

Konfigurationsbeispiel für eine AnyConnect VPN- Telefonverbindung mit einem Cisco IOS-Router

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerktopologie](#)

[SSL VPN-Serverkonfiguration](#)

[Allgemeine Konfigurationsschritte](#)

[Konfiguration mit AAA-Authentifizierung](#)

[Konfiguration mit dem LSC \(Locally Significant Certificate\) des IP-Telefons für die Client-Authentifizierung](#)

[Call Manager-Konfiguration](#)

[Exportieren Sie das selbst signierte oder Identitätszertifikat vom Router in den CUCM.](#)

[Konfigurieren des VPN-Gateways, der Gruppe und des Profils im CUCM](#)

[Wenden Sie Gruppe und Profil auf das IP-Telefon mit dem allgemeinen Telefonprofil an.](#)

[Wenden Sie das allgemeine Telefonprofil auf das IP-Telefon an.](#)

[Installation von LSC \(Locally Significant Certificates\) auf Cisco IP-Telefonen](#)

[Registrieren Sie das Telefon erneut beim Call Manager, um die neue Konfiguration herunterzuladen.](#)

[Überprüfen](#)

[Router-Verifizierung](#)

[CUCM-Verifizierung](#)

[Fehlerbehebung](#)

[Debuggen auf dem SSL VPN-Server](#)

[Debugger vom Telefon aus](#)

[Zugehörige Fehler](#)

Einführung

Dieses Dokument beschreibt die Konfiguration des Cisco IOS[®] Routers und der Call Manager-Geräte, sodass die Cisco IP-Telefone VPN-Verbindungen zum Cisco IOS Router herstellen können. Diese VPN-Verbindungen werden benötigt, um die Kommunikation mit einer der beiden folgenden Client-Authentifizierungsmethoden zu sichern:

- AAA-Server (Authentication, Authorization, and Accounting) oder lokale Datenbank
- Telefonzertifikat

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco IOS 15.1(2)T oder höher
- Funktionssatz/Lizenz: Universal (Daten & Sicherheit & UC) für Cisco IOS Integrated Service Router (ISR)-G2
- Funktionssatz/Lizenz: Erweiterte Sicherheit für Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM) Version 8.0.1.10000-4 oder höher
- IP-Telefon Version 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) oder höher

Gehen Sie wie folgt vor, um eine vollständige Liste der unterstützten Telefone in Ihrer CUCM-Version anzuzeigen:

1. URL öffnen: <https://<CUCM-Server-IP-Adresse>:8443/cucreports/systemReports.do>
2. Wählen Sie **Unified CM Phone Feature List (Funktionsliste des Unified CM-Telefons) > Generate a new report > Feature (Neuen Bericht erstellen): Virtuelles privates Netzwerk.**

In diesem Konfigurationsbeispiel werden folgende Versionen verwendet:

- Cisco IOS Router Version 15.1(4)M4
- Call Manager Version 8.5.1.1000-26
- IP-Telefon Version 9.1(1) SR1S

