Third-Party Certificate Installation on Converged Access Wireless LAN Controllers

This document describes installing a certificate on Cisco Catalyst 3850 Series Switch. Also, it explains the process to install certificates on Converged Access and to use the certificate for authentication.

Note

- For more information on the commands used in this section, refer to Command Lookup Tool (for Registered Users only).
- To view an analysis of show command output, refer to the Output Interpreter.
- After you receive a user certificate from a vendor, you receive the following entities in the Privacy Enhanced Mail (PEM) format:
  - User certificate
  - Rivest-Shamir-Adleman (RSA) key
  - Root certificate
- The installation process for the Cisco Catalyst 3850 Series Switch is different from the installation process for Cisco 5500 Series Wireless Controller.

Installing Third Party Certificates

Perform the following steps to install a third-party certificate:

Step 1 To install the trustpoint, use the following commands:

```
configure terminal
crypto pki trustpoint trustp1   <--- trustp1 is a word string any word can be used here.
```

```
(ca-trustpoint)#enrollment terminal pem
(ca-trustpoint)#exit
```

Step 2 To authenticate the trustpoint, perform the following:

1. Enter the **crypto pki authenticate** command.
   ```
   (config)#crypto pki authenticate trustp1
   Enter the base 64 encoded CA certificate.
   End with a blank line or the word "quit" on a line by itself
   ```
2. Copy and paste the user certificate. Ensure that the Begin Certificate and End Certificate lines are included.
3. Press **Enter** and then type *quit*.
   ```
   Trustpoint 'trustp1' is a subordinate CA and holds a non self signed
      cert
   Trustpoint 'trustp1' is a subordinate CA.
   but certificate is not a CA certificate.
   Manual verification required
   Certificate has the following attributes:

         Fingerprint MD5: EF9EE16F 535D51D4 0E5E9809 F48CF6EE
         Fingerprint SHA1: FB166D5D 5F301F93 3CA2015A F5745C52 46030D9E

   % Do you accept this certificate? [yes/no]:
   ```
4. Type *Yes*, when prompted.

Note To view the certificate, enter **show crypto pki trustpoint** command.

Step 3 To import the root certificate, perform the following:

1. Enter the following **crypto pki import** command:
   ```
   (config)crypto pki import trustroot pem terminal passphrase
   % Enter PEM-formatted CA certificate.
   % End with a blank line or "quit" on a line by itself
   ```
2. Copy and paste the root certificate.
3. Press **Enter**, and type quit.
   ```
   % Enter PEM-formatted encrypted private General Purpose key.
   % End with "quit" on a line by itself
   ```
4. Copy and paste the RSA key, press Enter, and then type quit.
   ```
   % Enter PEM-formatted General Purpose certificate.
   % End with a blank line or "quit" on a line by itself
   ```
5. Copy and paste the user certificate and press Enter.
6. The certificate import is successfully completed.

   The certificate can also be retrieved, converted to .p12 format, and imported with the crypto pki import command on the controller. To import the certificate, use the following command:
   ```
   crypto pki import name pkcs12 tftp: // url password
   ```

