

# Configuración de AnyConnect VPN Phone con autenticación de certificado en un ASA

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Tipos de certificado de teléfono](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona una configuración de ejemplo que muestra cómo configurar los dispositivos Adaptive Security Appliance (ASA) y CallManager para proporcionar autenticación de certificados para los clientes AnyConnect que se ejecutan en los teléfonos IP de Cisco. Después de completar esta configuración, los teléfonos IP de Cisco pueden establecer conexiones VPN al ASA que utilizan certificados para asegurar la comunicación.

## Prerequisites

### Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Licencia de AnyConnect Premium SSL
- Licencia de AnyConnect para Cisco VPN Phone

Según la versión de ASA, verá "AnyConnect para el teléfono de Linksys" para la versión 8.0.x de ASA o "AnyConnect para el teléfono VPN de Cisco" para la versión 8.2.x de ASA o posterior.

### Componentes Utilizados

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

hardware.

- ASA: versión 8.0(4) o posterior
- Modelos de teléfono IP - 7942 / 7962 / 7945 / 7965 / 7975
- Teléfonos - 8961 / 9951 / 9971 con firmware de la versión 9.1(1)
- Teléfono - Versión 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) o posterior
- Cisco Unified Communications Manager (CUCM): versión 8.0.1.100000-4 o posterior

Las versiones utilizadas en este ejemplo de configuración incluyen:

- ASA - Versión 9.1(1)
- CallManager - Versión 8.5.1.10000-26

Para obtener una lista completa de los teléfonos admitidos en la versión de CUCM, siga estos pasos:

1. Abra esta URL: [https:// <Dirección IP del servidor CUCM>:8443/cucreports/systemReports.do](https://<Dirección IP del servidor CUCM>:8443/cucreports/systemReports.do)
2. Elija **Lista de funciones de teléfono de Unified CM > Generar un nuevo informe > Función: Red privada virtual.**

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, make sure that you understand the potential impact of any command.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Tipos de certificado de teléfono

Cisco utiliza estos tipos de certificados en teléfonos:

- Certificado instalado por el fabricante (MIC): los MIC se incluyen en todos los teléfonos IP de Cisco 7941, 7961 y en los modelos más recientes. Los MIC son certificados de clave de 2048 bits firmados por la autoridad de certificación de Cisco (CA). Cuando hay un MIC presente, no es necesario instalar un certificado de importancia local (LSC). Para que CUCM confíe en el certificado MIC, utiliza los certificados CA preinstalados CAP-RTP-001, CAP-RTP-002 y Cisco\_Manufacturing\_CA en su almacén de confianza de certificados.
- LSC: LSC protege la conexión entre CUCM y el teléfono después de configurar el modo de seguridad del dispositivo para la autenticación o el cifrado. El LSC posee la clave pública para el teléfono IP de Cisco, que está firmado por la clave privada de la función proxy de autoridad de certificados de CUCM (CAPF). Este es el método preferido (a diferencia del uso de MIC) porque sólo los teléfonos IP de Cisco que son aprovisionados manualmente por un administrador pueden descargar y verificar el archivo CTL. **Nota:** Debido al mayor riesgo de seguridad, Cisco recomienda el uso de los MIC únicamente para la instalación de LSC y no para su uso continuo. Los clientes que configuran teléfonos IP de Cisco para utilizar MIC para la autenticación de seguridad de la capa de transporte (TLS) o para cualquier otro fin lo hacen

por su cuenta y riesgo.

## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener [más información sobre los comandos utilizados en esta sección.](#)

## Configuraciones

Este documento describe estas configuraciones:

- Configuración ASA
- Configuración de CallManager
- Configuración de VPN en CallManager
- Instalación del certificado en teléfonos IP

### Configuración ASA

La configuración del ASA es casi la misma que cuando se conecta un equipo cliente AnyConnect al ASA. Sin embargo, estas restricciones se aplican:

- El grupo de túnel debe tener una url de grupo. Esta URL se configurará en CM bajo la URL de la puerta de enlace VPN.
- La política de grupo no debe contener un túnel dividido.

