

Konfigurieren des AnyConnect VPN-Telefons mit Zertifikatsauthentifizierung auf einer ASA

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Telefonzertifikattypen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, in der veranschaulicht wird, wie die Adaptive Security Appliance (ASA)- und CallManager-Geräte so konfiguriert werden, dass Zertifikatsauthentifizierung für AnyConnect-Clients bereitgestellt wird, die auf Cisco IP-Telefonen ausgeführt werden. Nach Abschluss dieser Konfiguration können Cisco IP-Telefone VPN-Verbindungen zur ASA herstellen, die Zertifikate verwenden, um die Kommunikation zu sichern.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- AnyConnect Premium SSL-Lizenz
- AnyConnect für Cisco VPN-Telefonlizenz

Abhängig von der ASA-Version wird entweder "AnyConnect for Linksys Phone" für ASA Version 8.0.x oder "AnyConnect for Cisco VPN Phone" für ASA Version 8.2.x oder höher angezeigt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA - Version 8.0(4) oder höher
- IP-Telefonmodelle - 7942/7962/7945/7965/7975
- Telefone - 8961/9951/9971 mit Version 9.1(1)-Firmware
- Telefon - Version 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) oder höher
- Cisco Unified Communications Manager (CUCM) - Version 8.0.1.10000-4 oder höher

In diesem Konfigurationsbeispiel werden folgende Versionen verwendet:

- ASA - Version 9.1(1)
- CallManager - Version 8.5.1.1000-26

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.**

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Telefonzertifikattypen

Cisco verwendet die folgenden Zertifikatstypen auf Telefonen:

- MIC (Manufacturer Installed Certificate) - MICs sind in allen Cisco IP-Telefonen der Serien 7941, 7961 und neueren Modellen enthalten. MICs sind 2048-Bit-Schlüsselzertifikate, die von der Cisco Certificate Authority (CA) signiert werden. Wenn ein MIC vorhanden ist, muss kein LSC (Locally Significant Certificate) installiert 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.
- 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 bevorzugte Methode (im Gegensatz zur Verwendung von MICs), da nur Cisco IP-Telefone, die von einem Administrator manuell bereitgestellt werden, die CTL-Datei herunterladen und überprüfen dürfen. **Hinweis:** 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 so konfigurieren, dass sie MICs für die TLS-Authentifizierung (Transport Layer Security) oder für andere Zwecke verwenden, tun dies auf eigenes Risiko.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

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

Konfigurationen

In diesem Dokument werden die folgenden Konfigurationen beschrieben:

- ASA-Konfiguration
- CallManager-Konfiguration
- VPN-Konfiguration in CallManager
- Zertifikatinstallation auf IP-Telefonen

ASA-Konfiguration

Die Konfiguration der ASA ist fast identisch mit der Konfiguration eines AnyConnect-Client-Computers mit der ASA. Diese Einschränkungen gelten jedoch:

- Die Tunnelgruppe muss über eine Gruppen-URL verfügen. Diese URL wird im CM unter der VPN Gateway-URL konfiguriert.
- Die Gruppenrichtlinie darf keinen Split-Tunnel enthalten.

Bei dieser Konfiguration wird ein zuvor konfiguriertes und installiertes ASA-Zertifikat (selbstsigniertes oder Drittanbieter-Zertifikat) im SSL-Vertrauenspunkt (Secure Socket Layer) des ASA-Geräts verwendet. Weitere Informationen finden Sie in den folgenden Dokumenten:

- [Konfigurieren digitaler Zertifikate](#)
- [ASA 8.x Manuelles Installieren von Drittanbieter-Zertifikaten zur Verwendung mit WebVPN - Konfigurationsbeispiel](#)
- [ASA 8.x: Konfigurationsbeispiel für den VPN-Zugriff mit dem AnyConnect VPN-Client mithilfe eines selbstsignierten Zertifikats](#)

Die relevante Konfiguration der ASA ist:

```
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
```

CallManager-Konfiguration

Gehen Sie wie folgt vor, um das Zertifikat von der ASA zu exportieren und als Telefon-VPN-Trust-Zertifikat in CallManager zu importieren:

1. Registrieren Sie das generierte Zertifikat beim CUCM.
2. Überprüfen Sie das für SSL verwendete Zertifikat.

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

3. Exportieren Sie das Zertifikat.

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

Das PEM-kodierte Identitätszertifikat (Privacy Enhanced Mail) ist wie folgt:

```
-----BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9x0pR7BFpZd1yFyzwAPkoB11
-----END CERTIFICATE-----
```

4. Kopieren Sie den Text aus dem Terminal und speichern Sie ihn als .pem-Datei.
5. Melden Sie sich bei CallManager 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.