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

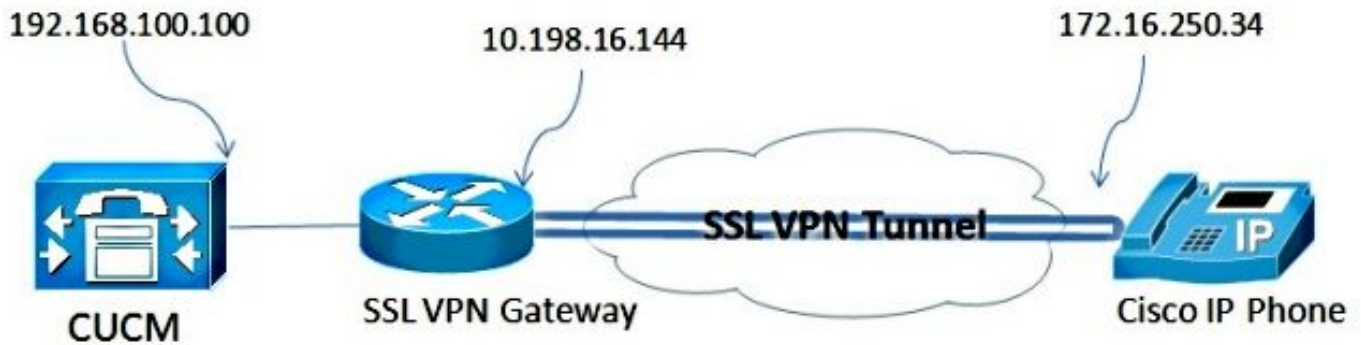
Konfigurieren

In diesem Abschnitt werden die Informationen behandelt, die zum Konfigurieren der in diesem Dokument beschriebenen Funktionen erforderlich sind.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerktopologie

Die in diesem Dokument verwendete Topologie umfasst ein Cisco IP-Telefon, den Cisco IOS-Router als SSL-VPN-Gateway (Secure Sockets Layer) und CUCM als Sprach-Gateway.



SSL VPN-Serverkonfiguration

In diesem Abschnitt wird beschrieben, wie das Cisco IOS-Headend konfiguriert wird, um eingehende SSL VPN-Verbindungen zuzulassen.

Allgemeine Konfigurationsschritte

1. Generieren Sie den RSA-Schlüssel (Rivest-Shamir-Adleman) mit einer Länge von 1024 Byte:

```
Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
```

2. Erstellen Sie den Trustpoint für das selbstsignierte Zertifikat, und fügen Sie den **SSL RSA-Schlüssel** an:

```
Router(config)#crypto pki trustpoint server-certificate
enrollment selfsigned
usage ssl-server
serial-number
subject-name CN=10.198.16.144
revocation-check none
rsakeypair SSL
```

3. Wenn der Vertrauenspunkt konfiguriert ist, registrieren Sie das selbstsignierte Zertifikat mit dem folgenden Befehl:

```
Router(config)#crypto pki enroll server-certificate
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
```

```
Router Self Signed Certificate successfully created
```

4. Aktivieren Sie das richtige AnyConnect-Paket am Headend. Das Telefon selbst lädt dieses Paket nicht herunter. Ohne das Paket wird der VPN-Tunnel jedoch nicht eingerichtet. Es wird empfohlen, die neueste Client-Softwareversion zu verwenden, die auf Cisco.com verfügbar ist. In diesem Beispiel wird Version 3.1.3103 verwendet.

In älteren Cisco IOS-Versionen ist dies der Befehl zum Aktivieren des Pakets:

```
Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

In der neuesten Cisco IOS-Version lautet der folgende Befehl:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

5. Konfigurieren Sie das VPN-Gateway. Das WebVPN-Gateway wird verwendet, um die SSL-Verbindung des Benutzers zu beenden.

```
webvpn gateway SSL
ip address 10.198.16.144 port 443
ssl encryption 3des-sha1 aes-sha1
http-redirect port 80
ssl trustpoint server-certificate
inservice
```

Hinweis: Entweder muss sich die hier verwendete IP-Adresse im gleichen Subnetz befinden wie die Schnittstelle, mit der die Telefone verbunden sind, oder das Gateway muss direkt von einer Schnittstelle am Router bezogen werden. Das Gateway wird auch verwendet, um festzulegen, welches Zertifikat vom Router verwendet wird, um sich für den Client zu validieren.

6. Definieren Sie den lokalen Pool, der verwendet wird, um den Clients bei der Verbindung IP-Adressen zuzuweisen:

```
ip local pool ap_phonevpn 192.168.100.1 192.168.100.254
```

Konfiguration mit AAA-Authentifizierung

In diesem Abschnitt werden die Befehle beschrieben, die Sie benötigen, um den AAA-Server oder die lokale Datenbank für die Authentifizierung Ihrer Telefone zu konfigurieren. Wenn Sie für die Telefone nur eine Zertifikatsauthentifizierung verwenden möchten, fahren Sie mit dem nächsten Abschnitt fort.

Konfigurieren der Benutzerdatenbank

Zur Authentifizierung können entweder die lokale Datenbank des Routers oder ein externer AAA-Server verwendet werden:

- Um die lokale Datenbank zu konfigurieren, geben Sie Folgendes ein:

```
aaa new-model
aaa authentication login SSL local
username phones password 0 phones
```

- Um einen Remote-AAA-RADIUS-Server für die Authentifizierung zu konfigurieren, geben Sie Folgendes ein:

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

Konfigurieren des virtuellen Kontexts und der Gruppenrichtlinie

Der virtuelle Kontext wird verwendet, um die Attribute zu definieren, die die VPN-Verbindung steuern, z. B.:

- Welche URL soll bei der Verbindung verwendet werden?

- Welcher Pool zum Zuweisen der Client-Adressen verwendet werden soll
- Welche Authentifizierungsmethode wird verwendet?

Diese Befehle sind ein Beispiel für einen Kontext, der AAA-Authentifizierung für den Client verwendet:

```
webvpn context SSL
aaa authenticate list SSL
gateway SSL domain SSLPhones
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonevpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

Konfiguration mit dem LSC (Locally Significant Certificate) des IP-Telefons für die Client-Authentifizierung

In diesem Abschnitt werden die Befehle beschrieben, die Sie zum Konfigurieren der zertifikatbasierten Client-Authentifizierung für die Telefone benötigen. Hierzu ist jedoch die Kenntnis der verschiedenen Arten von Telefonzertifikaten erforderlich:

- **MIC (Manufacturer Installed Certificate)** - MICs sind auf allen Cisco IP-Telefonen der Serien 7941, 7961 und neueren Modellen enthalten. MICs sind 2.048-Bit-Schlüsselzertifikate, die von der Cisco Certificate Authority (CA) signiert werden. Damit der CUCM dem MIC-Zertifikat vertrauen kann, verwendet er die vorinstallierten CA-Zertifikate CAP-RTP-001, CAP-RTP-002 und Cisco_Manufacturing_CA in seinem Zertifikats-Trust-Store. Da dieses Zertifikat vom Hersteller selbst bereitgestellt wird, wie im Namen angegeben, wird es nicht empfohlen, dieses Zertifikat für die Client-Authentifizierung zu verwenden.
- **LSC** - Das LSC sichert die Verbindung zwischen dem CUCM und dem Telefon, nachdem Sie den Gerätesicherheitsmodus für die Authentifizierung oder Verschlüsselung konfiguriert haben. Der LSC verfügt über den öffentlichen Schlüssel für das Cisco IP-Telefon, der vom privaten Schlüssel der CUCM Certificate Authority Proxy Function (CAPF) signiert wird. Dies ist die sicherere Methode (im Gegensatz zur Verwendung von MICs).
Vorsicht: Aufgrund des erhöhten Sicherheitsrisikos empfiehlt Cisco die Verwendung von MICs ausschließlich für die LSC-Installation und nicht für die weitere Verwendung. Kunden, die Cisco IP-Telefone konfigurieren, um MICs für die TLS-Authentifizierung (Transport Layer Security) oder für andere Zwecke zu verwenden, tun dies auf eigenes Risiko.

In diesem Konfigurationsbeispiel wird das LSC zur Authentifizierung der Telefone verwendet.

Tipp: Die sicherste Methode für den Anschluss Ihres Telefons ist die Verwendung einer dualen Authentifizierung, die Zertifikat und AAA-Authentifizierung kombiniert. Sie können dies konfigurieren, wenn Sie die für die einzelnen Befehle verwendeten Befehle in einem virtuellen Kontext kombinieren.

Konfigurieren Sie den Trustpoint, um das Clientzertifikat zu validieren.

Für die Validierung des LSC vom IP-Telefon muss auf dem Router das CAPF-Zertifikat installiert

sein. Gehen Sie wie folgt vor, um das Zertifikat zu erhalten und auf dem Router zu installieren:

1. Öffnen Sie die CUCM-Webseite für die Betriebssystemverwaltung.
2. Wählen Sie **Sicherheit > Certificate Management** aus.
Hinweis: Dieser Speicherort kann sich je nach CUCM-Version ändern.
3. Suchen Sie das Zertifikat mit der Bezeichnung **CAPF**, und laden Sie die Datei **.pem** herunter.
Speichern als **.txt**-Datei
4. Nachdem das Zertifikat extrahiert wurde, erstellen Sie einen neuen Trustpoint auf dem Router, und authentifizieren Sie den Trustpoint mit CAPF, wie hier gezeigt. Wenn Sie zur Eingabe des Base-64-codierten CA-Zertifikats aufgefordert werden, wählen Sie den Text aus und fügen ihn zusammen mit den BEGIN- und END-Zeilen in der heruntergeladenen **.pem**-Datei ein.

