

AnyConnect VPN-telefoon met certificaatverificatie op een ASA configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Telefooncertificaattypen](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie die toont hoe u de adaptieve security applicatie (ASA) en CallManager apparaten kunt configureren om certificatie te bieden voor AnyConnect-clients die op Cisco IP-telefoons worden uitgevoerd. Nadat deze configuratie is voltooid, kunnen Cisco IP-telefoons VPN-verbindingen naar de ASA maken die gebruik maken van certificaten om de communicatie te beveiligen.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- AnyConnect Premium SSL-licentie
- AnyConnect voor Cisco VPN-telefoonlicentie

Afhankelijk van de ASA versie ziet u "AnyConnect voor Linksys Phone" voor ASA release 8.0.x of "AnyConnect voor Cisco VPN-telefoon" voor ASA release 8.2.x of later.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA - release 8.0(4) of hoger
- IP-telefoonmodellen - 7942/7962/7945/7965/7975
- Telefoons - 8961/9951/9971 met release 9.1(1) firmware
- Telefoon - release 9.0(2)SR1S - Snipperry Call Control Protocol (SCCP) of hoger
- Cisco Unified Communications Manager (CUCM) - release 8.0.1.100/2000-4 of hoger

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

- ASA - release 9.1(1)
- CallManager - release 8.5.1.100/26

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 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.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Telefooncertificaattypen

Cisco gebruikt deze certificaattypen in telefoons:

- MIC's (fabriekscertificaat) - MIC's zijn meegeleverd voor alle 7941, 7961 en nieuwere modellen Cisco IP-telefoons. MIC's zijn 2048-bits belangrijke certificaten die door de Cisco certificaatinstantie (CA) zijn ondertekend. Wanneer er een MIC is aanwezig, is het niet nodig om een lokaal belangrijk certificaat (LSC) te installeren. 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 certificaat trust store.
- 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 meest gewenste methode (in tegenstelling tot het gebruik van MIC's) omdat alleen Cisco IP-telefoons die handmatig van provisioning zijn voorzien door een beheerder, het CTL-bestand mogen downloaden en controleren. **Opmerking:** 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.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het [Opdrachtuppgereedschap](#) (alleen [geregistreeerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuraties

In dit document worden deze configuraties beschreven:

- ASA-configuratie
- Configuratie van CallManager
- VPN-configuratie op CallManager
- Installatie van certificaat op IP-telefoons

ASA-configuratie

De configuratie van de ASA is vrijwel hetzelfde als wanneer u een AnyConnect-clientcomputer aansluit op de ASA. Deze beperkingen gelden echter:

- De tunnelgroep moet een groepring hebben. Deze URL wordt in CM ingesteld onder de URL van de VPN-gateway.
- Het groepsbeleid mag geen splitsende tunnel bevatten.

Deze configuratie gebruikt een eerder ingesteld en geïnstalleerd ASA (zelf-ondertekend of derde) certificaat in het Secure Socket Layer (SSL) trustpunt van het ASA-apparaat. Verwijs voor meer informatie naar deze documenten:

- [Digitale certificaten configureren](#)
- [ASA 8.x Installeer Verkrakers van 3 partijen handmatig voor gebruik met WebVPN-configuratievoorbeeld](#)
- [ASA 8.x: VPN-toegang met de AnyConnect VPN-client met zelfgetekende configuratievoorbeeld van certificaat](#)

De toepasselijke configuratie van de ASA is:

```
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

Configuratie van CallManager

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

1. Registreer het gegenereerde certificaat met CUCM.
2. Controleer het certificaat dat wordt gebruikt voor SSL.

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

3. Exporteren van het certificaat.

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

Het privacyuitgebreide e-mail (PEM) gecodeerde identiteitsbewijs:

```
-----BEGIN CERTIFICATE-----ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxZjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xssovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9xOpR7BFpZd1yFyzwAPkoB11
-----END CERTIFICATE-----
```

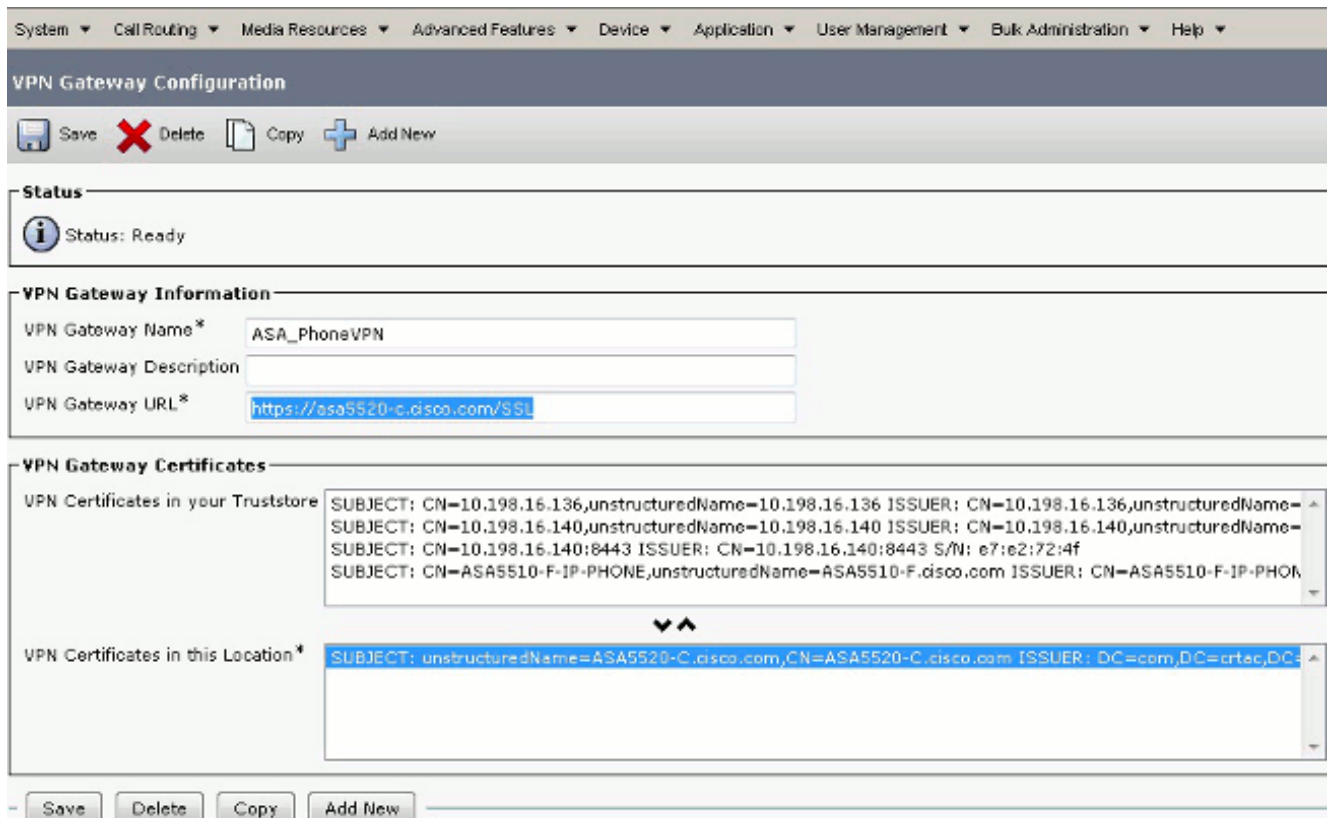
4. Kopieert de tekst uit het terminal en slaat deze op als een .pem-bestand.
5. Meld u aan bij CallManager en kiest u **Unified OS-beheer > Beveiliging > certificaatbeheer > Uploadcertificaat > Selecteer Phone-VPN-trust** om het certificaatbestand te uploaden dat in de vorige stap is opgeslagen.

VPN-configuratie op CallManager

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

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', and 'Bulk Administration'. The 'Advanced Features' menu is expanded, showing options like 'Voice Mail', 'SAF', 'EMCC', 'Intercompany Media Services', 'Fallback', and 'VPN'. The 'VPN' option is selected, and a sub-menu is displayed with 'VPN Profile', 'VPN Group', 'VPN Gateway', and 'VPN Feature Configuration'. The 'VPN Gateway' option is highlighted. The main content area displays 'Cisco Unified CM Administration' and 'System version: 8.5.1.10000-26'. A red warning message states: 'Licensing Warning: System is operating on Demo Licenses. Please visit the License Report Page for more details.' The VMware installation details are shown as '2 vCPU Intel(R) Xeon(R) CPU E5540 @ 2.53GHz'. The bottom status bar indicates 'Last Successful Logon: Feb 5, 2013 5:55:45 PM'.

