

Cambiar el tamaño de las claves SSH RSA predeterminadas en los extremos SD-WAN del IOS XE de Cisco

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

Introducción

Este documento describe cómo aumentar la longitud de las claves RSA SSH predeterminadas que se utilizan para los protocolos seguros a una mayor longitud en los extremos SD-WAN del IOS® XE de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- Operación básica de claves SSH y certificados
- Algoritmo RSA

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Secure Shell (SSH) es un protocolo de red que permite a los usuarios establecer conexiones remotas con los dispositivos incluso a través de una red no protegida. El protocolo protege las sesiones mediante mecanismos criptográficos estándar basados en una arquitectura cliente-servidor.

RSA es Rivest, Shamir, Adleman: Algoritmo de cifrado (sistema criptográfico de clave pública) que utiliza dos claves: Clave pública y privada, también conocidas como pares de claves. La clave RSA pública es la clave de cifrado y la clave RSA privada es la clave de descifrado.

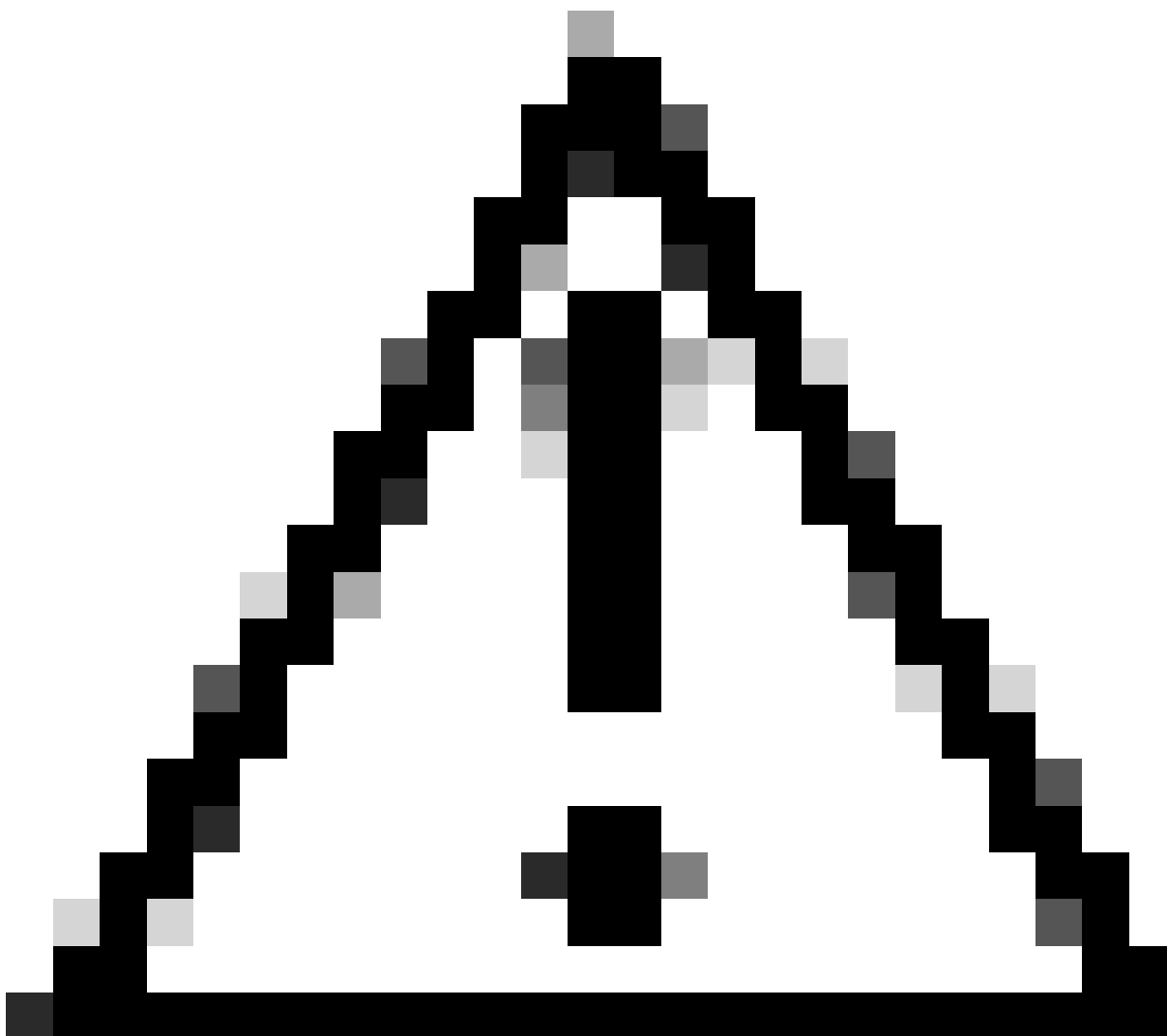
Las claves RSA tienen una longitud definida, en bits, del módulo. Cuando se dice que una clave RSA tiene una longitud de 2048 bits, en realidad significa que el valor del módulo se encuentra entre 22047 y 22048. Dado que las claves pública y privada de un par determinado comparten el mismo módulo, también tienen, por definición, la misma longitud.