Esta configuración utiliza un certificado ASA (autofirmado o de terceros) previamente configurado e instalado en el punto de confianza Secure Socket Layer (SSL) del dispositivo ASA. Para más información, refiérase a estos documentos:

- [Configuración de certificados digitales](#)
- [Ejemplo de Configuración de ASA 8.x Instalación Manual de Certificados de Proveedores de Terceros para su Uso con WebVPN](#)
- [ASA 8.x: Ejemplo de Configuración de Acceso VPN con AnyConnect VPN Client Usando Certificado Autofirmado](#)

La configuración relevante del ASA es:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client
```

```
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable
```

```
ssl trust-point SSL outside
```

## Configuración de CallManager

Para exportar el certificado del ASA e importarlo al CallManager como certificado Phone-VPN-Trust, complete estos pasos:

1. Registre el certificado generado con CUCM.
2. Verifique el certificado utilizado para SSL.

```
ASA(config)#show run ssl
ssl trust-point SSL outside
```

3. Exportar el certificado.

```
ASA(config)#crypto ca export SSL identity-certificate
```

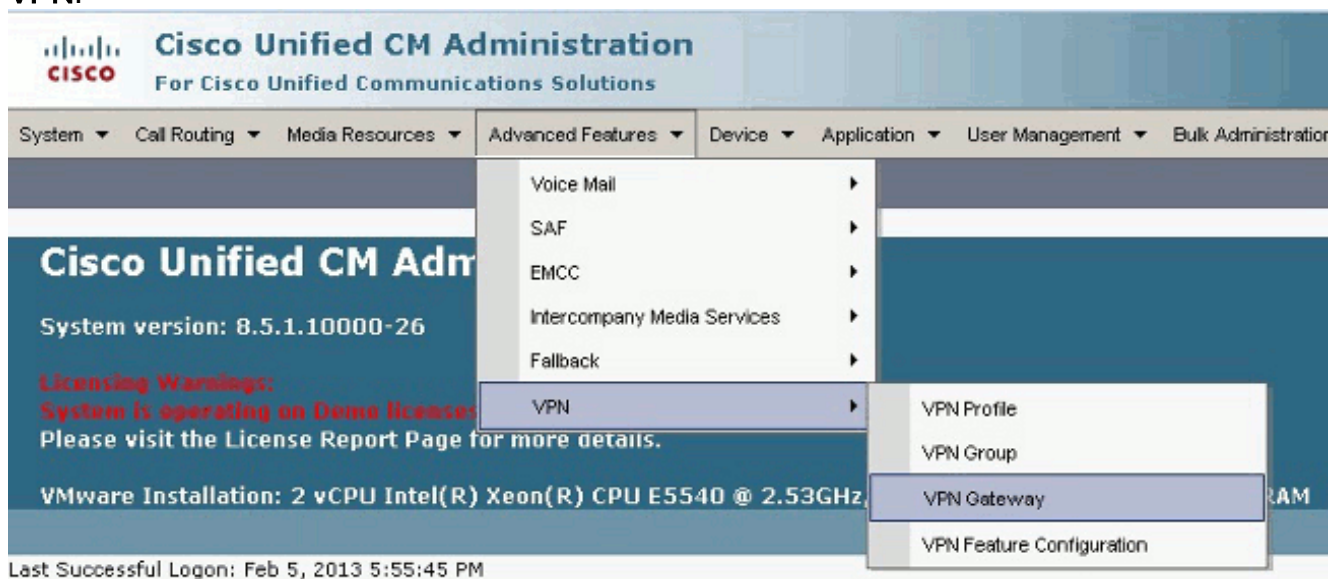
El certificado de identidad codificado por Privacy Enhanced Mail (PEM) es el siguiente:

```
-----BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrsyz+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOLv9xOpR7BFpZdlyFyzwAPkoB11
-----END CERTIFICATE-----
```

4. Copie el texto del terminal y guárdelo como un archivo .pem.
5. Inicie sesión en CallManager y elija **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust** para cargar el archivo de certificado guardado en el paso anterior.

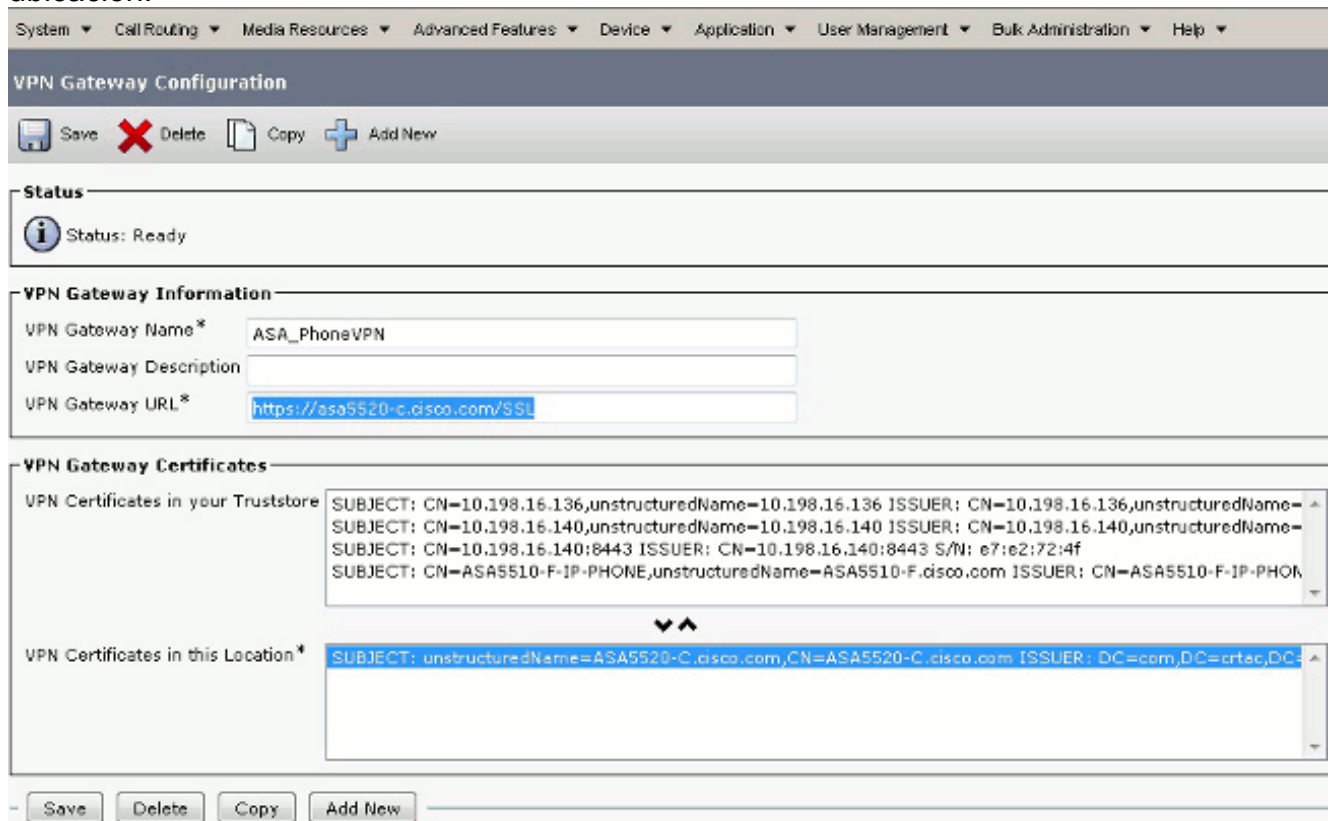
## Configuración de VPN en CallManager

1. Vaya a Administración de Cisco Unified CM.
2. En la barra de menús, elija **Funciones avanzadas > VPN > Gateway VPN**.

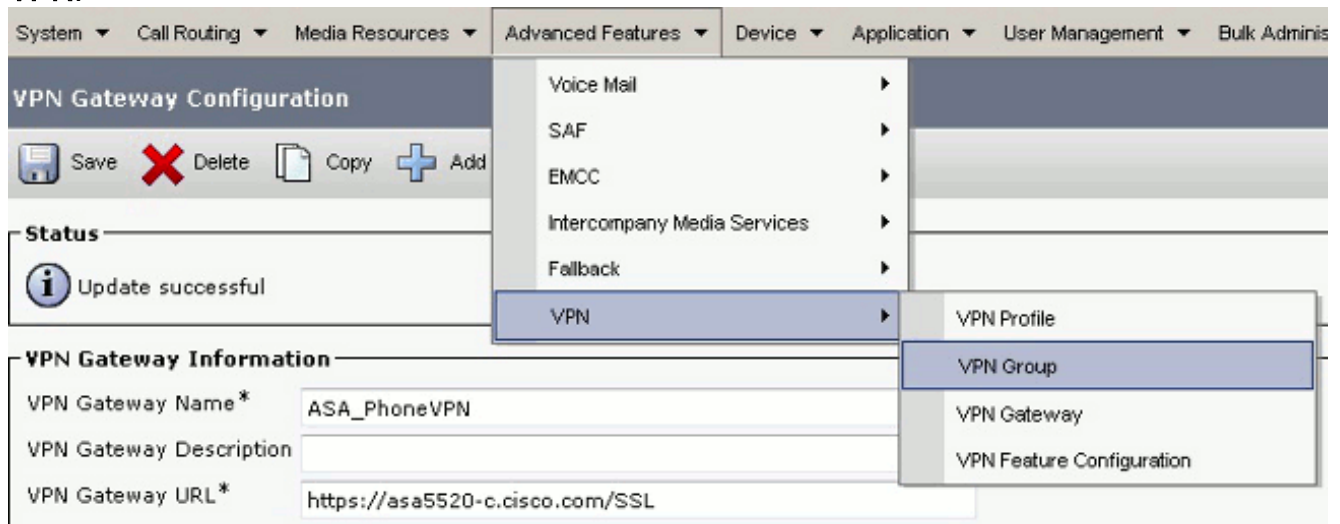


3. En la ventana VPN Gateway Configuration, complete estos pasos: En el campo VPN Gateway Name (Nombre de gateway VPN), introduzca un nombre. Puede ser cualquier nombre. En el campo Descripción de la puerta de enlace VPN, introduzca una descripción

(opcional). En el campo VPN Gateway URL, ingrese el grupo-url definido en el ASA. En el campo Certificados VPN de esta ubicación, seleccione el certificado que se cargó previamente en CallManager para moverlo del almacén de confianza a esta ubicación.



4. En la barra de menús, elija **Funciones avanzadas > VPN > Grupo VPN**.



5. En el campo All Available VPN Gateways (Todos los gateways VPN disponibles), seleccione el gateway VPN definido previamente. Haga clic en la flecha hacia abajo para mover el gateway seleccionado a las gateways VPN seleccionadas en este campo de grupo VPN.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manag

## VPN Group Configuration

Save Delete Copy Add New

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

**VPN Gateway Information**

All Available VPN Gateways