VPN-Konfiguration in CallManager

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

The screenshot shows the Cisco Unified CM Administration 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 shows 'Cisco Unified CM Administration' with system version '8.5.1.10000-26' and a license warning: 'System is operating on Demo Licenses. Please visit the License Report Page for more details.' The bottom status bar indicates 'Last Successful Logon: Feb 5, 2013 5:55:45 PM'.

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 der ASA definierte Gruppen-URL ein. Wählen Sie im Feld VPN Certificates in this Location (VPN-Zertifikate in diesem Speicherort) das Zertifikat aus, das zuvor in CallManager hochgeladen wurde, um es vom Truststore an diesen Speicherort zu verschieben.

The screenshot shows the 'VPN Gateway Configuration' page. At the top, there is a navigation menu with options like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below the menu, there are icons for Save, Delete, Copy, and Add New. The 'Status' section shows 'Status: Ready'. The 'VPN Gateway Information' section contains the following fields:

- VPN Gateway Name*: ASA_PhoneVPN
- VPN Gateway Description: (empty)
- VPN Gateway URL*: https://asa5520-c.cisco.com/SSL

 The 'VPN Gateway Certificates' section has two lists:

- 'VPN Certificates in your Truststore' with four entries, each showing a SUBJECT and ISSUER line.
- 'VPN Certificates in this Location*' with one entry: SUBJECT: unstructuredName=ASA5520-C.cisco.com, CN=ASA5520-C.cisco.com ISSUER: DC=com, DC=crtac, DC=...

 At the bottom, there are buttons for Save, Delete, Copy, and Add New.

4. Wählen Sie in der Menüleiste **Erweiterte Funktionen > VPN > VPN Group**.

The screenshot shows the same 'VPN Gateway Configuration' page, but with the 'Advanced Features' menu open. The 'VPN' option is selected, and the 'VPN Group' sub-option is highlighted. The configuration fields for the VPN Gateway are visible in the background:




- VPN Gateway Name*: ASA_PhoneVPN
- VPN Gateway Description: (empty)
- VPN Gateway URL*: https://asa5520-c.cisco.com/SSL

 The 'Status' section shows 'Update successful'.


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.

