

AnyConnect VPN-telefoonverbinding met een Cisco IOS-routerconfiguratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerktopologie](#)

[Configuratie van SSL VPN-server](#)

[Gemeenschappelijke configuratiestappen](#)

[Configuratie met AAA-verificatie](#)

[Configuratie met de IP-telefoon: Lokaal Significant Certificaat \(LSC\) voor clientverificatie](#)

[Configuratie van Call Manager](#)

[Exporteren van het zelfgetekende of identiteitsbewijs van de router naar CUCM](#)

[Het configureren van de VPN-gateway, -groep en -profiel in CUCM](#)

[Pas de groep en het profiel op de IP-telefoon met het gemeenschappelijke telefoonprofiel toe](#)

[Het gemeenschappelijke telefoonprofiel op IP-telefoon toepassen](#)

[Installeer lokaal significante certificaten \(LSC\) op Cisco IP-telefoons](#)

[Registreer de telefoon om Manager opnieuw te bellen om de nieuwe configuratie te downloaden](#)

[Verifiëren](#)

[Routerverificatie](#)

[CUCM-verificatie](#)

[Problemen oplossen](#)

[Debugs op de SSL VPN-server](#)

[Telefonische telefoons](#)

[Verwante bellen](#)

Inleiding

Dit document beschrijft hoe u de apparaten Cisco IOS[®] en Call Manager kunt configureren zodat Cisco IP-telefoons VPN-verbindingen kunnen maken met de Cisco IOS-router. Deze VPN-verbindingen zijn nodig om de communicatie met een van deze twee methoden voor clientverificatie te beveiligen:

- Verificatie, autorisatie en accounting (AAA) server of lokale database
- Telefooncertificaat

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco IOS 15.1(2)T of hoger
- Functieset/licentie: Universal (Data en Security & UC) voor Cisco IOS geïntegreerde services router (ISR)-G2
- Functieset/licentie: Geavanceerde beveiliging voor Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM) release 8.0.1.100/2000-4 of hoger
- IP-telefoonrelease 9.0(2)SR1S - SnipperNE Call Control Protocol (SCCP) voor later

Voltooi de volgende stappen voor een compleet overzicht van de ondersteunde telefoons in uw CUCM-versie:

1. Open deze URL: <https://<CUCM Server IP Address>:8443/cucreports/systemReports.do>
2. Kies **Unified CM-telefoonfunctielijst > Generate een nieuw rapport > Functie: Virtual Private Network**.

De releases die in dit configuratievoorbeeld worden gebruikt zijn onder meer:

- Cisco IOS-software release 15.1(4)M4
- Call Manager release 8.5.1.100-26
- IP-software release 9.1(1)SR1S

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

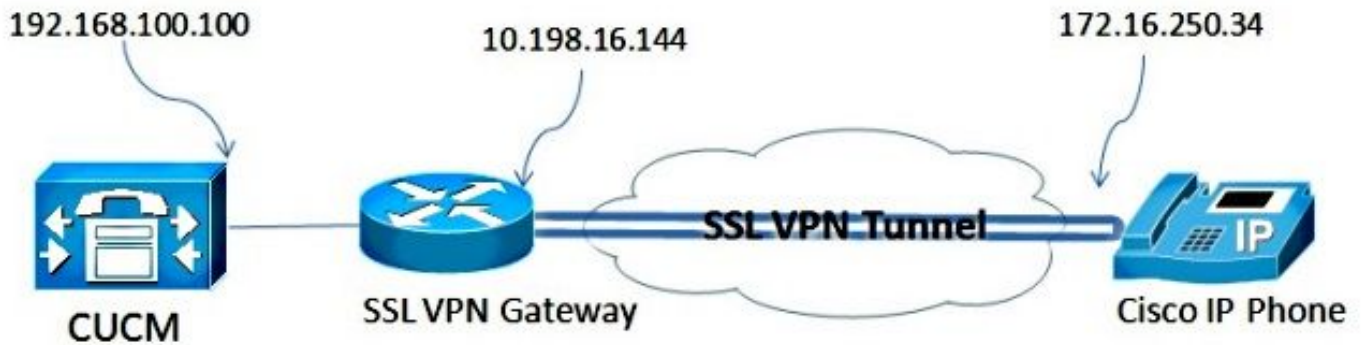
Configureren

Deze sectie bestrijkt de informatie die nodig is om de functies te configureren die in dit document worden beschreven.