Selected VPN Gateways in this VPN Group\* ASA\_PhoneVPN

**Move the Gateway down**

6. En la barra de menús, elija **Funciones avanzadas > VPN > Perfil VPN**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administ

## VPN Group Configuration

Save Delete Copy Add

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN





VPN Group Description

- Voice Mail
- SAF
- EMCC
- Intercompany Media Services
- Fallback
- VPN**
  - VPN Profile**
  - VPN Group
  - VPN Gateway
  - VPN Feature Configuration

7. Para configurar el perfil VPN, complete todos los campos marcados con un asterisco (\*).


System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

---

**Status**

 Status: Ready

---

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

---

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check

---

**Client Authentication**

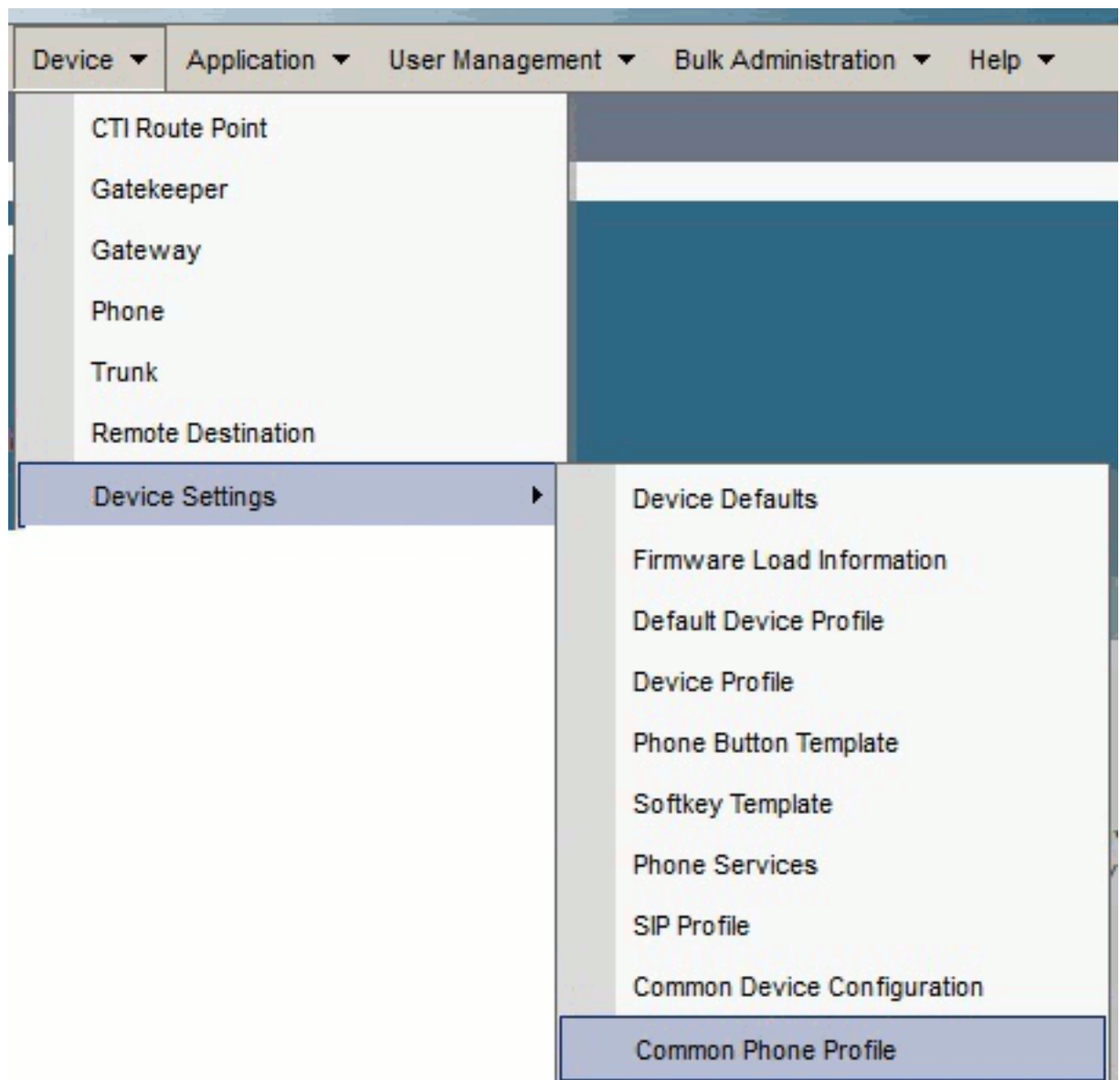
Client Authentication Method\*

Enable Password Persistence

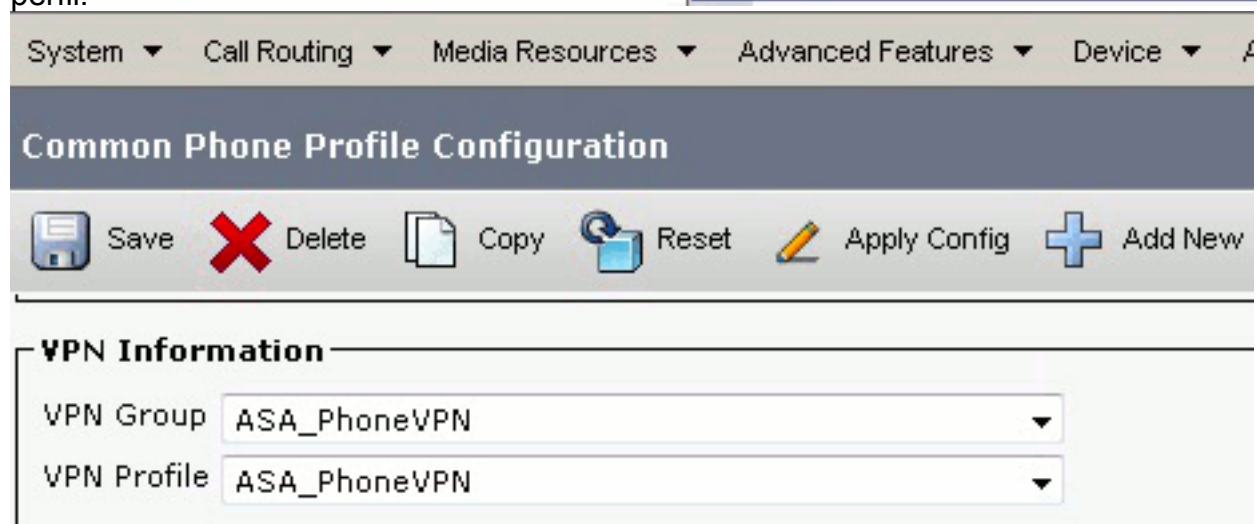
---

**Habilitar detección automática de red:** Si está activado, el teléfono VPN hace ping al servidor TFTP y si no se recibe respuesta, inicia automáticamente una conexión VPN. **Habilitar comprobación de ID de host:** Si está activado, el teléfono VPN compara el FQDN de la URL de la puerta de enlace VPN con el CN/SAN del certificado. El cliente no puede conectarse si no coincide o si se utiliza un certificado comodín con un asterisco (\*). **Habilitar persistencia de contraseña:** Esto permite que el teléfono VPN almacene en caché el nombre de usuario y la contraseña para el siguiente intento de VPN.

- En la ventana Common Phone Profile Configuration, haga clic en **Apply Config** para aplicar la nueva configuración VPN. Puede utilizar el "Perfil de teléfono común estándar" o crear un nuevo

