

Größe der Standard-SSH-RSA-Schlüssel am Cisco IOS XE SD-WAN-Edge ändern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die für sichere Protokolle verwendeten SSH-RSA-Standardschlüssel an Cisco IOS® XE SD-WAN-Edges auf eine höhere Länge erhöhen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- SSH-Schlüssel und grundlegende Zertifikatoperation
- RSA-Algorithmus

Verwendete Komponenten

- Cisco IOS® XE Catalyst SD-WAN-Kanten 17.9.4a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Secure Shell (SSH) ist ein Netzwerkprotokoll, mit dem Benutzer Remote-Verbindungen zu

Geräten auch über ein ungeschütztes Netzwerk herstellen können. Das Protokoll sichert die Sitzungen mithilfe standardmäßiger kryptografischer Mechanismen, die auf einer Client-Server-Architektur basieren.

RSA ist Rivest, Shamir, Adleman: Verschlüsselungsalgorithmus (kryptografisches System mit öffentlichem Schlüssel), der zwei Schlüssel verwendet: Öffentlicher und privater Schlüssel, auch Schlüsselpaar genannt. Der öffentliche RSA-Schlüssel ist der Verschlüsselungsschlüssel, der private RSA-Schlüssel der Entschlüsselungsschlüssel.

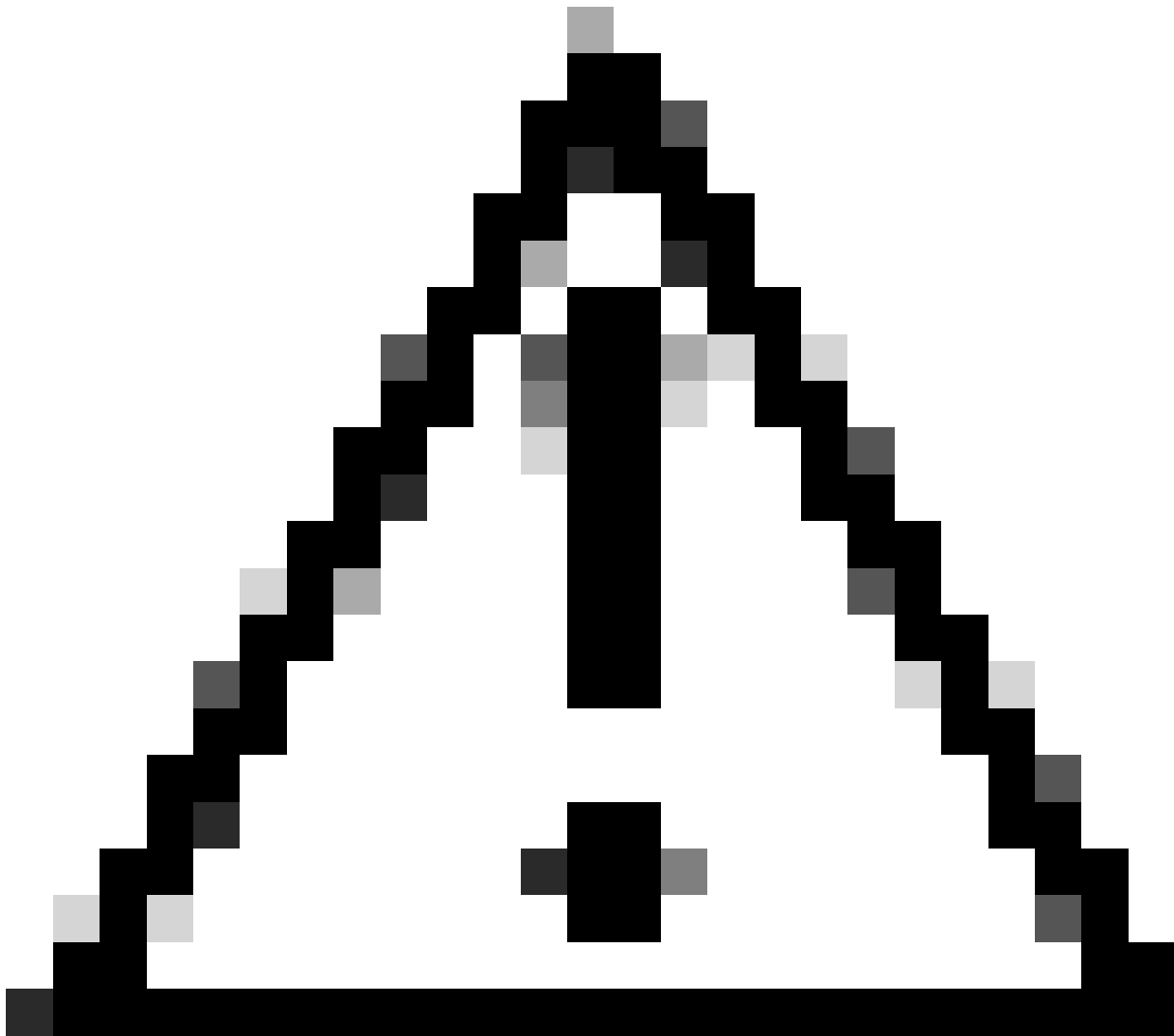
RSA-Schlüssel haben eine definierte Länge des Moduls in Bits. Wenn ein RSA-Schlüssel eine Länge von 2048 Bit haben soll, bedeutet dies wirklich, dass der Modulwert zwischen 22047 und 22048 liegt. Da der öffentliche und der private Schlüssel eines bestimmten Paares den gleichen Modul haben, haben sie per Definition auch die gleiche Länge.