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt](#).

Netwerktopologie

De topologie die in dit document wordt gebruikt omvat één Cisco IP-telefoon, de Cisco IOS-router als de Secure Socket Layer (SSL) VPN-gateway en CUCM als spraakgateway.



Configuratie van SSL VPN-server

Deze sectie beschrijft hoe u de Cisco IOS head-end kunt configureren om inkomende SSL VPN-verbindingen toe te staan.

Gemeenschappelijke configuratiestappen

1. Generate the Rivest-Shamir-Adleman (RSA) Key met een lengte van 1024 bytes:

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

2. Maak het vertrouwenspunt voor het zelfgetekende certificaat en voeg de **SSL RSA-toets** toe:

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

3. Nadat het trustpoint is ingesteld, kunt u het zelfgetekende certificaat met deze opdracht invoeren:

```
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. Schakel het juiste AnyConnect-pakket in op het head-end. De telefoon zelf downloaden dit pakket niet. Maar zonder het pakket kan de VPN-tunnel niet tot stand komen. Het wordt aanbevolen de nieuwste versie van de clientsoftware te gebruiken die beschikbaar is op Cisco.com. In dit voorbeeld wordt versie 3.1.3103 gebruikt.

In oudere Cisco IOS versies is dit de opdracht om het pakket in te schakelen:

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

In de nieuwste Cisco IOS-versie is dit echter de opdracht:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
```

3.1.03103-k9.pkg sequence 1

5. Configuratie van de gateway van VPN. De gateway van WebVPN wordt gebruikt om de SSL verbinding van de gebruiker te beëindigen.

```
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
```

Opmerking: Ofwel het IP adres dat hier gebruikt wordt moet op dezelfde subunit zijn als de interface waaraan de telefoons verbinden, of de gateway moet direct van een interface op de router zijn afkomstig. De gateway wordt ook gebruikt om te bepalen welk certificaat door de router wordt gebruikt om zichzelf aan de cliënt te valideren.

6. Definieer de lokale pool die wordt gebruikt om IP adressen aan de klanten toe te wijzen wanneer zij verbinden:

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

Configuratie met AAA-verificatie

In dit gedeelte worden de opdrachten beschreven die u nodig hebt om de AAA-server of de lokale database te configureren zodat u uw telefoons voor het eerst echt kunt maken. Als u van plan bent om certificaat-enige Verificatie voor de telefoons te gebruiken, ga dan verder naar de volgende sectie.

De gebruikersdatabase configureren

Ofwel de lokale database van de router of een externe AAA server kan gebruikt worden voor verificatie:

- Om de lokale database te configureren voert u in:

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

- Om een afgelegen AAA RADIUS-server voor verificatie te configureren voert u het volgende in:

```
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
```

De virtuele context en het groepsbeleid configureren

De virtuele context wordt gebruikt om de eigenschappen te definiëren die de VPN-verbinding regelen, zoals:

- Welke URL te gebruiken wanneer u verbinding maakt
- Welke pool te gebruiken om de clientadressen toe te wijzen
- Welke authenticatiemethode te gebruiken

Deze opdrachten zijn een voorbeeld van een context waarin AAA-verificatie voor de client wordt

gebruikt:

```
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
```

Configuratie met de IP-telefoon: Lokaal Significant Certificaat (LSC) voor clientverificatie