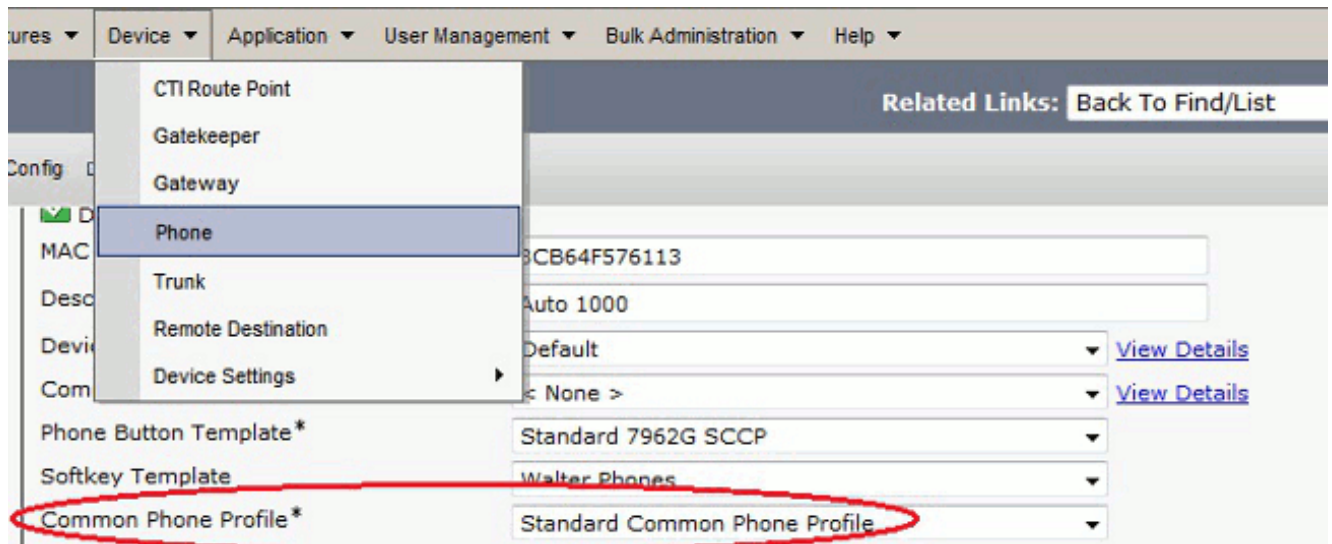


perfil.



9. Si ha creado un nuevo perfil para teléfonos/usuarios específicos, vaya a la ventana Configuración del teléfono. En el campo Perfil de teléfono común, elija **Perfil de teléfono común estándar**.





10. Vuelva a registrar el teléfono en CallManager para descargar la nueva configuración.





### Configuración de autenticación de certificados

Para configurar la autenticación de certificados, complete estos pasos en CallManager y ASA:

1. En la barra de menús, elija **Funciones avanzadas > VPN > Perfil VPN**.
2. Confirme que el campo Método de Autenticación del Cliente esté establecido en **Certificado**.


System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

---

**Status**

 Status: Ready

---

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

---

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check


---

**Client Authentication**

Client Authentication Method\*

Enable Password Persistence

3. Inicie sesión en CallManager. En la barra de menús, elija **Unified OS Administration > Security > Certificate Management > Find**.
4. Exportar los certificados correctos para el método de autenticación de certificados seleccionado: MIC: Cisco\_Manufacturing\_CA - Autentique los teléfonos IP con un MIC

Find Certificate List where  ▾ begins with  ▾    

Certificate Name	Certificate Type	.PEM File
tomcat	certs	<a href="#">tomcat.pem</a>
ipsec	certs	<a href="#">ipsec.pem</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>
ipsec-trust	trust-certs	<a href="#">CUCM85.pem</a>
CallManager	certs	<a href="#">CallManager.pem</a>