Un certificado de punto de confianza es un certificado autofirmado, de ahí el nombre punto de confianza, ya que no depende de la confianza de nadie más ni de ninguna otra parte.

La infraestructura de clave pública (PKI) de Cisco IOS proporciona administración de certificados para admitir protocolos de seguridad como IP Security (IPSec), Secure Shell (SSH) y Secure Socket Layer (SSL).

Las claves RSA SSH son importantes en Cisco Catalyst SD-WAN porque las utiliza el protocolo SSH para establecer la comunicación entre el administrador SD-WAN y los dispositivos periféricos SD-WAN, ya que el administrador SD-WAN utiliza el protocolo Netconf, que funciona sobre SSH para administrar, configurar y monitorear dispositivos.

Debido a este hecho, es necesario que las claves estén sincronizadas y actualizadas todo el tiempo. Si por cumplimiento y auditoría, es necesario modificar la longitud de la clave para la seguridad, es necesario completar el proceso descrito en este documento para cambiar el tamaño de las claves y sincronizarlas correctamente en el certificado para evitar la desconexión entre el Administrador de SD-WAN y los dispositivos periféricos de SD-WAN.



Precaución: Complete todos los pasos del proceso para evitar la pérdida de acceso al dispositivo. Si el dispositivo está en producción, se recomienda realizarlo en una ventana de mantenimiento y tener acceso a la consola del dispositivo.