Ein TrustPoint-Zertifikat ist ein selbstsigniertes Zertifikat, daher der Name TrustPoint, da es sich nicht auf die Vertrauenswürdigkeit einer anderen Person oder einer anderen Partei stützt.

Die Cisco IOS Public Key Infrastructure (PKI) stellt die Zertifikatsverwaltung zur Unterstützung von Sicherheitsprotokollen wie IP Security (IPSec), Secure Shell (SSH) und Secure Socket Layer (SSL) bereit.

SSH-RSA-Schlüssel sind für das Cisco Catalyst SD-WAN wichtig, da sie vom SSH-Protokoll zur Einrichtung der Kommunikation zwischen dem SD-WAN-Manager und den SD-WAN-Edge-Geräten verwendet werden, da der SD-WAN-Manager das Netconf-Protokoll verwendet, das über SSH Geräte verwaltet, konfiguriert und überwacht.

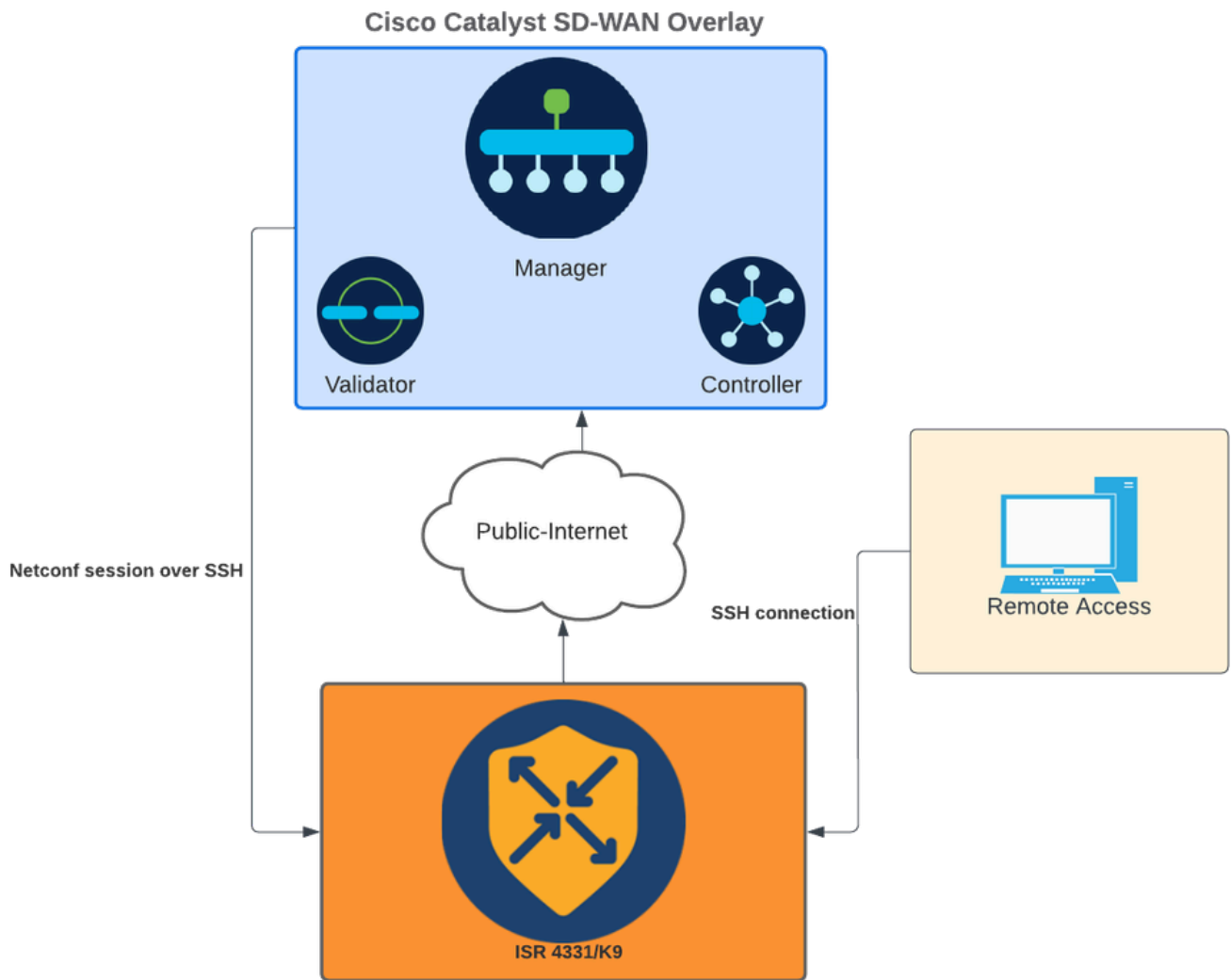
Aufgrund dieser Tatsache ist es notwendig, dass Schlüssel synchronisiert und aktualisiert werden die ganze Zeit. Wenn es aus Compliance- und Auditgründen erforderlich ist, die Schlüssellänge aus Sicherheitsgründen zu ändern, müssen Sie den in diesem Dokument beschriebenen Prozess abschließen, um die Größe der Schlüssel zu ändern und sie auf dem Zertifikat richtig zu synchronisieren, um eine Trennung zwischen dem SD-WAN-Manager und den SD-WAN-Edge-Geräten zu vermeiden.



Vorsicht: Führen Sie alle Schritte des Prozesses aus, um einen Verlust des Zugriffs auf das Gerät zu vermeiden. Wenn das Gerät in Betrieb ist, wird empfohlen, es in einem Wartungsfenster auszuführen und Konsolenzugriff auf das Gerät zu erhalten.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurationen

Die RSA-Schlüssel in den WAN-Edge-Geräten können nur über die Befehlszeilenschnittstelle (CLI) geändert werden. Für die Schlüsselaktualisierung können keine Vorlagen für CLI-Add-ons verwendet werden.



Warnung: Es wird empfohlen, den Vorgang mithilfe der Konsole auszuführen, da das SSH-Tool des SD-WAN-Managers erst nach Abschluss des Vorgangs verfügbar ist.



Warnung: Dieser Prozess erfordert einen Neustart des Geräts. Wenn das Gerät in Betrieb ist, wird empfohlen, es in einem Wartungsfenster auszuführen und Konsolenzugriff auf das Gerät zu erhalten. Wenn Sie keinen Konsolenzugriff haben, konfigurieren Sie vorübergehend ein anderes Remote-Zugriffsprotokoll als telnet.

