslog output on the ASAv after an attempted registration can show this:

```
<#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 .
```

For further information, run these debug commands while you attempt another registration. Secure Socket Layer errors are seen.

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

Specifically, this message is seen as part of that output:

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

In the default ASAv configuration, there is a trustpoint called _SmartCallHome_ServerCA that has a certificate loaded and issued to the subject name "cn=Verisign Class 3 Secure Server CA - G3".

<#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
```

However, in the the previous syslogs, the ASA indicates that it gets a certificate from the Smart Software Licensing Portal signed by an intermediate called "cn=Symantec Class 3 Secure Server CA - G4".

> **Note**: The subject names are similar, but have two differences; Verisign vs. Symantec at the beginning and G3 vs. G4 at the end.

Solution

The ASAv needs to download a trustpool that contains the proper intermediate and/or root certificates in order to validate the chain.

In Version 9.5.2 and later, the ASAv has the trustpool configured to auto-import at 10:00 PM device local time:

<#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
```

If this is an initial installation, and Domain Name System (DNS) lookups and Internet connectivity have not been up at that time yet, then the auto-import has not succeeded and needs to be completed manually.

On older versions, such as 9.4.x, the trustpool auto-import is not configured on the device and needs to be imported manually.

On any version, this command imports the trustpool and relevant certificates:

<#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
```

Verify

Once the trustpool is imported either by the manual command or it is after 10:00 PM local time, this command verifies that there are installed certificates in the trustpool:

<#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
```

> **Note**: In the previous output the last auto-update import failed since DNS was not operational the last time it attempted automatically, so it still shows the last auto-import result as failed. However, a manual trustpool update was run and did successfully update the trustpool (which is why it shows 14 certificates installed).

After the trustpool is installed, the token registration command can be run again in order to register the ASAv with the Smart Software Licensing Portal.

<#root>

ASAv#

license smart register idtoken *id_token* force

If the ASAv was already registered to the Smart Software Licensing Portal, but authorization renewals failed, those can also be attempted manually.

<#root>

```
ASAv#
```

license smart renew auth

Root CA Certificate Change - October 2018

The root CA certificate for tools.cisco.com was changed on Friday, October 5th, 2018.

The currently deployed ASAvâ€™s version 9.6(2) and later and Firepower 2100â€™s running ASA cannot be affected by this change if communication to http://www.cisco.com/security/pki/trs/ios_core.p7b is not allowed. There is a certificate auto-import feature that is enabled by default on all ASA Smart Licensed platforms mentioned before. The output of â€˜show crypto ca trustpoolâ€™ contains the â€˜QuoVadis Root CA 2â€™ certificate:

```
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
```

For new deployments, you can issue the â€˜crypto ca trustpool import defaultâ€™ command and download the default Cisco cert bundle that contains the QuoVadis cert. If that doesnâ€™t work you can install the cert manually:

```
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+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
```

```
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+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
```

4100/9300 Platforms Running ASA

This issue has affected some 4100/9300s in the field that are running ASA which relies on Firepower eXtensible Operating System (FXOS) to provide Smart Licensing information:

Affected unit:

<#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

Resolution Steps

To resolve, you need to create a new trustpoint and enter the certificate data in FXOS:

<#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
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
>ENDOFBUF
```

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

Next, commit the change and then renew the license:

```
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
```

You must now verify that the licensing has been renewed:

<#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
  Communication Deadline: Jan 07 17:33:11 2019 UTC
```

ASA Software Installations That Require Federal Information Processing Standards (FIPS) Compliance

For ASA-based platforms that require FIPS compliance, the import of the QuoVadis Root CA 2 certificate can fail for nonconformance to signature cryptographic requirements and this mesage can be displayed:

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

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

As a workaround for FIPS compliant ASA installations, import the HydrantID SSL ICA G2 intermediate certificate. The HydrantID SSL ICA G2 certificate is shown next and complies with sha256WithRSAEncryption signature algorithm requirements, refer to the documentation shown on this article in order to load the certificate based on your platform:

```
-----BEGIN CERTIFICATE-----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNXlG5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZ
```

```
BgNVBAMTElF1b1ZhZGlzIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xCzAJBgNVBAYTAlVTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2
YWxhbmNoZSBDbG91ZCBDb3Jwb3JhdGlvbikxHTAbBgNVBAMTFEh5ZHJhbnRJRCBT
U0wgSUNBIEcyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA9p1ZOA9+
H+tgdln+STF7bdOxvnOERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rhn0+
Jt0NVJM41jVctf9qwacVduR7CEi0qJgpAUJyZUuB9IpFWF1Kz14O3Leh6URuRZ43
RzHaRmNtzkxttGBuOtAg+ilOuwiGAo9VQLgdONlqQFcrbp97/fO8ZIqiPrbhLxCZ
fXkYi3mktZVRFKXG62FHAuH1sLDXCKba3avDcUR7ykG4ZXcmp6kl14UKa8JHOHPE
NYyr0R6oHELOGZMox1nQcFwuYMX9sJdAUU/9SQVXyA6u6YtxlpZiC8qhXM1IE00T
Q9+q5ppffSUDMC4V/5If5A6snKVP78M8qd/RMVswcjMUMEnov+wykwCbDLD+IReM
A57XX+HojN+8XFTL9Jwge3z3ZlMwL7E54W3cI7f6cxO5DVwoKxkdk2jRIg37oqSl
SU3z/bA9UXjHcTl/6BoLho2p9rWm6oljANPeQuLHyGJ3hc19N8nDo2IATp70klGP
kd1qhIgrdkki7gBpanMOK98hKMpdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jZoj4b+g+l+XU1SQ+9DWiuZtvfDW++k0BMCAwEAAaOCAZEwggGNMBIGA1UdEwEB
/wQIMAYBAf8CAQAweAYDVR0gBHEwbzAIBgZngQwBAgEwCAYGZ4EMAQICMA4GDCsG
AQQBvlgAAmQBAjBJBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oeWRyYW50aWQuY29tL3N1cHBvcnQvcmVwb3NpdG9yeTByBggrBgEFBQcB
AQRmMGQwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLnF1b3ZhZGlzZ2xvYmFsLmNv
bTA2BggrBgEFBQcwAoYqaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAfBgNVHSMEGDAWgBQahGK8SEwzJQTU
7tD2A8QZRtGUazA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3JsLnF1b3ZhZGlz
Z2xvYmFsLmNvbS9xdnJjYTIuY3JsMB0GA1UdDgQWBBSYarYtLr+nqp/299YJr9WL
V/mKtzANBgkqhkiG9w0BAQsFAAOCAgEAlraik8EDDUkpAnIOajO9/r4dpj/Zry76
6SH1oYPo7eTGzpDanPMeGMuSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqfimx9qAlFe9XcVlZrUu
9hph+/MfWMrUju+VPL5U7hZvUpg66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9wlYDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
83Hic/2Xgwksf1DKS3/z5nTzhsUIpCpwkN6nHp6gmA8JBXoUlKQz4eYHJCq/ZyC+
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtfwJPqdf+/9RgLriXeFTqwe
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEqgm1WG5mWW1PxHstu
Ew9jBMcJ6wjQc8He9rSUmrhBr0HyhckdC99RgEvpcZpV2XL4nPPrTI2ki/c9xQb9
kmhVGonSXy5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUStRxOsRfJozU0R9ysyP
EZAHFZ3Zivg2BaD4tOISO8/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
-----END CERTIFICATE-----
```


Related Information

- **Cisco Technical Support & Downloads**