# Catalyst 9000スイッチへのWeb Admin証明書のインストール

## 内容



## はじめに

このドキュメントでは、Catalyst 9000シリーズスイッチで証明書を生成、ダウンロード、およびインストールするプロセスについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Catalyst 9000シリーズスイッチの設定方法
- Microsoft Windows Serverを使用した証明書の署名方法
- 公開キーインフラストラクチャ(PKI)とデジタル証明書

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst 9300スイッチ、Cisco IOS® XEバージョン17.12.4
- Microsoft Windows Server 2022

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

# 背景説明

このドキュメントでは、証明書署名要求(CSR)の生成、認証局(CA)による署名の取得、および結果の証明書（およびCA証明書）のCatalyst 9000スイッチへのインストールの手順について説明します。

目標は、信頼できる証明書を使用してスイッチのセキュアなWeb(HTTPS)管理を実現し、最新のWebブラウザとの互換性と組織のセキュリティポリシーへのコンプライアンスを確保することです。

# 設定

このセクションでは、Catalyst 9000スイッチでWeb管理証明書を生成、署名、およびインストールするための詳細なワークフローを提供します。各ステップには、関連するCLIコマンド、説明、および出力例が含まれています。

## 手順1：キーを定義する

汎用RSAキーペアを生成し、それを使用して証明書を保護します。キーはエクスポート可能である必要があり、セキュリティのニーズ（1024 ~ 4096ビット）に従ってサイズを設定できます。

```
<#root>

device(config)#

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

モジュールサイズの入力を求められた場合の出力例：

```
<#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)
```

## ステップ2：証明書署名要求(CSR)を生成する

スイッチでWeb管理証明書のトラストポイントを設定し、ターミナル経由の登録を指定し、失効チェックを無効にして、識別情報（サブジェクト名、キー、およびサブジェクトの別名）を提供します。

<#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
```

トラストポイントを登録してCSRを生成します。必要に応じて「はい」または「いいえ」を入力し、さまざまなオプションを入力するように求めるプロンプトが表示されます。証明書要求が端末に表示される必要があります。

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

出力例：

<#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**

サブジェクト名の構成に使用できるパラメーター：

- C：国、2文字の大文字のみ（米国）
- ST：都道府県名
- L：事業所名（市区町村）
- O：組織名（会社）
- OU：組織単位名（部署/セクション）
- CN：共通名（アクセスされるFQDNまたはIPアドレス）

## ステップ3:CSRを認証局(CA)に送信します。

CSR文字列全体（BEGIN行とEND行を含む）をコピーし、CAに送信して署名を受けます。

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

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

Microsoft Windows Server CAを使用する場合は、Base64形式の署名付き証明書をダウンロードします。通常は、署名付きデバイス証明書と、場合によってはルートCA証明書を受け取ります。

## 手順4：ルートCA Base64証明書を認証する

CAの証明書（Base64形式）をスイッチにインストールし、デバイス証明書を発行したCAの信頼を確立します。

<#root>

```
device(config)#
```

**crypto pki authenticate webadmin-TP**

プロンプトが表示されたら、CA証明書（BEGIN行とEND行を含む）を貼り付けます。例：

<#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**

## ステップ5:Device Base64証明書の認証

インストールされたCA証明書に対してデバイスの署名付き証明書を認証します。

<#root>

```
device(config)#
```

**crypto pki trustpoint webadmin-TP**

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

**chain-validation stop**

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

**crypto pki authenticate webadmin-TP**

プロンプトが表示されたら、デバイス証明書を貼り付けます。

<#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**

## ステップ6:Catalyst 9000スイッチでのデバイス署名証明書のインポート

Base64署名付きデバイス証明書をトラストポイントにインポートします。

```
<#root>

device(config)#

crypto pki import webadmin-TP certificate
```

プロンプトが表示されたら、証明書を貼り付けます。

```
<#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
```

この時点で、デバイス証明書がすべての関連CAとともにスイッチにインポートされ、証明書はGUI(HTTPS)アクセスを含む使用の準備が整います。

## ステップ7：新しい証明書を使用する

トラストポイントをHTTPセキュアサーバに関連付け、スイッチでHTTPSアクセスを有効にします。

```
<#root>

device(config)#

ip http secure-trustpoint webadmin-TP
```

```
<#root>

device(config)#

no ip http secure-server
```

```
<#root>

device(config)#

ip http secure-server
```

### ステップ8：証明書がWebブラウザで信頼されていることを確認する方法

- 証明書の共通名(CN)またはサブジェクト代替名(SAN)は、ブラウザがアクセスするURLと一致する必要があります。
- 証明書は有効期間内である必要があります。
- 証明書は、ブラウザによって信頼されるルートを持つCA（またはCAのチェーン）によって発行される必要があります。スイッチは、完全な証明書チェーンを提供する必要があります（ただし、通常はブラウザのストアにすでに存在するルートCAは除きます）。
- 証明書に失効リストが含まれている場合は、ブラウザでダウンロードできること、および証明書のCNが失効リストに記載されていないことを確認してください。

## 確認

次のコマンドを使用して、証明書の設定と現在のステータスを確認できます。

トラストポイントのインストール済み証明書とそのステータスを表示します。

<#root>

device#

**show crypto pki certificate webadmin-TP**

出力例：

<#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
```

HTTPSサーバのステータスと関連するトラストポイントを確認します。

<#root>

```
device#

show ip http server secure status
```

出力例：

<#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
```

# トラブルシュート

証明書のインストールプロセス中に問題が発生した場合は、次のコマンドを使用してPKIトランザクションのデバッグを有効にします。これは、証明書のインポートまたは登録時の障害を診断する場合に特に役立ちます。

<#root>

device#

**debug crypto pki transactions**

成功したシナリオデバッグ出力の例：

<#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
```

## 注意と制限

- Cisco IOS® XEは、2099年を超える有効性のCA証明書をサポートしません(Cisco Bug ID CSCvp64208 )。

- Cisco IOS® XEは、SHA256 Message Digest PKCS 12バンドルをサポートしません（SHA256証明書はサポートされますが、PKCS12バンドル自体がSHA256で署名されている場合はサポートされません）(Cisco Bug ID CSCvz41428)。これは、17.12.1 で修正されています。

## 関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。