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#
```

```
quit
```

Zu beachten:

- Die Anmeldemethode ist terminal, da das Zertifikat manuell auf dem Router installiert werden muss.
- Der Befehl **authorized username** (Benutzername für die Autorisierung) ist erforderlich, um dem Router mitzuteilen, wie er beim Herstellen der Verbindung als Benutzername verwendet werden soll. In diesem Fall wird der Gemeinsame Name (CN) verwendet.
- Eine Widerrufsüberprüfung muss deaktiviert werden, da für Telefonzertifikate keine CRL (Certificate Revocation List) definiert ist. Wenn die Verbindung also nicht deaktiviert ist, schlägt sie fehl, und die Debugger der Public Key Infrastructure (PKI) zeigen diese Ausgabe an:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilities request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Konfigurieren des virtuellen Kontexts und der Gruppenrichtlinie

Dieser Teil der Konfiguration ähnelt der zuvor verwendeten Konfiguration, mit Ausnahme von zwei Punkten:

- Die Authentifizierungsmethode
- Der Trustpoint, den der Kontext zur Authentifizierung der Telefone verwendet.

Die Befehle werden hier angezeigt:

```
webvpn context SSL
gateway SSL domain SSLPhones
authentication certificate
ca trustpoint CAPF
!
ssl authenticate verify all
inservice
!
policy group phones
  functions svc-enabled
  svc address-pool "ap_phonevpn" netmask 255.255.255.0
  svc keep-client-installed
default-group-policy phones
```

Call Manager-Konfiguration

In diesem Abschnitt werden die Konfigurationsschritte für den Call Manager beschrieben.

Exportieren Sie das selbst signierte oder Identitätszertifikat vom Router in den CUCM.

Gehen Sie wie folgt vor, um das Zertifikat vom Router zu exportieren und als Telefon-VPN-Trust-Zertifikat in Call Manager zu importieren:

1. Überprüfen Sie das für SSL verwendete Zertifikat.

```
Router#show webvpn gateway SSL
SSL Trustpoint: server-certificate
```

2. Exportieren Sie das Zertifikat.

```
Router(config)#crypto pki export server-certificate pem terminal
The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
-----BEGIN CERTIFICATE-----

<output removed>

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

3. Kopieren Sie den Text aus dem Terminal und speichern Sie ihn als **.pem**-Datei.
4. Melden Sie sich bei Call Manager an, und wählen Sie **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust aus**, um die im vorherigen Schritt gespeicherte Zertifikatsdatei hochzuladen.

Konfigurieren des VPN-Gateways, der Gruppe und des Profils im CUCM

1. Navigieren Sie zu **Cisco Unified CM Administration**.
2. Wählen Sie in der Menüleiste **Erweiterte Funktionen > VPN > VPN Gateway aus**.

3. Gehen Sie im Fenster "VPN Gateway Configuration" wie folgt vor:
 Geben Sie im Feld VPN Gateway Name (VPN-Gateway-Name) einen Namen ein. Dabei kann es sich um einen beliebigen Namen handeln. Geben Sie im Feld VPN Gateway Description (Beschreibung des VPN-Gateways) eine Beschreibung ein (optional). Geben Sie im Feld VPN Gateway URL (VPN-Gateway-URL) die auf dem Router definierte Gruppen-URL ein. Wählen Sie im Feld VPN Certificates in this Location (VPN-Zertifikate in diesem Standort) das Zertifikat aus, das zuvor in Call Manager hochgeladen wurde, um es vom Trust Store an diesen Speicherort zu verschieben.