In dit gedeelte worden de opdrachten beschreven die u nodig hebt om op certificaat gebaseerde clientverificatie voor de telefoons te configureren. Om dat te kunnen doen is echter kennis van de verschillende typen telefooncertificaten vereist:

- **MIC-telefoons (Fabrikant Geïnstalleerd Certificaat)** - MIC's zijn meegeleverd voor alle 7941, 7961 en nieuwer-model Cisco IP-telefoons. MIC's zijn 2.048-bits belangrijke certificaten die door de Cisco certificaatinstantie (CA) zijn ondertekend. Om het CUCM te laten vertrouwen in het MIC certificaat gebruikt het de voorgeïnstalleerde CA certificaten CAP-RTP-001, CAP-RTP-002 en Cisco_Manufacturing_CA in zijn certificaatruimte store. Omdat dit certificaat door de fabrikant zelf wordt verstrekt, zoals aangegeven in de naam, wordt het niet aanbevolen dit certificaat te gebruiken voor de authenticatie van cliënten.
- **LSC** - De LSC waarborgt de verbinding tussen CUCM en de telefoon nadat u de apparaatbeveiligingsmodus voor verificatie of encryptie hebt ingesteld. LSC heeft de openbare sleutel voor de Cisco IP-telefoon, die door de privé-sleutel van de CUCM certificaatautoriteit Proxy-functie (CAPF) wordt ondertekend. Dit is de veiligere methode (in tegenstelling tot het gebruik van MIC's).

Voorzichtig: Vanwege het verhoogde veiligheidsrisico adviseert Cisco het gebruik van MIC's alleen voor LSC-installatie en niet voor doorlopend gebruik. Klanten die Cisco IP-telefoons configureren om MIC's te gebruiken voor TLS-verificatie (Transport Layer Security), of voor een ander doel, doen dit op hun eigen risico.

In dit configuratievoorbeeld, wordt LSC gebruikt om de telefoons voor het echt te verklaren.

Tip: De veiligste manier om uw telefoon aan te sluiten is door dubbele authenticatie te gebruiken, die certificaat en AAA authenticatie combineert. U kunt dit configureren als u de opdrachten die voor elk onderdeel van één virtuele context zijn gebruikt, combineert.

Het trustpunt configureren om het clientcertificaat te valideren

De router moet het CAPF certificaat hebben geïnstalleerd om LSC van de IP telefoon te valideren. Voltooi de volgende stappen om dat certificaat te verkrijgen en het op de router te installeren:

1. Ga naar de webpagina van het CUCM Operating System (OS).
2. Kies **Beveiliging > certificaatbeheer**.

Opmerking: Deze locatie kan veranderen op basis van de CUCM-versie.

3. Vind het certificaat met het label **CAPF** en download het bestand **.pem**. Opslaan als een **.txt**-bestand
4. Zodra het certificaat wordt afgeleid, creëer een nieuw trustpunt op de router, en bevestig het trustpunt met CAPF, zoals hier getoond. Wanneer dit wordt gevraagd voor het basis-64 gecodeerde CA-certificaat, selecteert en plakt u de tekst in het gedownload **.pem**-bestand samen met de regels BEGIN en END.

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

```
quit
```

Opmerkingen:

- De inschrijvingsmethode is terminal omdat het certificaat handmatig op de router moet worden geïnstalleerd.
- De opdracht **gebruikersnaam** voor autorisatie is vereist om de router te vertellen wat hij als gebruikersnaam moet gebruiken wanneer de client de verbinding maakt. In dit geval gebruikt het de GN-code.
- Een herroepingscontrole moet worden uitgeschakeld omdat telefooncertificaten geen certificaatherroeping (CRL) hebben gedefinieerd. Dus, tenzij het uitgeschakeld is, mislukt de verbinding en tonen de PKI-implementaties (Public Key Infrastructure) deze output:

```
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
```

De virtuele context en het groepsbeleid configureren

Dit gedeelte van de configuratie lijkt op de configuratie die eerder is gebruikt, behalve voor twee punten:

- De authenticatiemethode
- Het vertrouwde punt van de context gebruikt om de telefoons voor authentiek te verklaren

De opdrachten worden hier weergegeven:

```
webvpn context SSL
gateway SSL domain SSLPhones
authentication certificate
```

```
ca trustpoint CAPF
!
ssl authenticate verify all
inervice
!
policy group phones
  functions svc-enabled
  svc address-pool "ap_phonevpn" netmask 255.255.255.0
  svc keep-client-installed
default-group-policy phones
```

Configuratie van Call Manager

In deze sectie worden de configuratiestappen in Call Manager beschreven.

Exporteren van het zelfgetekende of identiteitsbewijs van de router naar CUCM

Voltooi de volgende stappen om het certificaat van de router te exporteren en het certificaat in Call Manager te importeren als een Phone-VPN-Trust-certificaat:

1. Controleer het certificaat dat wordt gebruikt voor SSL.

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

2. Exporteren van het certificaat.

```
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. Kopieert de tekst uit het terminal en slaat deze op als een **.pem**-bestand.
4. Meld u aan bij Call Manager en kiest u **Unified OS-beheer > Beveiliging > certificaatbeheer > Uploadcertificaat > Selecteer Phone-VPN-trust** om het certificaatbestand te uploaden dat in de vorige stap is opgeslagen.

Het configureren van de VPN-gateway, -groep en -profiel in CUCM

1. Navigeer naar **Cisco Unified CM Management**.
2. Kies in de menubalk **geavanceerde functies > VPN > VPN-gateway**.

3. Vultooi de volgende stappen in het venster VPN-gateway Configuration:

Typ een naam in het veld Naam van de VPN-gateway. Dit kan elke naam zijn. Typ een beschrijving (optioneel) in het veld VPN Gateway Description. Voer in het veld URL van de VPN-gateway de groep-URL in die op de router is gedefinieerd. In het veld VPN-certificaten in deze locatie kiest u het certificaat dat eerder is geüpload naar Call Manager om het te verplaatsen van de trustwinkel naar deze locatie.

