

# Instalação certificada da terceira convirgida dos controladores do Wireless LAN do acesso

## Índice

[Introdução](#)

[Instalação](#)

[Comandos](#)

[Procedimento](#)

[Exemplo](#)

## Introdução

Este documento descreve como instalar um certificado em um Cisco Catalyst 3850 Series Switch ou em um controlador do Wireless LAN de Cisco 5760 (WLC), de modo que o certificado possa ser usado mais tarde para propósitos de autenticação. Este é um documento genérico esse focos na instalação certificada em um interruptor wireless do controlador da nova geração (NGWC).

## Instalação

Quando você obtém um certificado de usuário de um vendedor, você recebe geralmente três entidades no formato do Privacy Enhanced Mail (PEM):

1. Certificado de usuário
2. Chave de Rivest-Shamir-Adleman (RSA)
3. Certificado de raiz

Este processo de instalação para o Cisco Catalyst 3850 Series Switch e o Cisco 5760 WLC difere da instalação para Cisco 5508 WLC.

Notas:

Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

[A ferramenta Output Interpreter](#) ([clientes registrados somente](#)) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

## Comandos

Estes são os comandos usados no exemplo da instalação:

1. configure terminal
2. *nome cripto do ponto confiável do pki*
3. PEM do terminal do registro
4. o pki cripto autentica o *nome*
5. mostre Certificados criptos do pki

## Procedimento

Este procedimento descreve como instalar um certificado da terceira.

1. Instale o ponto confiável com estes comandos:

```
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
```

2. Autentique o ponto confiável:

Entre no pki cripto autentica o comando:

```
(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

A cópia e cola o certificado de usuário; seja certo incluir -----COMECE O CERTIFICADO-----  
e -----CERTIFICADO DA EXTREMIDADE----- linhas.

A imprensa **entra**, e datilografa **parado**.

```
(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

Tipo **sim**.

Incorpore o comando **cripto sh do ponto confiável do pki** a fim ver o certificado.

3. Importe o certificado de raiz.

Inscreva o comando **import cripto do pki**:

```
(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
```

A cópia e cola o certificado de raiz.



```
XElnleRlcbE1z1/wpRxlFH4XMpTL79F8FQTWZ0MvMzyLEriR+dHXxtbBUkCPvgFY
7Nruz4Rj5Uk4S33G1EVvExfMF/wa+rtFU4RwlV4DESbrhSFhLeEruFfpzOWhmj0C
AwEAAaOCAYswggGHMCYGA1UdEQQfMB2CG3dsZ3Vlc3RjaGVjay50cm93ZXByaWNl
LmNvbTAJBgNVHRMEAjAAMA4GA1UdDwEB/wQEAWIFoDBFBGnVHR8EPjA8MDqgOKA2
hjRodHRwOi8vU1ZSU2VjdXJlLWUzLWVhY2Z2ZXJpc2lnbi5jb20vU1ZSU2VjdXJl
RzMuY3JSMEMGA1UdIAQ8MDowOAYKYIZIAYb4RQEHNjAqMCGCCsGAQUFBwIBFhxo
dHRwcovL3d3dy52ZXJpc2lnbi5jb20vY3BzMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAFBgNVHSMEGDAWgBQNRfWU0TBgn4dIKs19AFj2L55pTB2Bggr
BgEFBQcBAQRqMGgwJAYIKwYBBQUHMAggGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBABggrBgEFBQcwoAoY0aHR0cDovL1NWU1NlY3VyZS1HMy1haWEudmVyaXNpZ24u
Y29tL1NWU1NlY3VyZUczLmNlcjANBgkqhkiG9w0BAQUFAAOCAQEAREYq+92lCiDX
8hG4FyAesvc1lDEhGUVy0URn8U7nYF7kN4NZdUKHFx86izPYJiC0yB6SsbMtz68t
r8OwPFUOzRvPfhzivtn/mL1TcEPjWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3eylzYVVVCqavw2BsvPAcklqvX7stSjQhtAoXeL9WBCfPlI5w/Fd6OP5J6XVBF
CHGAuqR5hONWge9M4xh6jDC0kLcrRcFXLbcdtS0DXHVBfBfDipoM2yRDdaVOwfZ
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-----