3. Voltooi 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 ASA is gedefinieerd. In het veld VPN-certificaten in deze locatie selecteert u het certificaat dat eerder is geüpload naar CallManager om het vanuit de trustwinkel naar deze locatie te verplaatsen.



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



5. Selecteer 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.

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

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

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

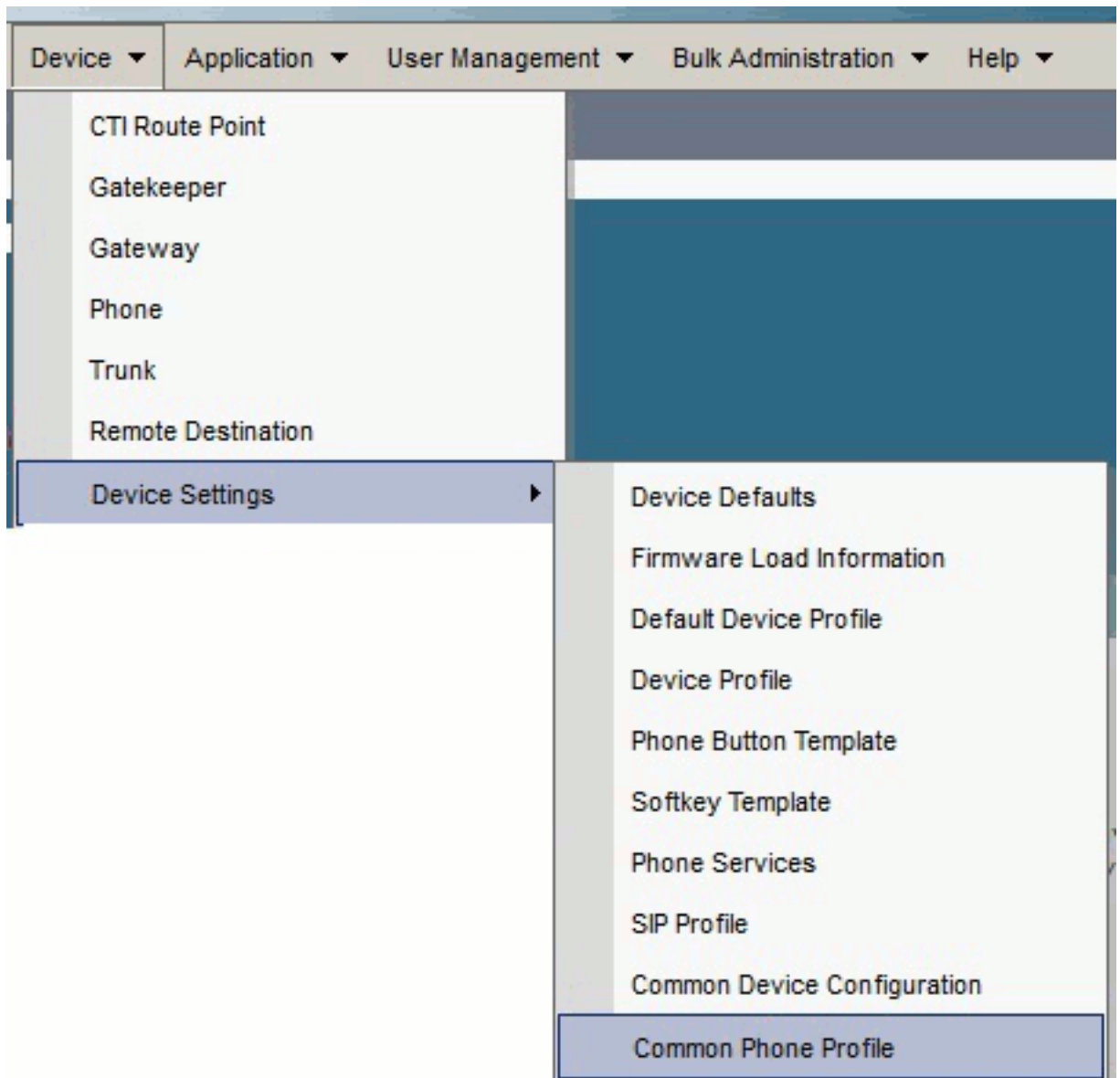
Client Authentication

Client Authentication Method*

Enable Password Persistence

Auto netwerk detecteren: Als ingeschakeld, wordt de VPN-telefoon op de TFTP-server geplaatst en als er geen respons wordt ontvangen, wordt er een VPN-verbinding automatisch gestart. **Schakel Host ID in:** Als deze functie is ingeschakeld, vergelijkt de VPN-telefoon de FQDN van de VPN-gateway met de N/SAN van het certificaat. De client heeft geen verbinding als deze niet overeenkomen of als een certificaat met jokerteken met een sterretje (*) is 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.

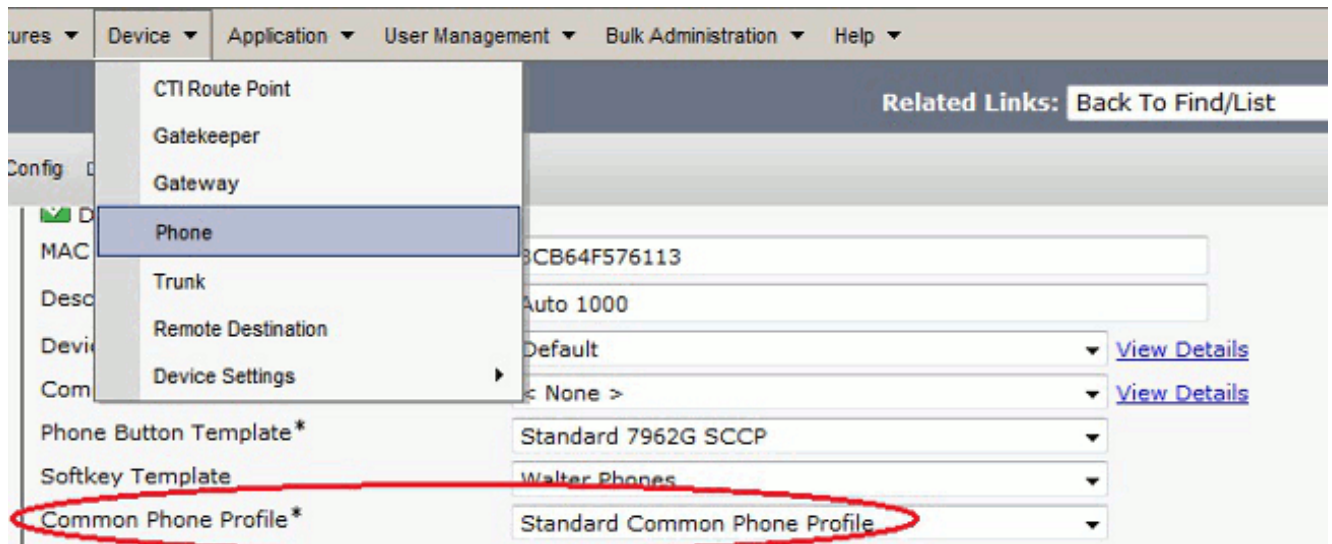
- Klik in het venster Common Phone Profile Configuration op **Config** om de nieuwe VPN-configuratie toe te passen. U kunt het "Standaard gemeenschappelijke telefoonprofiel" gebruiken of een nieuw profiel



maken.



9. Als u een nieuw profiel voor specifieke telefoons/gebruikers hebt gemaakt, gaat u naar het venster Configuration. Kies in het veld Gemeenschappelijk telefoonprofiel de optie **Standaard gemeenschappelijk telefoonprofiel**.