4. Wählen Sie in der Menüleiste **Advanced Features > VPN > VPN Group (Erweiterte Funktionen > VPN > VPN-Gruppe)** aus.

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

VPN Gateway Configuration

Save Delete Copy Add

Status

Status: Ready

VPN Gateway Information

VPN Gateway Name*

VPN Gateway Description

VPN Gateway URL*

Voice Mail ▸

SAF ▸

EMCC ▸

Intercompany Media Services ▸

Fallback ▸

VPN ▸

VPN Profile

VPN Group

VPN Gateway

VPN Feature Configuration

5. Wählen Sie im Feld All Available VPN Gateways (Alle verfügbaren VPN-Gateways) das zuvor definierte **VPN-Gateway aus**. Klicken Sie auf den Pfeil nach unten, um das ausgewählte Gateway in das Feld Ausgewählte VPN-Gateways in dieser VPN-Gruppe zu verschieben.

VPN Group Configuration

Save Delete Copy Add New

Status

Status: Ready

VPN Group Information

VPN Group Name*

VPN Group Description

VPN Gateway Information

All Available VPN Gateways

Selected VPN Gateways in this VPN Group*

Save Delete Copy Add New

6. Wählen Sie in der Menüleiste **Advanced Features > VPN > VPN Profile (Erweiterte Funktionen > VPN > VPN-Profil)** aus.