Example for Installing Third Party Certificates

The following is an example to install a certificate:

```
(config)#crypto pki trustpoint verisign.com ?
  <cr>

(config)#crypto pki trustpoint verisign.com
(ca-trustpoint)#enrollment terminal pem
(ca-trustpoint)#exit

(config)#crypto pki authenticate verisign.com  <--- This is the USER CERTIFICATE

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

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

MIIFczCCBFugAwIBAgIQQRtXHG8Y534dY6EkS6gHiDANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzMwHhcNMTIwNzIz
MDAwMDAwWhcNMTQwODE5MjM1OTU5WjCBpTELMAkGA1UEBhMCVVMxETAPBgNVBAgT
CE1hcnlsYW5kMRIwEAYDVQQHFAlCYWx0aW1vcmUxJzAlBgNVBAoUHlQuIFJvd2Ug
UHJpY2UgQXNzb2NpYXRlcywgSW5jLjEgMB4GA1UECxQXSW52ZXN0bWVudCBUZWNo
bm9sb2dpZXMxJDAiBgNVBAMUG3dsZ3Vlc3RjaGVjay50cm93ZXByaWNlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJvJpXRzliY8d11vCZcChi2c
5uIn0TnUhR8QQrw0kstROJTtmSJpaOVTwOb0HoLgC8lH2VRAIxvxXdi49AQpYoY5
z8UxeH29XqKIkYR399K7/L9W9caYwWSjn4eLq1lk0GLmGMtE7T4I2bhssAgfV2+k
kpS4RymNUdSgCWzDrm575xyzVCciOGUPjTxpB5U7sWPASqpEvgoX88fPPpTtzTJl
XE1n1eRIcbE1z1/wpRxlFH4XMPtL79F8FQTWZ0MvMzyLEriR+dHXxtbBUkCPvgFY
7Nruz4Rj5Uk4S33G1EVvExfMF/wa+rtFU4RwlV4DESbrhSFhLeEruFfpzOWhMj0C
AwEAAaOCAYswggGHMCYGA1UdEQQfMB2CG3dsZ3Vlc3RjaGVjay50cm93ZXByaWNl
LmNvbTAJBgNVHRMEAjAAMA4GA1UdDwEB/wQEAwIFoDBFBgNVHR8EPjA8MDqgOKA2
hjRodHRwOi8vU1ZSU2VjdXJlLUczLWNybC52ZXJpc2lnbi5jb20vU1ZSU2VjdXJl
RzMuY3JsMEMGA1UdIAQ8MDowOAYKYIZIAYb4RQEHNjAqMCgGCCsGAQUFBwIBFhxo
dHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3BzMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAfBgNVHSMEGDAWgBQNRFwWU0TBgn4dIKsl9AFj2L55pTB2Bggr
BgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMy1haWEudmVyaXNpZ24u
Y29tL1NWUlNlY3VyZUczLmNlcjANBgkqhkiG9w0BAQUFAAOCAQEAReYq+92lCiDX
8hG4FyAEsvc1lDEhGUVy0URn8U7nYF7kN4NZdUKHFX86izPYJiC0yB6SsbMtz68t
r8OwPFUOzRvPfhzivtn/mL1TcEPjWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3ey1zYVVVCqavw2BsvPAcklqvx7stSjQHtAoXeL9WBCfPlI5w/Fd6OP5J6XVBF
CHgAauqR5hONWge9M4xh6jDC0kLcrRcFXLbcdtS0DXHVBfBfDipoM2yRDdaVOwfZ
CrTL3cZA9HLzI3QtPkzLC7RrRP8r3bBkIYMNyGO465fe9IMV3MgTFey8G26mn+R5
iG3ddRLhhA==
-----END CERTIFICATE-----

Trustpoint 'verisign.com' is a subordinate CA and holds a non self signed cert
Trustpoint 'verisign.com' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:

       Fingerprint MD5: EF9EE16F 535D51D4 0E5E9809 F48CF6EE
      Fingerprint SHA1: FB166D5D 5F301F93 3CA2015A F5745C52 46030D9E

% Do you accept this certificate? [yes/no]:
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#s
% Incomplete command.

# show crypto pki trustpoints

Trustpoint verisign.com:
    Subject Name:
```

```
    cn=ciscouser
    ou=ciscotech
    o=ciscoj
    l=Bangalore
    c=IN
          Serial Number (hex): 411B571C6F18E77E1D63A1244BA80788
    Certificate configured.

(config)#  crypto pki import VeriG3 pem terminal password
% Enter PEM-formatted CA certificate.         <--- This is the ROOT CERTIFICATE
% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE-----
MIIF7DCCBNSgAwIBAgIQbsx6pacDIAm4zrz06VLUkTANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMjAwMjA3MjM1OTU5WjCBtTEL
MAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2UgYXQg
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMC0GA1UEAxMmVmVy
aVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCxh4QfwgxF9byrJZenraI+nLr2wTm4i8rCrFbG
5btljkRPTc5v7QlK1K9OEJxoiy6Ve4mbE8riNDTB81vzSXtig0iBdNGIeGwCU/m8
f0MmV1gzgzszChew0E6RJK2GfWQS3HRKNKEdCuqWHQsV/KNLO85jiND4LQyUhhDK
tpo9yus3nABINYYpUHjoRWPNGUFP9ZXse5jUxHGzUL4os4+guVOc9cosI6n9FAbo
GLSa6Dxugf3kzTU2s1HTaewSulZub5tXxYsU5w7HnO1KVGrJTcW/EbGuHGeBy0RV
M5l/JJs/U0V/hhrzPPptf4H1uErT9YU3HLWm0AnkGHs4TvoPAgMBAAGjggHfMIIB
2zA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTASBgNVHRMBAf8ECDAGAQH/AgEAMHAGA1UdIARpMGcwZQYLYIZIAYb4
RQEHFwMwVjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw
czAqBggrBgEFBQcCAjAeGhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMDQG
A1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMtZzUu
Y3JsMA4GA1UdDwEB/wQEAwIBBjBtBggrBgEFBQcBDARhMF+hXaBbMFkwVzBVFglp
bWFnZS9naWYwITAfMAcGBSsOAwIaBBSP5dMahqyNjmvDz4Bq1EgYLHsZLjAlFiNo
dHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvLmdpZjAoBgNVHREEITAfpB0w
GzEZMBcGA1UEAxMQVmVyaVNpZ25NUEtJLTItNjAdBgNVHQ4EFgQUDURcFlNEwYJ+
HSCrJfQBY9i+eaUwHwYDVR0jBBgwFoAUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMwDQYJ
KoZIhvcNAQEFBQADggEBAAyDJO/dwwzZWJz+NrbrioBL0aP3nfPMU++CnqOh5pfB
WJ11bOAdG0z60cEtBcDqbrIicFXZIDNAMwfCZYP6j0M3m+oOmmxw7vacgDvZN/R6
bezQGH1JSsqZxxkoor7YdyT3hSaGbYcFQEFn0Sc67dxIHSLNCwuLvPSxe/20majp
dirhGi2HbnTTiN0eIsbfFrYrghQKlFzyUOyvzv9iNw2tZdMGQVPtAhTItVgooazg
W+yzf5VK+wPIrSbb5mZ4EkrZn0L74ZjmQoObj49nJOhhGbXdzbULJgWOw27EyHW4
Rs/iGAZeqa6ogZpHFt4MKGwlJ7net4RYxh84HqTEy2Y=
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,1E71580604A10032
xz3n4/odG8PFwe/FL6lhNmkXUgg09A82kupYuA1jWy4Pmz0gAk7fMTNBnrilk/Uq
c2WrM34tdURukNfYv3IbvkGa6QsTQu5sYZ+83Igsdsh0xOw/xJNvs6aaOnF0frNN
wiRYOS5QGf9+A98kEw0g66ye04C9XjR39+peSgmAchI4smAF486bK2xDRzlp2Ewi
bL+pqsY61/fYMDQwASRzJkkCi4sG4kQo5c5j3HpAwz3nVoQcj/R3AU7zcywMuVz0
qYiU4DcCq0Za6HXQS8vJ0yct10FjoXaDZmgYtj7LbX1c+mJhTPDaPyKC56X3LOBg
KAQ0xwIC/ucyBoR02NhlSDoXGvX76W0J6J/jdaam/vcWdO212SEq68FkRNsJr8y/
DS7/aU4rhw3pI994essfAgke1oqSx20OzRb4SXy5pfR/yVrlszwDmqOadFYogQxS
UR7KruVaXqZBFNhesUnxs5EmIMWsbTe+qbavSJVYUYQus0FTezNWSaLkTTsQaCE2
AkhSajND2HwzBrGvMBwObIFgk0000wcwras216uBp3mEGtjqdpmYhY7C5JXzkYUI
Ct8ZY+DJHMF0Uips/JvmglJ7Vr+ixCKa3ZmAf7J9sbJfChRKDAvKXVzVZXkf3W12
AAGVNlbTf8xHyFsRA/b/BXJjuJAKSgzbDdHU19GJNh/CjRIgpJyvcRfVK+dirC50
r1EsIBP+xuplfQphVTEwHo1+NYPg7sMLFV/vR8tHIlzrJAxtdE/LsXQDHd2XFwuo
VMeXTY9t9EhtM4tHOoLlEDOzv/niUocDqKorAd8/arJ4iSQKTtjnlIUCF1TS1Lqg
U2icCL4/9NL0Ulnuy2DxL1j7u6gNIxGLTuDWgaKR90UwEqLuw2he73pUS2eAIBw6
AP7YGKhOqMLa5MlJYHNz6uWDtqBLbNXlTopVcqKk4EWemTSZtRD94ucNsBmH7GBJ
juUYPh8mFrvBRDOBe70vche0vzN3ouw3CcVdT6VAuVzns3LFpGxeSbBUyoAV6SD7
7xHahcoCXAGcff2eXmTWNWocm2sf19Hv4tPrWzfTyKdltHcg+GxPqAOGp5NsGw4D
H/61+6tO3lZt73/NIt2jO+sdgQs+MaRqWpOJfwV1bW2/4cjn39qa4jB33QUebuJu
zXJdWWK9jfCmZJM7lQVcnGT8xqsC/+mcVY72rYf5QwQDagUcpOirHc+6/ULvYMy7
lWPjKlAoZDt1fqnI1kgY+cQkbPBrbBARZ1XhqjKBMuM2oaCU5Bh6ppRIBrBB/+Il
```

```
DAt43W3/MBOvu9LBC+oPB8MXVeuMYU96Uky1l3hh7YX0iP7Wn9wuwr+jx/NIlStO