4. Kies in de menubalk Geavanceerde functies > VPN > VPN-groep.

5. Kies in het veld Alle beschikbare VPN-gateways de eerder gedefinieerde **VPN-gateway**. Klik op de pijl-omlaag om de geselecteerde gateway naar de geselecteerde VPN-gateways in het veld VPN-groep te verplaatsen.

VPN Group Configuration

Save Delete Copy Add New

Status

Status: Ready

VPN Group Information

VPN Group Name* IOS_SSL_Phones

VPN Group Description

VPN Gateway Information

All Available VPN Gateways

Selected VPN Gateways in this VPN Group* IOS_SSL_Phones

Save Delete Copy Add New

6. Kies in de menubalk **geavanceerde functies > VPN > VPN-profiel**.

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* IOS_SSL_Phones

VPN Group Description

Voice Mail

SAF

EMCC

Intercompany Media Services

Fallback

VPN

VPN Profile

VPN Group

VPN Gateway

VPN Feature Configuration

7. Voltooi alle velden die met een asterisk (*) zijn gemarkeerd om het VPN-profiel te configureren.

VPN Profile Configuration



Save



Delete



Copy



Add New

Status



Status: Ready

VPN Profile Information

Name*

IOS_SSL_Phones

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

1290

Fail to Connect*

30

Enable Host ID Check

Client Authentication

Client Authentication Method* Certificate

Enable Password Persistence

Save

Delete

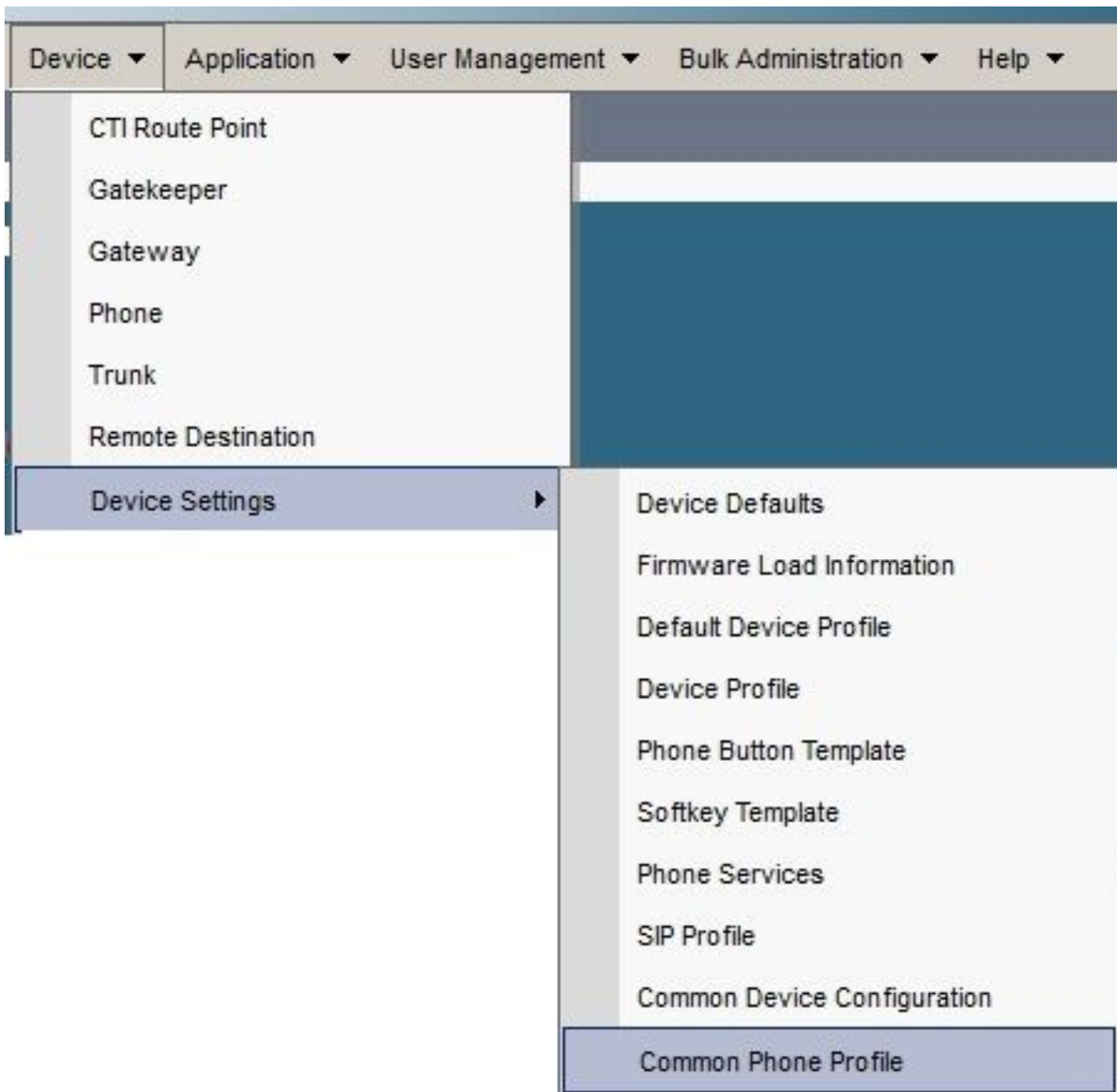
Copy

Add New

Auto netwerk detecteren: Indien ingeschakeld, pingelt de VPN-telefoon de TFTP-server. Als geen antwoord wordt ontvangen, start het automatisch een VPN-verbinding.
Schakel Host ID in: Als deze functie is ingeschakeld, wordt op de VPN-telefoon de Full Qualified Domain Name (FQDN) van de VPN-gateway vergeleken met de CN/Storage Area Network (SAN) van het certificaat. De client heeft geen verbinding als deze items niet overeenkomen of als een wildkaartcertificaat met een sterretje (*) wordt gebruikt.