Dieses Konfigurationsbeispiel zeigt, wie Sie RSA 2048 entfernen und den RSA 4096-Schlüssel verwenden.

1 - Ruft den aktuellen SSH-Schlüsselnamen ab.

```
<#root>
```

```
Device#
```

```
show ip ssh
```

```
SSH Enabled - version 2.0
```

```
Authentication methods:publickey,keyboard-interactive,password
```

```
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha2-512-etm@openssh.com
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
```

```
TP-self-signed-1072201169 <<<< RSA Key Name
```

```
Modulus Size : 2048 bits
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAZ5urq7f/X+AZJjUnM0dF9pLX+V0jPR8arK6bLSU7diGeSDDwW2MPNck/U5HBry9P/L4nKyZ1oEvAhfy7cJVvmoHD41NQW9wb/hLtimuujnRRYkKuIWLmoI7AHy6YQoetew8XVg1VIjva+JzQ5ZX1JGm8AzN6a95RbRNhGRzgz9cTFmD7m6ArIKZPMYqabXfrY+m/HuQ2aytbHtJMgm0Qk2fLPak03PnQNYXpiDP3Cm0Eh3LJg82FZQ1eohmhm+mAIwU4m1LHUouigyBuq1KEBVe3zvxjB9X8rGF3qzUcx21pHmhXaNpXWen2QQbyfAIDo8WxVoff24uLY1wCVkv
```

2 - Holen Sie sich das aktuelle selbstsignierte Trustpoint-Zertifikat.

```
<#root>
```

```
Device#
```

```
show crypto pki trustpoint
```

```
Trustpoint TP-self-signed-1072201169: <<<< Self-signed Trustpoint name
```

```
Subject Name:
```

```
cn=IOS-Self-Signed-Certificate-1072201169
```

```
Serial Number (hex): 01
```

```
Persistent self-signed certificate trust point
```

```
Using key label
```

```
TP-self-signed-1072201169
```

Beide Wertnamen müssen übereinstimmen.

3 - Löschen Sie den aktuellen Schlüssel.

```
<#root>
```

```
Device#
```

```
crypto key zeroize rsa
```

4 - Überprüfen, ob der alte Schlüssel erfolgreich gelöscht wurde

```
<#root>  
Device#  
show ip ssh
```

5 - Generieren Sie den neuen Schlüssel.

```
<#root>  
Device#  
crypto key generate rsa modulus 4096 label
```

```
The name for the keys will be: TP-self-signed-1072201169  
% The key modulus size is 4096 bits  
% Generating crypto RSA keys in background ...  
*Jun 25 21:35:18.919: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been generated  
*Jun 25 21:35:18.924: %SSH-5-ENABLED: SSH 2.0 has been enabled  
*Jun 25 21:35:23.205: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been generated  
*Jun 25 21:35:29.674: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
```

Dieser Vorgang kann 2 bis 5 Minuten dauern.

6 - Validieren Sie den generierten neuen Schlüssel.

```
<#root>  
Device#  
show ip ssh
```

```
SSH Enabled - version 2.0  
Authentication methods:publickey,keyboard-interactive,password  
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521  
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa  
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr  
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
```


KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits

IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169

Modulus Size : 4096 bits <<<< Key Size

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm808mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eF00H1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELB06yYEipPwMRaZYffTRbNjM8/7S0JG1FkgFVW5nITTIgISoMV8EJv
bL18cVgATDb10ckeDb7uU6PDXm3zonmZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKYvkcqXi6nDfAKb8o+Z8/43xbvW1DIKAuj1rbdyqPAJB411TZJk0Hk8zRP5gZ8u4jTjNKQHb
vNa3ieg4RLED0x41qCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MM0u14YDJYr
D+jnyoZr4PnfwAgk4M9U89deWS1IRPMIXYd35YmLvD60eQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

Jetzt wird ein neuer Schlüssel generiert. Zum Zeitpunkt der Löschung des alten Schlüssels wird das selbstsignierte Zertifikat, das von Netconf-Sitzungen verwendet wird, jedoch ebenfalls vom Vertrauenspunkt gelöscht.