10. Registreer de telefoon aan CallManager opnieuw om de nieuwe configuratie te downloaden.





Configuratie van certificaten

Voltooi de volgende stappen in CallManager en de ASA:


1. Kies in de menubalk **geavanceerde functies > VPN > VPN-profiel**.
2. Controleer of het veld Clientverificatiemethode is ingesteld op **Certificaat**.

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. Meld u aan bij CallManager. Kies in de menubalk **Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken**.

4. Exporteren van de juiste certificaten voor de geselecteerde certificeringsmethode: MIC' s:
Cisco_Manufacturing_CA - Authenticate IP-telefoons met een MIC

Find Certificate List where ▾ begins with ▾  

Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

LSC's: Cisco Certificate Authority Proxy-functie (CAPF) - Verifieer IP-telefoons met een LSC

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	tomcat.pem	tomcat.der
psec	certs	ipsec.pem	ipsec.der
tomcat-trust	trust-certs	CUCM85.pem	CUCM85.der
psec-trust	trust-certs	CUCM85.pem	CUCM85.der
CallManager	certs	CallManager.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TVS.pem	TVS.der
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem	

- Vind het certificaat, of Cisco_Manufacturing_CA of CAPF. Download het .pem-bestand en slaat het op als een .txt-bestand
- Maak een nieuw betrouwbaar punt op de ASA en bevestig het trustpunt met het vorige opgeslagen certificaat. Wanneer u wordt gevraagd om een standaard-64 gecodeerd CA-certificaat, selecteert en plakt u de tekst in het gedownload .pem-bestand samen met de regels BEGIN en END. Een voorbeeld wordt getoond:

```
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
```

- Bevestig de authenticatie in de tunnelgroep op certificatie.

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

Installatie van certificaat op IP-telefoons

De IP-telefoons kunnen werken met MIC's of LSC's, maar het configuratieproces is voor elk certificaat anders.

MIC-installatie

Standaard worden alle telefoons die VPN ondersteunen vooraf geladen met MIC's. De 7960- en 7940-telefoons hebben geen MIC en hebben een speciale installatieprocedure nodig voor de LSC om zich veilig te kunnen registreren.

Opmerking: Cisco raadt u aan MICs alleen te gebruiken voor LSC-installatie. Cisco ondersteunt LSC's om de TLS-verbinding met CUCM te authenticeren. Omdat de MIC wortelcertificaten kunnen worden gecompromitteerd, doen klanten die telefoons configureren om MICs voor TLS authenticatie of voor een ander doel te gebruiken dit op hun eigen risico. Cisco is niet aansprakelijk als MIC's gecompromitteerd zijn.

LSC-installatie

- CAPF-service op CUCM inschakelen.
- Nadat de CAPF-dienst is geactiveerd, verdeel de telefooninstructies om een LSC in CUCM te genereren. Meld u aan bij Cisco Unified CM Management en kies **Apparaat > Telefoon**. Selecteer de telefoon die u hebt ingesteld.
- Zorg ervoor dat in het gedeelte Informatie over certificaatfunctie (CAPF) alle instellingen correct zijn en de bewerking is ingesteld op een toekomstige datum.

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. Als de verificatiemodus is ingesteld op Ongeldige string of bestaand certificaat, hoeft u geen verdere actie te ondernemen.
5. Als de verificatiemodus op een string is ingesteld, selecteert u handmatig **Instellingen > Beveiligingsconfiguratie > *# > LSC > Update** in de telefoonconsole.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

ASA-verificatie

```
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

CUCM-verificatie

The screenshot shows the 'Find and List Phones' interface in CUCM. The table below lists the phones found:

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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Verwante bellen

- Cisco bug-ID [CSCtf09529](#), ondersteuning voor VPN-functie in CUCM voor 8961, 9951 en 9971 telefoons
- Cisco bug ID [CSCuc71462](#), IP-telefoon VPN-failover duurt 8 minuten

- Ondersteuning van Cisco bug-ID [CSCtz42052](#), IP-telefoon SSL VPN voor niet-standaard poortnummers
- Cisco bug-ID [CSCth96551](#), niet alle ASCII-tekenen worden ondersteund bij de inlognaam van een telefoon VPN-gebruiker + wachtwoord.
- Cisco bug-ID [CSCuj71475](#), handmatige TFTP-ingang die nodig is voor IP-telefoon VPN
- Cisco bug-ID [CSCum10683](#), IP-telefoons die niet kunnen worden vastgezet, geplaatst of ontvangen oproepen

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)