CAPF	certs	<a href="#">CAPF.pem</a>
TVS	certs	<a href="#">TVS.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-001.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco Root CA 2048.pem</a>
CallManager-trust	trust-certs	<a href="#">CAPF-18cf046e.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-002.pem</a>

LSC: Función Proxy de autoridad certificadora de Cisco (CAPF): autentique los teléfonos IP con un LSC

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>
psec	certs	<a href="#">ipsec.pem</a>	<a href="#">ipsec.der</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
psec-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
CallManager	certs	<a href="#">CallManager.pem</a>	<a href="#">CallManager.der</a>
CAPF	certs	<a href="#">CAPF.pem</a>	<a href="#">CAPF.der</a>
TVS	certs	<a href="#">TVS.pem</a>	<a href="#">TVS.der</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>	

5. Busque el certificado, ya sea Cisco\_Manufacturing\_CA o CAPF. Descargue el archivo .pem y guárdelo como archivo .txt

6. Cree un nuevo punto de confianza en el ASA y autentique el punto de confianza con el certificado guardado anterior. Cuando se le solicite un certificado de CA codificado base-64, seleccione y pegue el texto en el archivo .pem descargado junto con las líneas BEGIN y END. Se muestra un ejemplo a continuación:

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

7. Confirme que la autenticación en el grupo de túnel esté configurada en la autenticación de certificado.

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

## Instalación del certificado en teléfonos IP

Los teléfonos IP pueden funcionar con MIC o LSC, pero el proceso de configuración es diferente para cada certificado.