<#root>

Device#


sh crypto pki trustpoint status

```
Trustpoint TP-self-signed-1072201169:
Issuing CA certificate configured::
Issuing CA certificate configured:
Subject Name:
cn=Cisco Licensing Root CA,o=Cisco
Fingerprint MD5: 1468DC18 250BDFCF 769C29DF E1F7E5A8
Fingerprint SHA1: 5CA95FB6 E2980EC1 5AFB681B BB7E62B5 AD3FA8B8
State:
```

Keys generated No <<<< Depending on the version, it can erase the key or even that, delete

```
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
```

Nach der Generierung des neuen Schlüssels 4096 werden die Schlüssel im selbstsignierten Zertifikat nicht automatisch aktualisiert, und es sind zusätzliche Schritte erforderlich, um das Zertifikat zu aktualisieren.

 Anmerkung: Wenn nur der Schlüssel generiert, aber nicht im Zertifikat aktualisiert wird, verliert der SD-WAN-Manager die Netconf-Sitzungen, wodurch alle Verwaltungsaktivitäten für das Gerät unterbrochen werden könnten (Vorlagen, Konfiguration usw.).

Es gibt zwei Möglichkeiten, das Zertifikat zu generieren bzw. den Schlüssel zuzuweisen:

1 - Laden Sie das Gerät neu.

```
<#root>
```

```
Device#
```

```
reload
```

2 - Starten Sie den sicheren HTTP-Server neu. Diese Option ist nur verfügbar, wenn sich das Gerät im CLI-Modus befindet.

```
<#root>
```

```
Device (config)#
```

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

```
Device (config)#
```

```
commit
```

```
Device (config)#
```

```
ip http secure-server
```

```
Device (config)#
```

```
commit
```

Überprüfung

Überprüfen Sie nach dem Neuladen, ob ein neuer Schlüssel generiert wurde und das Zertifikat unter dem gleichen Namen als vertrauenswürdig eingestuft wurde.

```
<#root>
```

```
Device#
```

```
show ip ssh
```

```
SSH Enabled - version 2.0
```

```
Authentication methods:publickey,keyboard-interactive,password
```

```
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
```

```
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
```

```
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
```

```
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512
```

```
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
```

Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits

IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169

Modulus Size : 4096 bits

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm808mb6bcWfU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eF00H1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELB06yYEipPwMRaZYFfTRbNjM8/7S0JG1FkgFVW5nITTIgISoMV8EJv
bL18cVgATDb10ckeb7uU6PDxm3zomZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKYvkccqXi6nDfAKb8o+Z8/43xbvW1DIKAuj1rbdyqPAJB411TZJk0Hk8zRP5gZ8u4jTjNKQHb
vNa3ieg4RLED0x41qCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOu14YDJYr
D+jnyoZr4PnfwAgk4M9U89deWS1IRPMIXYd35YmLvD60eQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

<#root>

Device#

show crypto pki trustpoint

Trustpoint TP-self-signed-1072201169: <<<< Trustpoint name

Subject Name:

cn=IOS-Self-Signed-Certificate-1072201169

Serial Number (hex): 01

Persistent self-signed certificate trust point

Using key label TP-self-signed-107220116

<#root>

Device#

show crypto pki certificates

Router Self-Signed Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: General Purpose

Issuer:

cn=IOS-Self-Signed-Certificate-1072201169

Subject:

Name: IOS-Self-Signed-Certificate-1072201169

cn=IOS-Self-Signed-Certificate-1072201169

Validity Date:

start date: 21:07:33 UTC Dec 27 2023

end date: 21:07:33 UTC Dec 26 2033

Associated Trustpoints: TP-self-signed-1072201169

Storage: nvram:IOS-Self-Sig#4.cer

Vergewissern Sie sich, dass der SD-WAN-Manager Konfigurationsänderungen auf den Router anwenden kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.