dNST+pSRIPDgdph2ebRA7zNMruu9/U0+zQH+hJ8KdpGWVe3r4R6aR+FHRYT17rXZ
JbnlgT/yfIU4QnMTFislbJNbJNZgRWKC55A7kDPshUJ/gB5OIYtB4covXFtEel7g
odqkmLAc3Pgb6YQnVvHC4kCNtbGSvtPdidQRxMT2nVwFrpn7qI5x9pFp+IW0l5gk
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE-----                    <--- This is the USER CERTIFICATE
MIIFczCCBFugAwIBAgIQQRtXHG8Y534dY6EkS6gHiDANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzMwHhcNMTIwNzIz
MDAwMDAwWhcNMTQwODE5MjM1OTU5WjCBpTELMAkGA1UEBhMCVVMxETAPBgNVBAgT
CE1hcnlsYW5kMRIwEAYDVQQHFAlCYWx0aW1vcmUxJzAlBgNVBAoUHlQuIFJvd2Ug
UHJpY2UgQXNzb2NpYXRlcywgSW5jLjEgMB4GA1UECxQXSW52ZXN0bWVudCBUZWNo
bm9sb2dpZXMxJDAiBgNVBAMUG3dsZ3Vlc3RjaGVjay50cm93ZXByaWNlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJvJpXRzliY8d11vCZcChi2c
5uIn0TnUhR8QQrw0kstROJTtmSJpaOVTwOb0HoLgC8lH2VRAIxvxXdi49AQpYoY5
z8UxeH29XqKIkYR399K7/L9W9caYwWSjn4eLq1lk0GLmGMtE7T4I2bhssAgfV2+k
kpS4RymNUdSgCWzDrm575xyzVCciOGUPjTxpB5U7sWPASqpEvgoX88fPPpTtzTJl
XE1n1eRIcbE1z1/wpRxlFH4XMPtL79F8FQTWZ0MvMzyLEriR+dHXxtbBUkCPvgFY
7Nruz4Rj5Uk4S33G1EVvExfMF/wa+rtFU4RwlV4DESbrhSFhLeEruFfpzOWhMj0C
AwEAAaOCAYswggGHMCYGA1UdEQQfMB2CG3dsZ3Vlc3RjaGVjay50cm93ZXByaWNl
LmNvbTAJBgNVHRMEAjAAMA4GA1UdDwEB/wQEAwIFoDBFBgNVHR8EPjA8MDqgOKA2
hjRodHRwOi8vU1ZSU2VjdXJlLUczLWNybC52ZXJpc2lnbi5jb20vU1ZSU2VjdXJl
RzMuY3JsMEMGA1UdIAQ8MDowOAYKYIZIAYb4RQEHNjAqMCgGCCsGAQUFBwIBFhxo
dHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3BzMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAfBgNVHSMEGDAWgBQNRFwWU0TBgn4dIKsl9AFj2L55pTB2Bggr
BgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMy1haWEudmVyaXNpZ24u
Y29tL1NWUlNlY3VyZUczLmNlcjANBgkqhkiG9w0BAQUFAAOCAQEAReYq+92lCiDX
8hG4FyAEsvc1lDEhGUVy0URn8U7nYF7kN4NZdUKHFX86izPYJiC0yB6SsbMtz68t
r8OwPFUOzRvPfhzivtn/mL1TcEPjWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3ey1zYVVVCqavw2BsvPAcklqvx7stSjQHtAoXeL9WBCfPlI5w/Fd6OP5J6XVBF
CHgAauqR5hONWge9M4xh6jDC0kLcrRcFXLbcdtS0DXHVBfBfDipoM2yRDdaVOwfZ
CrTL3cZA9HLzI3QtPkzLC7RrRP8r3bBkIYMNyGO465fe9IMV3MgTFey8G26mn+R5
iG3ddRLhhA==
-----END CERTIFICATE-----

% PEM files import succeeded.
(config)#
#sh crypto pki trustpoints
Trustpoint TP-self-signed-0:

Trustpoint CISCO_IDEVID_SUDI:
    Subject Name:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
          Serial Number (hex): 6A6967B3000000000003
    Certificate configured.

Trustpoint CISCO_IDEVID_SUDI0:
    Subject Name:
    cn=Cisco Root CA 2048
    o=Cisco Systems
          Serial Number (hex): 5FF87B282B54DC8D42A315B568C9ADFF
    Certificate configured.

Trustpoint HTTPS_SS_CERT_KEYPAIR:
    Subject Name:
    serialNumber=FOC1618V3T0+hostname=
    cn=
          Serial Number (hex): 01

Trustpoint verisign.com:
    Subject Name:
    cn=ciscouser
    ou=ciscotech
    o=ciscoj
    l=Bangalore
```

```
    c=IN
          Serial Number (hex): 411B571C6F18E77E1D63A1244BA80788
    Certificate configured.

Trustpoint VeriG3:    Subject Name:    cn=VeriSign Class 3 Secure Server CA - G3

    ou=Terms of use at <url>
    ou=VeriSign Trust Network
    o=VeriSign\
     Inc.
    c=US
          Serial Number (hex): 6ECC7AA5A7032009B8CEBCF4E952D491
    Certificate configured
```