Install Web Admin Certificates on Catalyst 9000 Switches

Contents

Introduction

This document describes the process to generate, download, and install certificates on Catalyst 9000 series switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How to configure Catalyst 9000 series switches
- How to sign Certificates using Microsoft Windows Server
- Public Key Infrastructure (PKI) and digital certificates

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9300 Switch, Cisco IOS® XE version 17.12.4
- Microsoft Windows Server 2022

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 provides a step-by-step guide for generating a Certificate Signing Request (CSR), getting it signed by a Certification Authority (CA), and installing the resulting certificate (along with the CA certificate) on a Catalyst 9000 switch.

The goal is to enable secure web (HTTPS) administration of the switch using a trusted certificate, ensuring compatibility with modern web browsers and compliance with organizational security policies.

Configure

This section provides a detailed workflow for generating, signing, and installing a web admin certificate on a Catalyst 9000 switch. Each step includes relevant CLI commands, explanations, and example outputs.

Step 1: Define a Key

Generate a general-purpose RSA key pair and use it to secure the certificate. The key must be exportable and can be sized according to security needs (1024 to 4096 bits).

<#root>

```
device(config)#
```

crypto key generate rsa general-keys label csr-key exportable

Example output when prompted for modulus size:

<#root>

```
The name for the keys will be:
```

csr-key

```
Choose the size of the key modulus in the range of 512 to 4096 for your  General Purpose Keys. Choosing
How many bits in the modulus [1024]:
```

4096

```
% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 4 seconds)
```

Step 2: Generate a Certificate Signing Request (CSR)

Configure a trustpoint on the switch for the web admin certificate, specifying enrollment via terminal, disabling revocation check, and providing identifying information (subject name, key, and subject alternative names).

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

```
device(ca-trustpoint)#
```

enrollment terminal pem

```
device(ca-trustpoint)#
```

revocation-check none

```
device(ca-trustpoint)#
```

subject-name C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain

```
device(ca-trustpoint)#
```

rsakeypair csr-key

```
device(ca-trustpoint)#
```

subject-alt-name mywebadmin.com

```
device(ca-trustpoint)#exit
```

Enroll the trustpoint to generate the CSR. You must be prompted for various options; providing "yes" or "no" as needed. The certificate request must be displayed on the terminal.

```
device(config)#crypto pki enroll webadmin-TP
```

Example output:

<#root>

```
% Start certificate enrollment ..
% The subject name in the certificate will include:
```

C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain

```
% The subject name in the certificate will include: C9300.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Parameters available for subject name configuration:

- **C**: Country, two capital letters only (US)
- **ST**: State or Province Name
- **L**: Location Name (city)
- **O**: Organization Name (company)
- **OU**: Organizational Unit Name (department/section)
- **CN**: Common Name (FQDN or IP address to be accessed)

Step 3: Submit the CSR to the Certification Authority (CA)

Copy the full CSR string (including the BEGIN and END lines) and submit it to your CA for signing.

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

-----END CERTIFICATE REQUEST-----
```

If you use a Microsoft Windows Server CA, download the signed certificate in Base64 format.
You typically receive the signed device certificate and possibly a Root CA certificate.

Step 4: Authenticate Root CA Base64 Certificate

Install the CA's certificate (in Base64 format) onto the switch to establish trust in the CA that issued your device certificate.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Paste the CA certificate (including the BEGIN and END lines) when prompted. Example:

<#root>

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

-----END CERTIFICATE-----
Certificate has attributes:
      Fingerprint MD5: C7224F3A A9B0426A FDCC50E6 8A04583E
      Fingerprint SHA1: 9B31C319 A515AC41 0114EA43 33716E8B 472A4EF5
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
%
```

Certificate successfully imported

Step 5: Authenticate Device Base64 Certificate

Authenticate the device's signed certificate against the installed CA certificate.

```
<#root>

device(config)#

crypto pki trustpoint webadmin-TP

device(ca-trustpoint)#

chain-validation stop

device(ca-trustpoint)#

crypto pki authenticate webadmin-TP
```

When prompted, paste in the device certificate:

```
<#root>

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

-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Step 6: Import Device Signed Certificate on the Catalyst 9000 Switch

Import the Base64 signed device certificate into the trustpoint.

```
<#root>

device(config)#

crypto pki import webadmin-TP certificate
```

Paste the certificate when prompted:

```
<#root>

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

-----BEGIN CERTIFICATE-----
< 9300 device certificate >
```

```
-----END CERTIFICATE-----
```

```
% Router Certificate successfully imported
```

At this point, the device certificate is imported to the switch along with all relevant CA(s), and the certificate is ready for use, including GUI (HTTPS) access.

