

Actualización del certificado ASA en CUCM para la función Phone VPN with AnyConnect

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[¿Cómo se actualiza el certificado ASA sin la interrupción de los servicios de los teléfonos VPN?](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso correcto para actualizar el certificado del dispositivo de seguridad adaptable (ASA) en Cisco Unified Communications Manager (CUCM) para teléfonos a través de una red privada virtual (VPN) con la función AnyConnect para evitar la interrupción del servicio telefónico.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Phone VPN con función AnyConnect.
- Certificados ASA y CUCM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Software Cisco Adaptive Security Appliance versión 9.8(2)20.
- Teléfono IP Cisco CP-8841.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

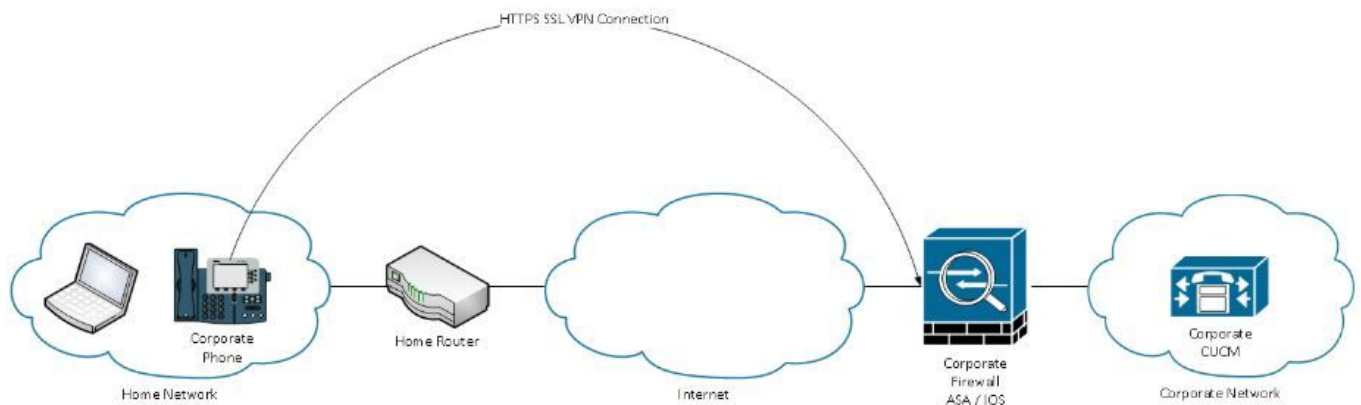
La función VPN del teléfono con AnyConnect permite la prestación de servicios telefónicos a través de una conexión VPN.

Antes de que el teléfono esté listo para VPN, primero debe aprovisionarse en la red interna. Esto requiere acceso directo al servidor TFTP de CUCM (protocolo trivial de transferencia de archivos).

El primer paso después de que el ASA esté completamente configurado, es tomar el certificado seguro (HTTPS) del protocolo de transferencia de hipertexto ASA y cargarlo en el servidor CUCM como Phone-VPN-trust, y asignarlo al gateway VPN correcto en CUCM. Esto permite al servidor CUCM generar un archivo de configuración del teléfono IP que indica al teléfono cómo llegar al ASA.

El teléfono debe aprovisionarse dentro de la red antes de que pueda moverse fuera de la red y utilizar la función VPN. Una vez que el teléfono se ha aprovisionado internamente, se puede mover a la red externa para obtener acceso VPN.

El teléfono se conecta en el puerto TCP 443 a través de HTTPS al ASA. El ASA responde con el certificado configurado y verifica el certificado presentado.



¿Cómo se actualiza el certificado ASA sin la interrupción de los servicios de los teléfonos VPN?

En algún momento, el certificado ASA debe ser cambiado, debido a cualquier circunstancia, por ejemplo.

El certificado está a punto de caducar

El certificado está firmado por terceros y la autoridad certificadora (CA) cambia, etc

Hay algunos pasos a seguir para evitar la interrupción del servicio para los teléfonos que están conectados a CUCM a través de VPN con AnyConnect.

Precaución: Si no se siguen los pasos, los teléfonos deben aprovisionarse de nuevo en la red interna antes de que puedan implementarse en una red externa.

Paso 1. Genere el nuevo certificado ASA pero no lo aplique aún a la interfaz.

El certificado puede ser firmado automáticamente o firmado por la CA.

Nota: Para obtener más información sobre los certificados ASA, consulte [Configuración de Certificados Digitales](#)

Paso 2. Cargue ese certificado en CUCM como confianza de VPN de teléfono en CUCM Publisher.

Inicie sesión en Call Manager y navegue hasta **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust.**

Como recomendación, cargue la cadena completa de certificados, si los certificados raíz e intermedio ya están cargados en CUCM, vaya al siguiente paso.

Precaución: Tenga en cuenta que si el certificado de identidad antiguo y el nuevo tienen el mismo CN (Nombre común), debe seguir la solución temporal para el error [CSCuh19734](#) para evitar que el nuevo certificado sobrescriba el anterior. De esta manera, el nuevo certificado está en la base de datos para la configuración de la puerta de enlace VPN del teléfono pero el anterior no se sobrescribe.