```
MIIF7DCBNSGawIBAgIQbsx6pacDIAM4zrz06VLUkTANBgkqhkiG9w0BAQUFADCB
yJELMAKGA1UEBhMCVVMxZmVzAVBGNVBAOTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXXJpU2lnbiBUcncvZdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBwZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmV5MUUwQWYDVQQDEzww
ZXJpU2lnbiBDbGFzcyAzIFB1YmVycyYyBQcmltYXJ5IENlcnRpb2ZlYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMTAwMjA3MjMjMTU5WjCBTEL
MAKGA1UEBhMCVVMxZmVzAVBGNVBAOTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcncvZdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtYyBvZiB1c2UgYXQg
aHR0cHM6Ly93d3cuZmVyaXNpZ24uY29tL3JwYSAoYyYkxMDEvMC0GA1UEAxMmVmVv
aVNpZ24gQ2xhc3MgMyBTZW51cmUgU2VydMvYIENBIC0gRzRzMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCxh4QfwgxF9byrJZenraI+nLr2wTm4i8rCrFbG
5bt1jkrPTc5v7Q1K1K90EJxoiy6Ve4mbE8riNDTB81vzSxtig0iBdNGIeGwCU/m8
```

f0MmV1gzgzszChew0E6RJK2GfWQS3HRKNKEdCuqWHQsV/KNLO85jiND4LQyUhhDK  
tpo9yus3nABINYYPUHjoRWPNGUFP9ZXse5jUxHGzUL4os4+guVoc9cosI6n9FAbo  
GLSa6Dxugf3kzTU2s1HTaewSulZub5tXxYsU5w7Hn01KVGrJTcW/EbGuHGeBy0RV  
M5l/JJs/U0V/hhrzPPptf4HluErT9YU3HLWm0AnkGHs4TvoPAgMBAAGjggHFMIIB  
2za0BggrBgEFBQCBAQQoMCYwJAYIKwYBBQUHMAGGGH0dHA6Ly9vY3NwLnZlcmlz  
aWduLmNvbTASBGNVHRMBAf8ECDAGAQH/AgEAMHAGA1UdIARpMGcwZQYLYIZIAYb4  
RQEHFwMwVjAoBggrBgEFBQCcARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw  
czAqBggrBgEFBQCAjAeGhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMDQG  
A1UdHwQtMCswKAAncWGI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMtZzUu  
Y3JsMA4GA1UdDwEB/wQEAwIBBjBtBggrBgEFBQCBDARhMF+hXaBbMFkwVzBVfGlp  
bWFnZS9naWYwITAFMACGBSsOAwIaBBSP5dMahqyNjmvDz4Bq1EgYLHsZLjAlFiNo  
dHRwOi8vbG9nby52ZXJpc2lnbi5jb20vbnNsb2dvLmdpZjAoBgNVHREITAFpB0w  
GzEZMbcGA1UEAxMQVnVyaVNPZ25NUetJLTItNjAdBgNVHQ4EFgQUODURcFlNEwYJ+  
HSCrJfQBY9i+eaUwHwYDVR0jBBgwFoAUF9Nlp8Ld7LvWManzQzn6Aq8zMTMwDQYJ  
KoZIHvNAQEFBQADggEBAAYDJO/dwwzZWJz+NrbrioBL0aP3nfPMU++CnqOh5pfb  
WJ1lboAdG0z60cEtBcDqbrIicFXZIDNAMwfCZYP6j0M3m+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/FL6lhNmKXUgg09A82kupYuAljWy4Pmz0gAk7fMTNBnrilk/Uq  
c2WrM34tdURukNfYv3IbvKga6QsTQu5sYZ+83Igsdsh0xOw/xJNvs6aaOnF0frNN  
wiRYOS5QGf9+A98kEw0g66ye04C9Xjr39+peSgmAchI4smAF486bK2xDRz1p2Ewi  
bL+pgsY61/fYMDQwASRzJkkCi4sG4kQo5c5j3HpAwz3nVoQcj/R3AU7zcywMuVz0  
qYiU4DcCq0Za6HXQS8vJ0yct10FjoXadZmgYtj7LbX1c+mJhTPDaPyKC56X3LOBg  
KAQ0xwIC/ucyBoR02NhlSDoXGvX76W0J6J/jdaam/vcWd0212SEq68FkRNsJr8y/  
DS7/aU4rhw3pI994essfAgke1oqSx200zRb4SXY5pfr/yVr1szwDmqOadFYogQxS  
UR7KruVaXqZBFNhesUnxs5EmIMWsbTe+qbavSJVYUYQus0FTEzNWSaLkTTsQaCE2  
AkhSajND2HwzBrGvMBWobIFgk0000wcwras216uBp3mEGTjqdpmYhY7C5JXzkYUI  
Ct8ZY+DJHMF0Uips/JvmglJ7Vr+ixCKa3ZmAf7J9sbJfChRKDAvKXVzVZXkf3W12  
AAGVnlbTf8xHyFsRA/b/BXJjuJAKSGzbDdHU19GJNh/CjRIgppJyvcrfVK+dirC50  
r1EsIBP+xuplfQphVTEwHo1+NYPg7sMLFV/vR8tHilzrJAxtde/LsXQDhd2XFwuo  
VMexTY9t9EhtM4tHOoLLED0zv/niUocDqKorAd8/arJ4iSQTtjnlIUCF1TS1Lqg  
U2icCL4/9NL0Ulnuy2DxLl1j7u6gNixGLTuDWgaKR90UwEqLuw2he73pUS2eAIBw6  
AP7YgKhOqMLa5m1JYHNz6uWDTqBLbNX1TopVcqKk4EWemTSZtRD94ucNsBmH7GBJ  
juUYPh8mFrvBRDOBe70vche0vzN3ouw3CcVdT6VAuVzns3LFpGxeSbBUyoAV6SD7  
7xHahcoCXAGcfff2eXmTWNWocm2sf19Hv4tPrWzftYKdltHcg+GxPqAOGp5NsGw4D  
H/61+6t03lZt73/Nit2j0+sdgQs+MarqWp0JfwV1bW2/4cJn39qa4jB33QUebuJu  
zXJdWwK9jfcMzJM71QvCnGT8xqsC/+mcVY72ryf5QwQDagUcpOirHc+6/ULvYMy7  
lWPjKlAoZDt1fqnI1kgY+cQkbPBrbBARZ1XhqjKBmUM2oaCU5Bh6ppRIBrBB/+I1  
Dat43W3/MBOvu9LBC+oPB8MXVeuMYU96Uky1l3hh7YX0iP7Wn9uwur+jx/Ni1St0  
dNST+pSRIPDgdph2ebRA7zNMruu9/U0+zQH+hJ8KdpGWVe3r4R6aR+FHRyT17rXZ  
JbnlgT/yfIU4QnMTFislBNbJNZgRWKC55A7kDPshUJ/gB50IYtB4covXftEel7g  
odqkMLAc3Pgb6YQnVvHC4kCNTbGSvtPdidQRxMT2nVwFrpn7qI5x9pFp+IW015gk  
-----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  
MIIFCzCCBFugAwIBAgIQQRtXHG8Y534dY6EkS6gHiDANBbkqhkiG9w0BAQUFADCB  
tTELMakGAlUEBhMCMVmxFzAVBgNVBAoTDlZlcmlTaWduLCBjb20wMR8wHQYDVQQL  
ExZWZXXJpU2lnbiBUcncvZDcBOZXR3b3JrMTswOQYDVQQLLeZlUzXjJtcyBvZiBlc2Ug  
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYyYkxMDEvMCOGA1UEAxMm  
VmVyaVNPZ24gQ2xhc3MgMyBTZWNIcmUgU2VydmVyeIENBIC0gRzRmWmhcNMTIwNzIz  
MDAwMDAwWhcNMTQwODE5MjM0OTU5WjBpTELMAkGAlUEBhMCMVmxETAPBgNVBAgT