Wachtwoordpersistentie inschakelen: Dit staat de VPN telefoon toe om de gebruikersnaam en het wachtwoord voor de volgende VPN-poging in het geheugen te stoppen.

Pas de groep en het profiel op de IP-telefoon met het gemeenschappelijke telefoonprofiel toe

Klik in het venster Common Phone Profile Configuration op **Config** om de nieuwe VPN-configuratie toe te passen. U kunt het standaard **Gemeenschappelijk telefoonprofiel** gebruiken of een nieuw profiel maken.



Het gemeenschappelijke telefoonprofiel op IP-telefoon toepassen

Als u een nieuw profiel voor specifieke telefoons/gebruikers hebt gemaakt, navigeer dan naar het venster **Phone Configuration**. Kies in het veld Gemeenschappelijke telefoonprofiel het **standaard** profiel **Gemeenschappelijke telefoon**.



Installeer lokaal significante certificaten (LSC) op Cisco IP-telefoons

De volgende handleiding kan worden gebruikt om lokaal belangrijke certificaten op Cisco IP-telefoons te installeren. Deze stap is alleen nodig als de verificatie met behulp van de LSC wordt gebruikt. Verificatie met het geïnstalleerde certificaat (MIC) of de gebruikersnaam en het wachtwoord vereist geen LSC te installeren.

[Installeer een LSC op een telefoon met CUCM Cluster Security Mode die is ingesteld op Non-Secure.](#)

Registreer de telefoon om Manager opnieuw te bellen om de nieuwe configuratie te downloaden

Dit is de laatste stap in het configuratieproces.

Verifiëren

Routerverificatie

Om de statistieken van de zitting van VPN in de router te controleren, kunt u deze opdrachten gebruiken, en de verschillen tussen de uitgangen (gemarkeerd) controleren voor gebruikersnaam en certificatie:

Voor gebruikersnaam/wachtwoordverificatie:

```
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

```

Voor certificatie:

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-verificatie

Bevestig dat de IP-telefoon bij de Call Manager met het toegewezen adres van de router wordt geregistreerd die aan de SSL-verbinding wordt geleverd.

Phone (1 - 4 of 4)							
Find Phone where Device Name begins with <input type="text"/> Find Clear Filter							
Select item or enter search text							
<input type="checkbox"/>		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
<input type="checkbox"/>		SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B2C	Auto 1000	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

Problemen oplossen

Debugs op de SSL VPN-server

```
Router#show debug
```

WebVPN Subsystem:

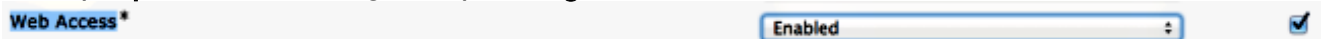
```
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on
```

PKI:

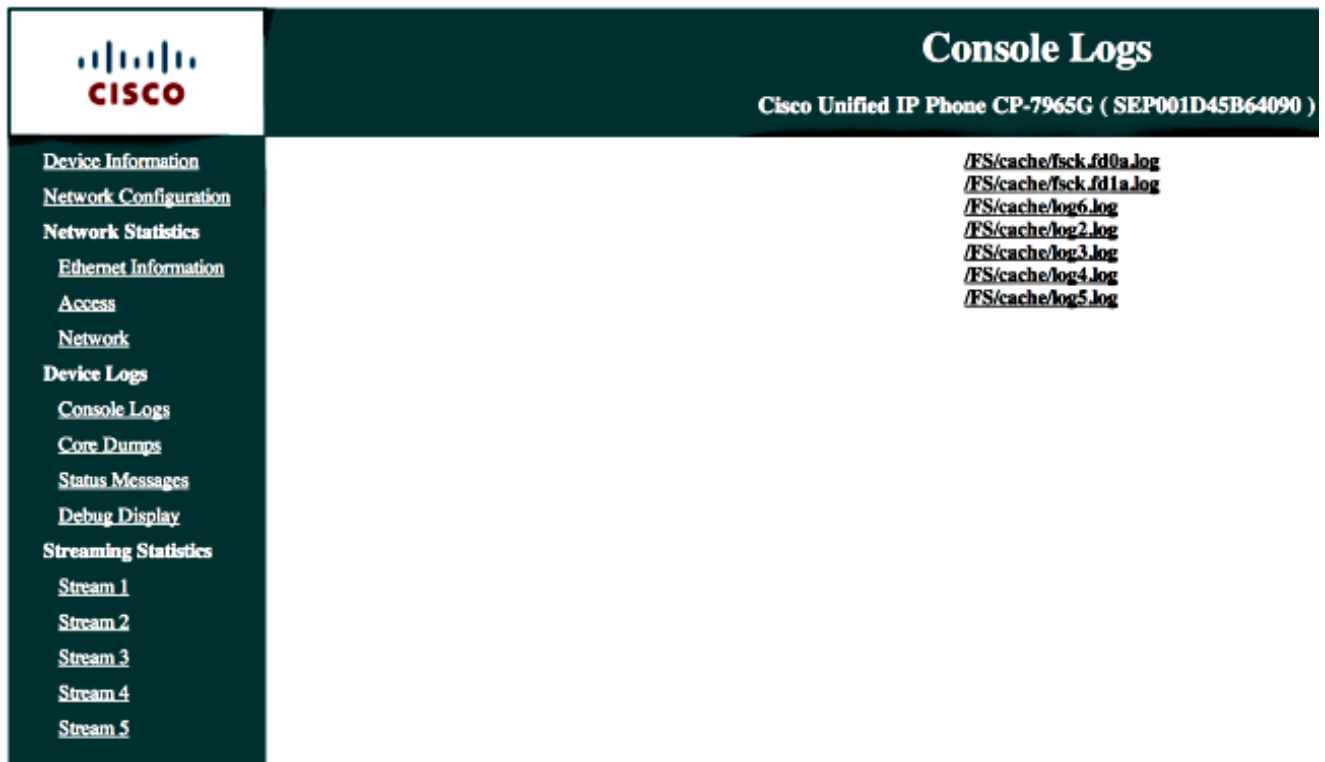
```
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

Telefonische telefoons

1. Navigeer naar **apparaat > telefoon** vanaf CUCM.
2. Op de pagina van de apparaatconfiguratie, stelt u Web Access in op **Enabled**.
3. Klik op **Opslaan** en vervolgens op **Config**.



4. Voer in een browser het IP-adres van de telefoon in en kies **Logs van de console** in het menu links.

A screenshot of the Cisco Unified IP Phone configuration page. The top left shows the Cisco logo. The top right shows 'Console Logs' and 'Cisco Unified IP Phone CP-7965G (SEP001D45B64090)'. On the left is a navigation menu with options like 'Device Information', 'Network Configuration', 'Device Logs', and 'Console Logs'. The 'Console Logs' option is selected. On the right, a list of log files is displayed: /FS/cache/fsck.fd0a.log, /FS/cache/fsck.fd1a.log, /FS/cache/log6.log, /FS/cache/log2.log, /FS/cache/log3.log, /FS/cache/log4.log, and /FS/cache/log5.log.

5. Download alle **/FS/cache/log*.log** bestanden. De logbestanden van de console bevatten informatie over waarom de telefoon geen verbinding maakt met VPN.

Verwante bellen

Cisco bug-id [CSCty46387](#), IOS VPN: Verbetering in een context als standaard

Cisco bug-id [CSCty46436](#), IOS VPN: Verbetering van de validatie van klantcertificaten