Step 7: Use the New Certificate

Associate the trustpoint with the HTTP secure server and enable HTTPS access on the switch.

<#root>

```
device(config)#
```

```
ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#
```

```
no ip http secure-server
```

<#root>

```
device(config)#
```

```
ip http secure-server
```

Step 8: How to Ensure the Certificate is Trusted by Web Browsers

- The certificate's Common Name (CN) or a Subject Alternative Name (SAN) must match the URL accessed by the browser.
- The certificate must be within its validity period.
- The certificate must be issued by a CA (or chain of CAs) whose root is trusted by the browser. The switch must provide the full certificate chain (except the root CA, which is typically already present in the browser's store).
- If the certificate contains revocation lists, ensure the browser can download them and that the certificate's CN is not listed in any revocation list.

Verify

You can use these commands to verify the certificate configuration and current status:

View the installed certificates and their status for a trustpoint:

<#root>

device#

show crypto pki certificate webadmin-TP

Example output:

<#root>

Certificate Status:

Available

Certificate Serial Number (hex): 4700000129584BB4BAFA13EABB000000000129
Certificate Usage: General Purpose
Issuer:

cn=mitch-DC02-CA   dc=mitch   dc=local

Subject: Name:

C9300.cisco.com

Serial Number: XXXXXXXXXX
cn=

myc9300.local-domain

ou=LANSW
o=TAC
l=CA
st=CA
c=SJ

hostname=C9300.cisco.com

Validity Date:
    start date: 05:09:42 UTC Jun 12 2025
    end   date: 07:25:06 UTC Dec 16 2026
Associated Trustpoints:

webadmin-TP

CA Certificate Status: Available
Certificate Serial Number (hex): 101552448B9C2EBB488C40034C129F4A
Certificate Usage: Signature
Issuer: cn=mitch-DC02-CA   dc=mitch   dc=local
Subject: cn=mitch-DC02-CA   dc=mitch   dc=local

Validity Date:

start date: 07:15:06 UTC Dec 16 2021

end   date: 07:25:06 UTC Dec 16 2026

```
Associated Trustpoints: webadmin-TP RootCA
```

Verify the HTTPS server status and associated trustpoint:

<#root>

```
device#
```

```
show ip http server secure status
```

Example output:

<#root>

```
HTTP secure server status: Enabled

HTTP secure server port: 443
HTTP secure server ciphersuite:  rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
                                 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
                                 ecdhe-rsa-aes-cbc-sha2
                                 ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
HTTP secure server TLS version:  TLSv1.2 TLSv1.1
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: webadmin-TP

HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

Troubleshoot

If you encounter issues during the certificate installation process, use this commands to enable debugging of PKI transactions. This is especially useful for diagnosing failures during certificate import or enrollment.

<#root>