```
CElhcnlsYW5kMRIwEAYDVQQHFALCYWx0aW1vcmluXzAlBgNVBAoUHLQuIFJvd2Ug
UHJpY2UgQXNzb2NpYXRlc3RjaGVjaW50cm93ZXByaWNlLmNvbTCC
bm9sb2dpZXMxJDAiBgNVBAMUG3dsZ3Vlc3RjaGVjaW50cm93ZXByaWNlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAJvJpXRzliY8d11vCZcChi2c
5uIn0TnUhr8QQrW0kstROJTTmSjpaOVTwOb0HoLgC8lH2VRAIvxXdi49AqPYoY5
z8UxeH29XqKIkYR399K7/L9W9caYwWSjn4eLq1lk0GLmGMtE7T4I2bhssAgfV2+k
kpS4RymNUdSgCWzDrm575xyzVCciOGUPjTxB5U7sWPASqpEvgoX88fPPpTtzTJl
XEln1eRIcbE1z1/wpRxlFH4XMptL79F8FQTWZ0MvMzyLEriR+dHXxtbBUkCPvgFY
7Nruz4Rj5Uk4S33G1EVvExfMF/wa+rtFU4Rwlv4DESbrhSFhLeEruFfpzOWhmj0C
AwEAAaOCAYswggGHMCYGA1UdEQQfMB2CG3dsZ3Vlc3RjaGVjaW50cm93ZXByaWNl
LmNvbTBJBgNVHRMEAjaAAMA4GA1UdDwEB/wQEAwIFoDBFBGNVHR8EPja8MDqgOKA2
hjRodHRwOi8vU1ZSU2VjdXJlLWUyZjZlbnBi5jb20vU1ZSU2VjdXJl
RzMuY3JSMEMGA1UdIAQ8MDowOAYKYIZIAYb4RQEHNjAqMCGCCsGAQUFBwIBFhxo
dHRwc3ovL3d3dy52ZXJpc2lnbi5jb20vY3BzMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAFBgNVHSMGDAWgBQNRfWU0TBgn4dIKs19AFj2L55pTB2Bggr
BgEFBQcBAQRqMGGwJAYIKwYBBQUHMAggGh0dHA6Ly9vY3NwLnZlcm1zaWduLmNv
bTBABGgrBgEFBQcAwY0aHR0cDovL1NWU1NlY3VyZS1HMy1haWEudmVyaXNpZ24u
Y29tL1NWU1NlY3VyZUczLmNlcjANBgkqhkiG9w0BAQUFAAOCAQEAREYq+92lCiDX
8hG4FyAeSvcl1DEHGUvY0URn8U7nYF7kN4NZdUKHFx86izPYJiC0yB6SsbMtZ68t
r8OwPFUOzRvPfhzivtn/mL1TcEPjWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3eylZyVVVcQavw2BsvPAcklqvX7stSjQHTAoXeL9WBCfPLI5w/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 <https://www.verisign.com/rpa> (c)10

ou=VeriSign Trust Network

o=VeriSign\  
Inc.

c=US

Serial Number (hex): 6ECC7AA5A7032009B8CEBCF4E952D491

Certificate configured.