Configurar

Diagrama de la red

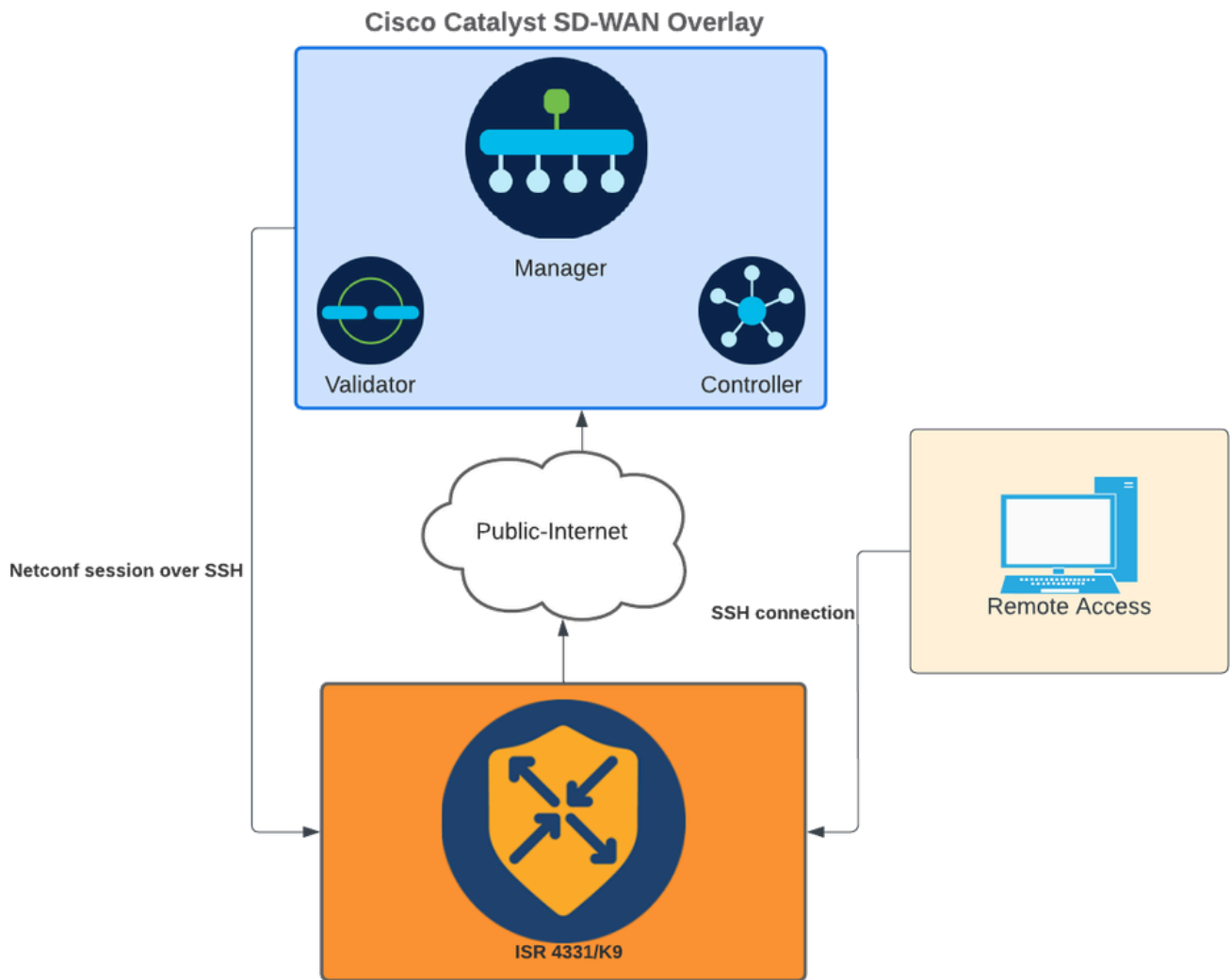


Diagrama de la red

Configuraciones

Las claves RSA en los dispositivos periféricos WAN solo se pueden modificar mediante la interfaz de línea de comandos (CLI); Las plantillas de la función de complemento de CLI no se pueden utilizar para actualizar las claves.



Advertencia: Se recomienda realizar el proceso con el uso de la consola, ya que la herramienta SSH del administrador de SD-WAN no está disponible hasta que el proceso finaliza.



Advertencia: Este proceso requiere reiniciar el dispositivo. Si el dispositivo está en producción, se recomienda realizarlo en una ventana de mantenimiento y tener acceso a la consola del dispositivo. Si no hay acceso a la consola, configure temporalmente otro protocolo de acceso remoto como telnet.

Este ejemplo de configuración muestra cómo quitar RSA 2048 y utilizar la clave RSA 4096.