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

VPN Group Configuration

Save Delete Copy Add

Status

Status: Ready

VPN Group Information

VPN Group Name*

VPN Group Description

Voice Mail ▸

SAF ▸

EMCC ▸

Intercompany Media Services ▸

Fallback ▸

VPN ▸

VPN Profile

VPN Group

VPN Gateway

VPN Feature Configuration

7. Um das VPN-Profil zu konfigurieren, füllen Sie alle mit einem Sternchen (*) gekennzeichneten Felder aus.

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

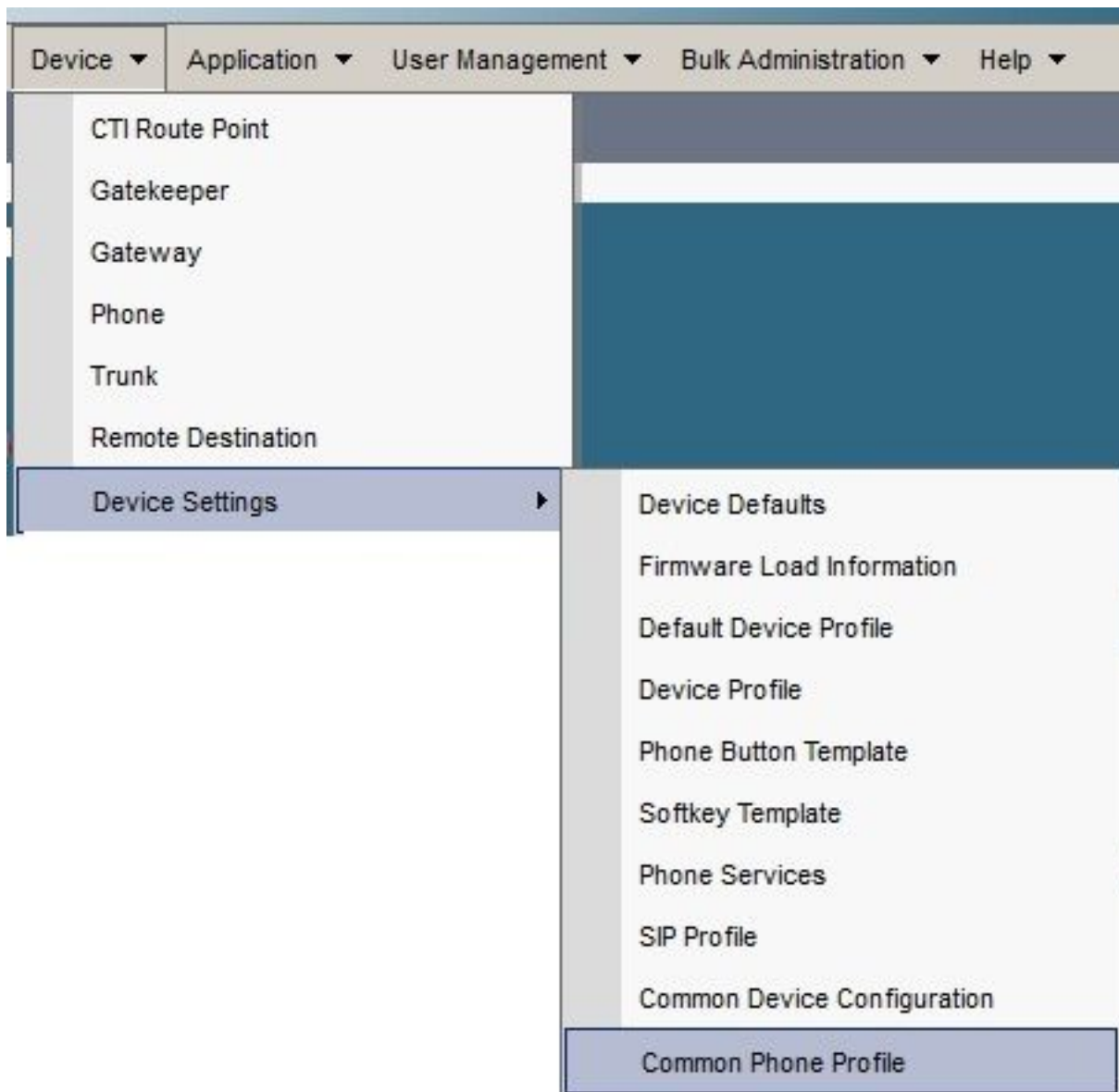
Save Delete Copy Add New

Automatische Netzwerkerkennung aktivieren: Wenn diese Funktion aktiviert ist, pingt das VPN-Telefon den TFTP-Server an. Wenn keine Antwort empfangen wird, wird automatisch eine VPN-Verbindung initiiert.**Host-ID-Prüfung aktivieren:** Wenn diese Funktion aktiviert ist, vergleicht das VPN-Telefon den FQDN (Fully Qualified Domain Name) der VPN Gateway-URL mit dem CN/Storage Area Network (SAN) des Zertifikats. Der Client kann keine

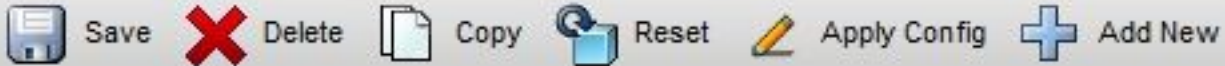
Verbindung herstellen, wenn diese Elemente nicht übereinstimmen oder ein Platzhalterzertifikat mit einem Sternchen (*) verwendet wird. **Kennwortpersistenz aktivieren:** Auf diese Weise kann das VPN-Telefon den Benutzernamen und das Kennwort für den nächsten VPN-Versuch zwischenspeichern.

Wenden Sie Gruppe und Profil auf das IP-Telefon mit dem allgemeinen Telefonprofil an.

Klicken Sie im Fenster Konfiguration des allgemeinen Telefonprofils auf **Config anwenden**, um die neue VPN-Konfiguration anzuwenden. Sie können das standardmäßige **allgemeine Telefonprofil** verwenden oder ein neues Profil erstellen.