```
device#
```

```
debug crypto pki transactions
```

Example of a successful scenario debug output:

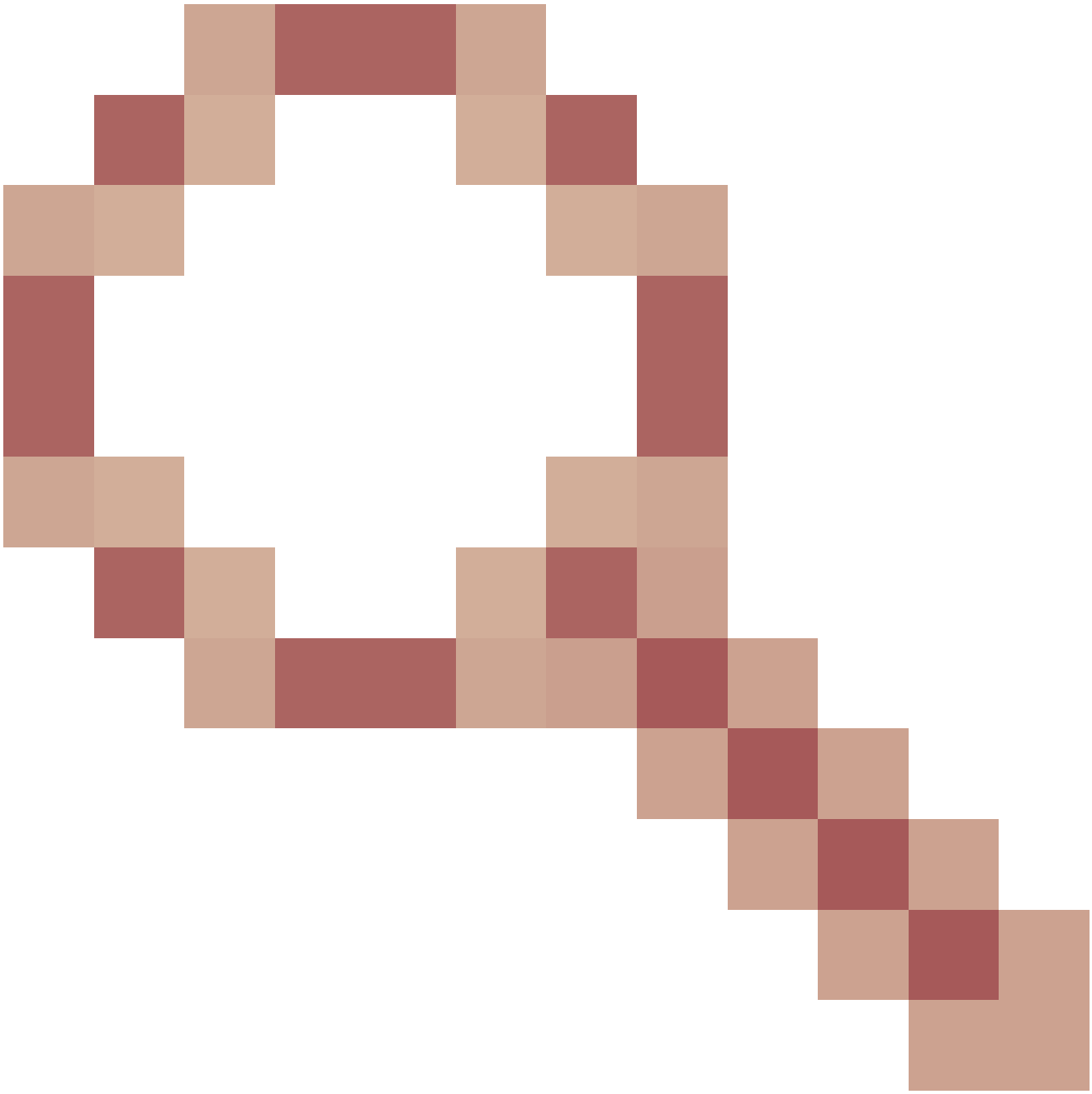
<#root>

```
*Jun 12 05:16:03.531: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named C9300.cisco.com has been generated or
*Jun 12 05:16:03.534:
```

```
 %CRYPTO-6-AUTOGEN: Generated new 2048 bit key pair

*Jun 12 05:16:03.556: CRYPTO_PKI: unlocked trustpoint RootCA, refcount is 0
*Jun 12 05:16:03.556: CRYPTO_PKI: using private key C9300.cisco.com for enrollment
*Jun 12 05:16:04.489: CRYPTO_PKI: Adding myc9300.local-domain to subject-alt-name field
*Jun 12 05:16:17.463: CRYPTO_PKI: using private key csr-key for enrollment
*Jun 12 05:18:32.378: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:19:15.464: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:19:15.470: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:19:15.472: CRYPTO_PKI: (A018E) Session started - identity not specified
*Jun 12 05:19:15.473: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a subject match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Check for identical certs
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a issuer match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Suitable trustpoints are: RootCA,
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Attempting to validate certificate using RootCA policy
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E)

Using RootCA to validate certificate

*Jun 12 05:19:15.474: CRYPTO_PKI(make trusted certs chain)
*Jun 12 05:19:15.474: CRYPTO_PKI:

Added 1 certs to trusted chain.

*Jun 12 05:20:05.555: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:20:25.734: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:20:25.735: CRYPTO_PKI(Cert Lookup)

issuer="cn=mitch-DC02-CA,dc=mitch,dc=local"

 serial number= 10 15 52 44 8B 9C 2E BB 48 8C 40 03 4C 12 9F 4A
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_get_cert_record_by_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI:

Found a cert match

*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:20:32.094: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Jun 12 05:20:32.096: CRYPTO_PKI:

Notify subsystem about new certificate.

*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:21:50.789: CRYPTO_PKI:

using private key csr-key for enrollment

*Jun 12 05:22:12.947: CRYPTO_PKI:

make trustedCerts list for webadmin-TP
```

Notes and Limitations

- Cisco IOS® XE does not support CA certificates with a validity beyond 2099 (Cisco bug ID CSCvp64208



).

- Cisco IOS® XE does not support SHA256 message digest PKCS 12 bundles (SHA256 certs are supported, but not if the PKCS12 bundle itself is signed with SHA256) (Cisco bug ID CSCvz41428). This is fixed in 17.12.1.

Related Information

- Cisco Technical Support & Downloads