Paso 3. En el gateway VPN, seleccione ambos certificados (el anterior y el nuevo).

Vaya a **Administración de Cisco Unified CM > Funciones avanzadas > VPN > Gateway VPN.**

Asegúrese de tener ambos certificados en los certificados VPN en este campo de ubicación.

VPN Gateway Configuration Related Links: [Back To](#)

Save X Delete Copy + Add New

Status

i Status: Ready

VPN Gateway Information

VPN Gateway Name*

VPN Gateway Description

VPN Gateway URL*

VPN Gateway Certificates

VPN Certificates in your Truststore

▼ ▲

VPN Certificates in this Location*

Save Delete Copy Add New

Paso 4. Verifique que el grupo VPN, el perfil y el perfil de teléfono común estén configurados correctamente.

Paso 5. Reinicie los teléfonos.

Este paso permite que los teléfonos descarguen los nuevos valores de configuración y asegura que los teléfonos tengan ambos hashes de certificados, de modo que puedan confiar en el certificado antiguo y en el nuevo.

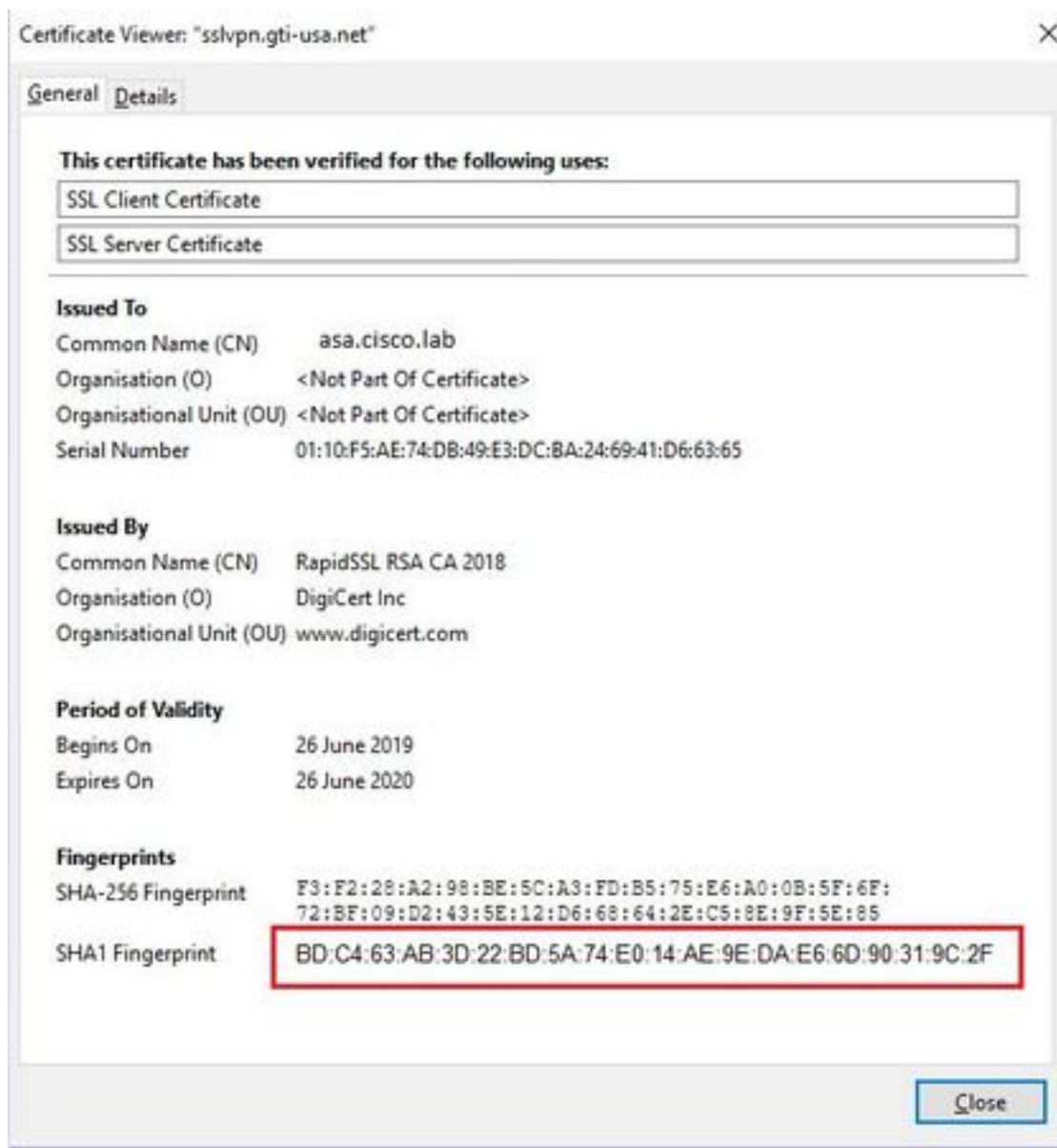
Paso 6. Aplique el nuevo certificado en la interfaz ASA.