### Instalación de MIC

De forma predeterminada, todos los teléfonos que admiten VPN están precargados con MIC. Los teléfonos 7960 y 7940 no incluyen un MIC y requieren un procedimiento de instalación especial para que el LSC se registre de forma segura.

**Nota:** Cisco recomienda utilizar los MIC sólo para la instalación de LSC. Cisco admite LSC para autenticar la conexión TLS con CUCM. Debido a que los certificados raíz de MIC pueden verse comprometidos, los clientes que configuran teléfonos para utilizar MIC para la autenticación TLS o para cualquier otro propósito lo hacen por su cuenta y riesgo. Cisco no asume ninguna responsabilidad si los MIC se ven comprometidos.

### Instalación de LSC

1. Habilite el servicio CAPF en CUCM.
2. Después de activar el servicio CAPF, asigne las instrucciones del teléfono para generar un LSC en CUCM. Inicie sesión en Cisco Unified CM Administration y elija **Device > Phone**. Seleccione el teléfono que ha configurado.
3. En la sección Información de la función de proxy de la autoridad certificadora (CAPF), asegúrese de que todas las configuraciones sean correctas y de que la operación se establezca en una fecha futura.

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Size (Bits)\*

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

4. Si Authentication Mode se establece en Null String o Existing Certificate , no se requiere ninguna otra acción.
5. Si Authentication Mode se establece en una cadena, seleccione manualmente **Settings > Security Configuration > \*\*# > LSC > Update** en la consola del teléfono.

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

### Verificación ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
```