Common Phone Profile Configuration

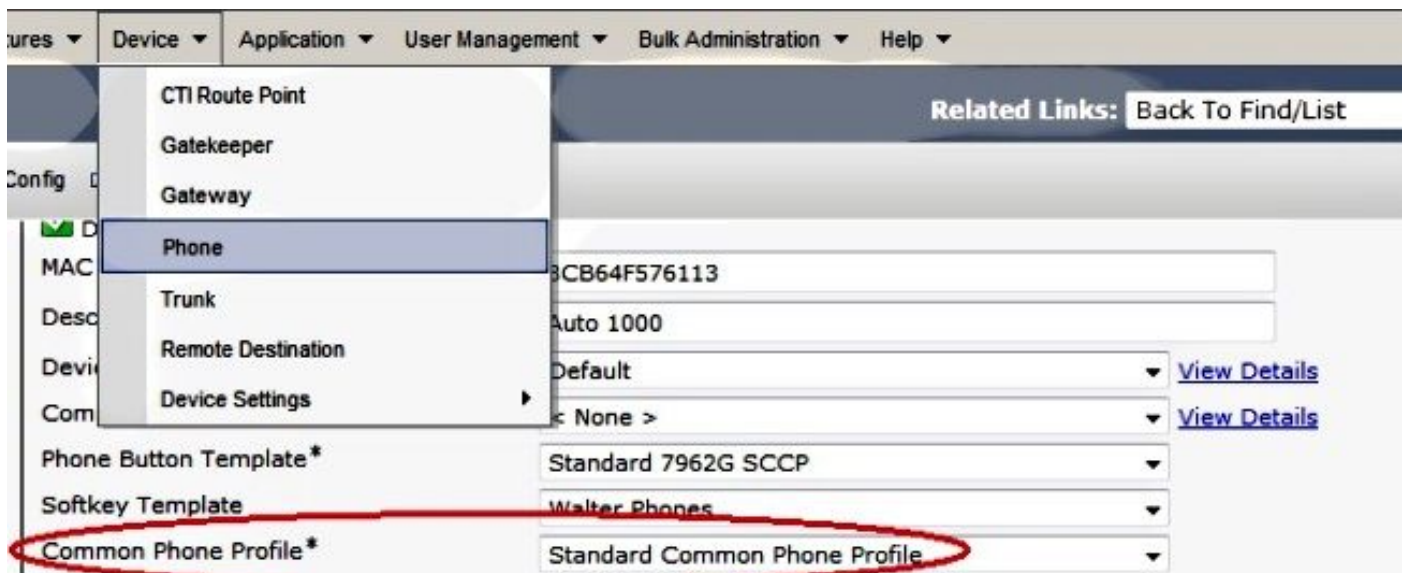


VPN Information

VPN Group	IOS_SSL_Phones
VPN Profile	IOS_SSL_Phones

Wenden Sie das allgemeine Telefonprofil auf das IP-Telefon an.

Wenn Sie ein neues Profil für bestimmte Telefone/Benutzer erstellt haben, navigieren Sie zum Fenster **Telefonkonfiguration**. Wählen Sie im Feld Common Phone Profile (Allgemeines Telefonprofil) das **Standard Common Phone Profile** (Standardtelefonprofil) aus.



Installation von LSC (Locally Significant Certificates) auf Cisco IP-Telefonen

Der folgende Leitfaden kann verwendet werden, um lokale Zertifikate mit hoher Relevanz auf Cisco IP-Telefonen zu installieren. Dieser Schritt ist nur erforderlich, wenn die LSC-Authentifizierung verwendet wird. Für die Authentifizierung mithilfe des MIC (Manufacturer Installed Certificate) oder des Benutzernamens und Kennworts ist die Installation eines LSC nicht erforderlich.

[Installieren Sie ein LSC auf einem Telefon, dessen CUCM-Cluster-Sicherheitsmodus auf "Nicht sicher" eingestellt ist.](#)

Registrieren Sie das Telefon erneut beim Call Manager, um die neue Konfiguration herunterzuladen.

Dies ist der letzte Schritt im Konfigurationsprozess.

Überprüfen

Router-Verifizierung

Um die Statistiken der VPN-Sitzung im Router zu überprüfen, können Sie diese Befehle verwenden und die Unterschiede zwischen den Ausgaben (hervorgehoben) für Benutzernamen und Zertifikatsauthentifizierung überprüfen:

Zur Authentifizierung von Benutzernamen und Kennwort:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)
```

```
Username : phones Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#
```

```
Router#show webvpn session context all
```

```
WebVPN context name: SSL
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
phones 172.16.250.34 1 00:30:38 00:00:20
```

Zur Zertifikatsauthentifizierung:

```
Router#show webvpn session user SEP8CB64F578B2C context all
```

```
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)
```

```
Username : SEP8CB64F578B2C Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
```

Client Ports : 50122
DTLS Port : 52932

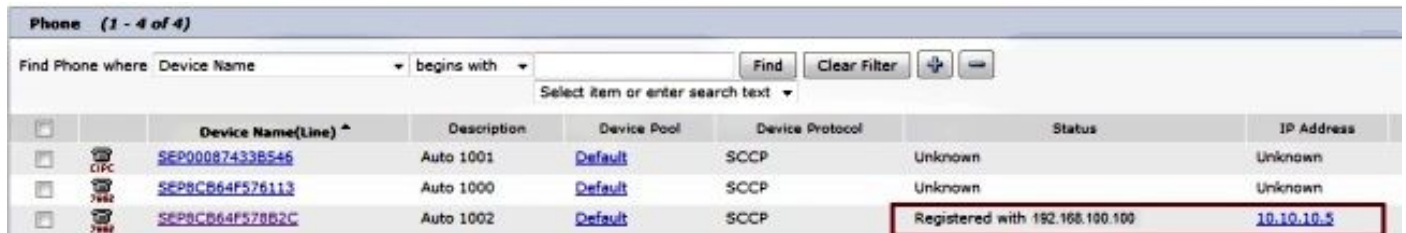
Router#**show webvpn session context all**

WebVPN context name: SSL

Client_Login_Name	Client_IP_Address	No_of_Connections	Created	Last_Used
SEP8CB64F578B2C	172.16.250.34	1	3d04h	00:00:16

CUCM-Verifizierung

Bestätigen Sie, dass das IP-Telefon beim Call Manager mit der zugewiesenen Adresse registriert ist, die der Router für die SSL-Verbindung bereitstellt.



Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
SEP8CB64F578113	Auto 1000	Default	SCCP	Unknown	Unknown
SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

Fehlerbehebung

Debuggen auf dem SSL VPN-Server

Router#**show debug**

WebVPN Subsystem:

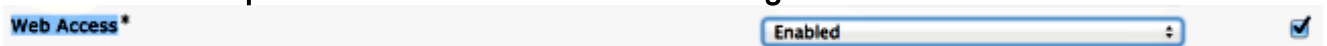
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on

PKI:


Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on

Debugger vom Telefon aus

1. Navigieren Sie vom CUCM zu **Gerät > Telefon**.
2. Legen Sie auf der Seite Gerätekonfiguration den Webzugriff auf **Aktiviert fest**.
3. Klicken Sie auf **Speichern** und anschließend auf **Konfig. übernehmen**.



4. Geben Sie in einem Browser die IP-Adresse des Telefons ein, und wählen Sie im Menü auf der linken Seite die Option **Konsolenprotokolle** aus.

	<h2 style="text-align: right;">Console Logs</h2> <p style="text-align: right;">Cisco Unified IP Phone CP-7965G (SEP001D45B64090)</p>
<ul style="list-style-type: none"> Device Information <u>Network Configuration</u> Network Statistics <u>Ethernet Information</u> Access Network Device Logs <ul style="list-style-type: none"> <u>Console Logs</u> Core Dumps Status Messages Debug Display Streaming Statistics <ul style="list-style-type: none"> <u>Stream 1</u> Stream 2 <u>Stream 3</u> Stream 4 <u>Stream 5</u> 	<ul style="list-style-type: none"> <u>/FS/cache/fsck.fd0a.log</u> <u>/FS/cache/fsck.fd1a.log</u> <u>/FS/cache/log6.log</u> <u>/FS/cache/log2.log</u> <u>/FS/cache/log3.log</u> <u>/FS/cache/log4.log</u> <u>/FS/cache/log5.log</u>

5. Laden Sie alle **/FS/Cache/log*.log**-Dateien herunter. Die Konsolenprotokolldateien enthalten Informationen darüber, warum das Telefon keine Verbindung zum VPN herstellen kann.

Zugehörige Fehler

Cisco Bug ID [CSCty46387](#), IOS SSLVPN: Erweiterung, um einen Kontext als Standard festzulegen

Cisco Bug ID [CSCty46436](#), IOS SSLVPN: Verbesserung des Validierungsverhaltens von Clientzertifikaten