1 - Obtener el nombre actual de la clave SSH.

```
<#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 <<<< RSA Key Name

Modulus Size : 2048 bits

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAZ5urq7f/X+AZJjUnM0dF9pLX+V0jPR8arK6bLSU7d
iGeSDDwW2MPNck/U5HBry9P/L4nKyZ1oEvAhfy7cJVvmoHD41NQW9wb/hLtimuujnRRYkKuIWLmoI7AH
y6YQoetew8XVg1VIjva+JzQ5ZX1JGm8AzN6a95RbRNhGRzgz9cTFmD7m6ArIKZPMYyQabXfrY+m/HuQ2
aytbHtJMgm0Qk2fLPak03PnQNYXpiDP3Cm0Eh3LJg82FZQ1eohmhm+mAIwU4m1LHUouigyBuq1KEBVe
z3vxjB9X8rGF3qzUcx21pHmhXaNpXWen2QQbyfAIDo8WXVoff24uLY1wCVkv
```

2 - Obtener el certificado autofirmado de trustpoint actual.

<#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

Ambos nombres de valor deben coincidir.

3 - Eliminar la clave actual.

<#root>

Device#

```
crypto key zeroize rsa
```

4 - Validar que la clave antigua se eliminó correctamente.

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

5 - Generar la nueva clave.

```
<#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
```

Este proceso puede tardar entre 2 y 5 minutos en completarse.

6 - Valide la nueva clave generada.

```
<#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

Modulus Size : 4096 bits <<<< Key Size

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm808mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eF00H1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELB06yYEipPwMraZYffTRbNjM8/7S0JG1FkgFVW5nITTIgISoMV8EJv
bLl8cVgATDb10ckeDb7uU6PDXm3zonmZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKyvkcx4i6nDfAKb8o+Z8/43xbvW1DIKAuj1rbdyqPAJB411TZJk0Hk8zRP5gZ8u4jtjNKQHb
vNa3ieg4RLED0x4lqCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOu14YDJYr
D+jnyoZr4PnfwAgk4M9U89deWS1IRPMIXYd35YmLvD60eQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

Ahora, se genera una nueva clave. Sin embargo, en el momento en que se eliminó la clave antigua, el certificado autofirmado que está siendo utilizado por las sesiones de Netconf también se elimina del punto de confianza.

```
<#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
```

Una vez generada la nueva clave 4096, las claves no se actualizan automáticamente en el certificado autofirmado y es necesario realizar pasos adicionales para actualizarla.

 Nota: Si sólo se genera la clave, pero no se actualiza en el certificado, el administrador de SD-WAN pierde las sesiones de Netconf, lo que podría interrumpir todas las actividades de administración del dispositivo (plantillas, configuración, etc.).

Hay dos formas de generar el certificado o asignar la clave:

1 - Recargue el dispositivo.

```
<#root>
```

```
Device#
```

```
reload
```

2 - Reinicie HTTP secure-server. Esta opción sólo está disponible si el dispositivo está en modo CLI.

```
<#root>
```

```
Device (config)#
```

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

```
Device (config)#
```

```
commit
```

```
Device (config)#
```

```
ip http secure-server
```

```
Device (config)#
```

```
commit
```

Verificación

Después de la recarga, valide que se genere la nueva clave y que el certificado esté en el punto de confianza con el mismo nombre.

```
<#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-sha1
```

```
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 AAAAB3NzaC1yc2EAAAADAQABAAQCE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQGGsdxo2+2Y/idAFm808mb6bcWfU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+711YawrDzpJ6d8RgUWLOtghSszQ7P796c0B1YLtK3eFO0H1AFmFy5ec8Own7ik0
JjKtwEozImFmJHZfUEUjFuhPJELBO6yYEipPwMRaZYfFTRbNjM8/7SOJG1FkgFVW5nITTIgISoMV8EJv
bL18cVgATDb10ckeDb7uU6PDxm3zonmZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+Tsmfp7Dh3k6qUTFUSy2h3
Kiibov1HKyvkcqXi6nDfAKb8o+Z8/43xbvW1DIKAuj1rbdyqPAJB411TZJkOHk8zRP5gZ8u4jTjNKQHb
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

Confirme que el Administrador de SD-WAN pueda aplicar los cambios de configuración al router del dispositivo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).