Encapsulation: TLSv1.0 TCP Dst Port : 443  
Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
Bytes Tx : 1759 Bytes Rx : 799  
Pkts Tx : 2 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 57.2  
Public IP : 172.16.250.15  
Encryption : AES128 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 50529  
TCP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client Type : SSL VPN Client  
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
Bytes Tx : 835 Bytes Rx : 0  
Pkts Tx : 1 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
Tunnel ID : 57.3  
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 51096  
UDP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client Type : DTLS VPN Client  
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
Bytes Tx : 303255 Bytes Rx : 269270  
Pkts Tx : 5642 Pkts Rx : 5649  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

## Verificación de CUCM

The screenshot shows the 'Find and List Phones' interface in CUCM. It displays a table of phones with the following data:

Device Name	Description	Device Pool	Device Protocol	Status	IP Address
SEPXXXXXXXXXXXX	Auto 1001	Default	SCCP	Unknown	Unknown
SEPXXXXXXXXXXXX	Auto 1000	Default	SCCP	Registered with 192.168.100.1	10.10.10.2

A red circle highlights the status 'Registered with 192.168.100.1' and the IP address '10.10.10.2' in the second row. A red arrow points to the IP address column header with the text 'IP Phone registered with the CUCM using VPN address'.

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

### Errores relacionados

- Cisco bug ID [CSCtf09529](#), Add support for VPN feature in CUCM for 8961, 9951, 9971 phones
- Cisco bug ID [CSCuc71462](#), la conmutación por fallas de VPN del teléfono IP dura 8 minutos

- Cisco bug ID [CSCtz42052](#), IP Phone SSL VPN Support for Non Default Port Numbers
- El Id. de bug Cisco [CSCth96551](#), no todos los caracteres ASCII se soportan durante el usuario de VPN del teléfono + login de contraseña.
- Id. de error de Cisco [CSCuj71475](#), entrada TFTP manual necesaria para VPN de teléfono IP
- Id. de error de Cisco [CSCum10683](#), teléfonos IP que no registran llamadas perdidas, realizadas o recibidas

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)