Una vez que el certificado se aplica en la interfaz ASA, los teléfonos deben confiar en ese nuevo certificado, ya que ambos tienen hashes de certificado del paso anterior.

Verificación

Utilice esta sección para confirmar que ha seguido los pasos correctamente.

Paso 1. Abra los certificados ASA antiguos y nuevos y anote la huella digital SHA-1.



Paso 2. Elija un teléfono que se debe conectar a través de VPN y recopile su archivo de configuración.

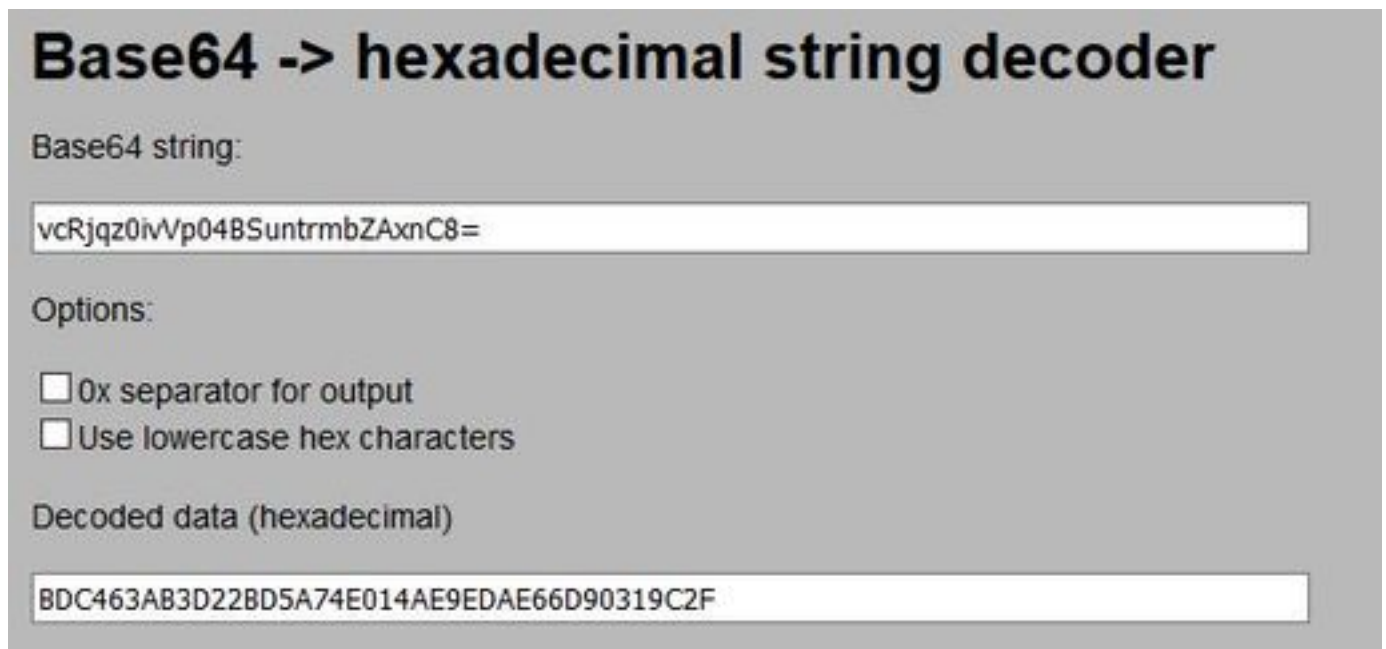
Nota: Para obtener más información sobre cómo recopilar el archivo de configuración del teléfono, consulte [Dos formas de obtener un archivo de configuración del teléfono de CUCM](#)

Paso 3. Una vez que tenga el archivo de configuración, busque la sección:

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>1</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1> https://radc.cgsinc.com/Cisco_VOIP_VPN</url1>;
</addresses>
<credentials>
<hashAlg>0</hashAlg>

      </credentials>
</vpnGroup>
```

Paso 4. El hash en el archivo de configuración se imprime en formato Base 64 y en el certificado ASA se imprime en formato hexadecimal, por lo que puede utilizar un descodificador de Base 64 a Hexadecimal para verificar que ambos hash (teléfono y ASA) coincidan.



The image shows a web-based tool titled "Base64 -> hexadecimal string decoder". It has a text input field containing the Base64 string "vcRjqz0ivVp04BSuntrmbZAxnC8=". Below the input field are two checkboxes: "0x separator for output" and "Use lowercase hex characters", both of which are unchecked. At the bottom, there is a text output field displaying the decoded hexadecimal string "BDC463A83D22BD5A74E014AE9EDAE66D90319C2F".

Información Relacionada

Para obtener más información sobre la función AnyConnect VPN Phone:

- Configure AnyConnect VPN Phone con autenticación de certificado en un ASA.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications->

<manager-callmanager/115785-anyconnect-vpn-00.html>