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*

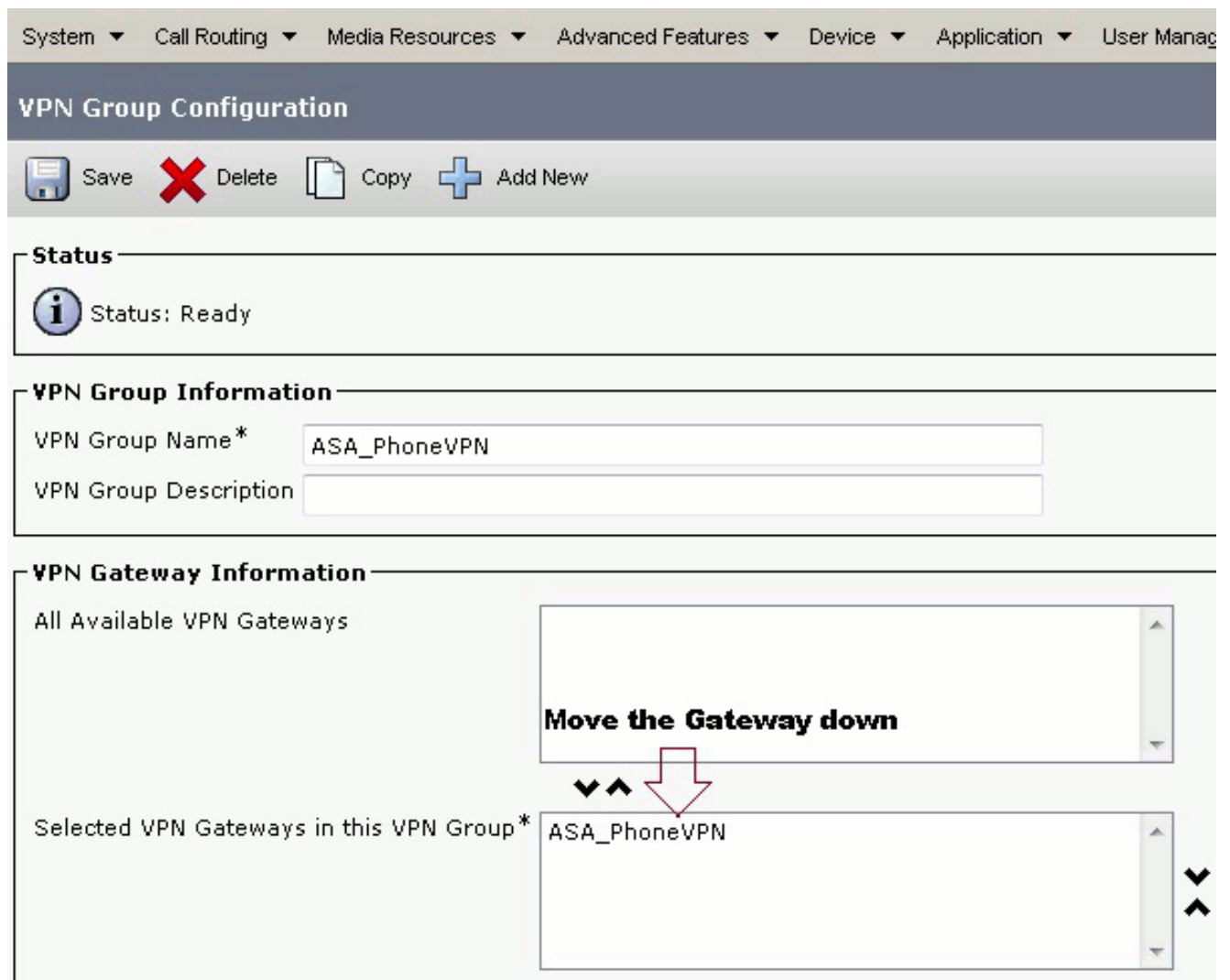
VPN Group Description

VPN Gateway Information

All Available VPN Gateways

Move the Gateway down




Selected VPN Gateways in this VPN Group*




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

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

VPN Group Configuration

Save  Delete  Copy  Add

Status

 Status: Ready

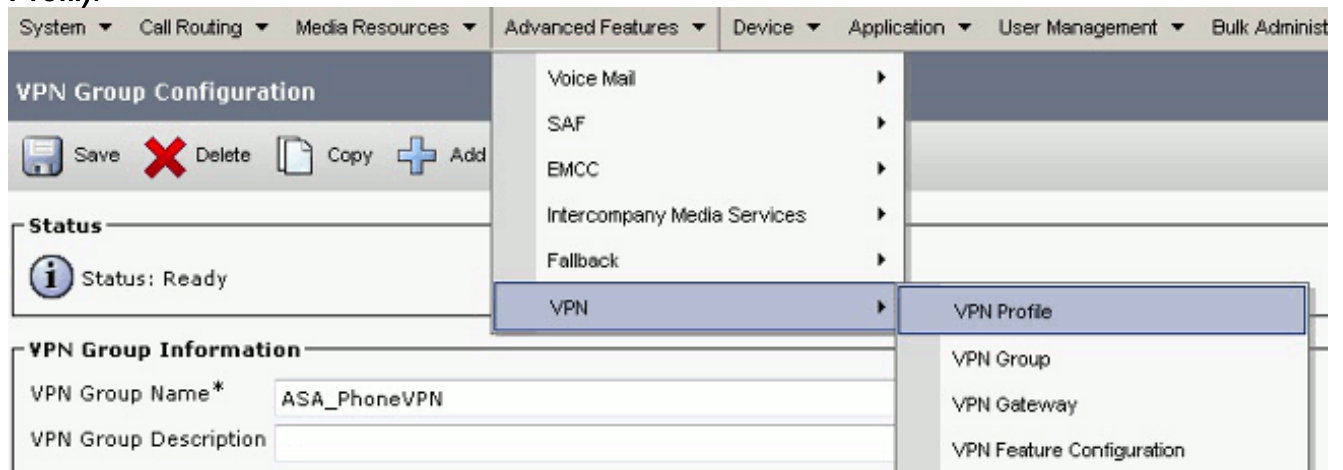
VPN Group Information

VPN Group Name*

VPN Group Description

Advanced Features ▾





- 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.

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

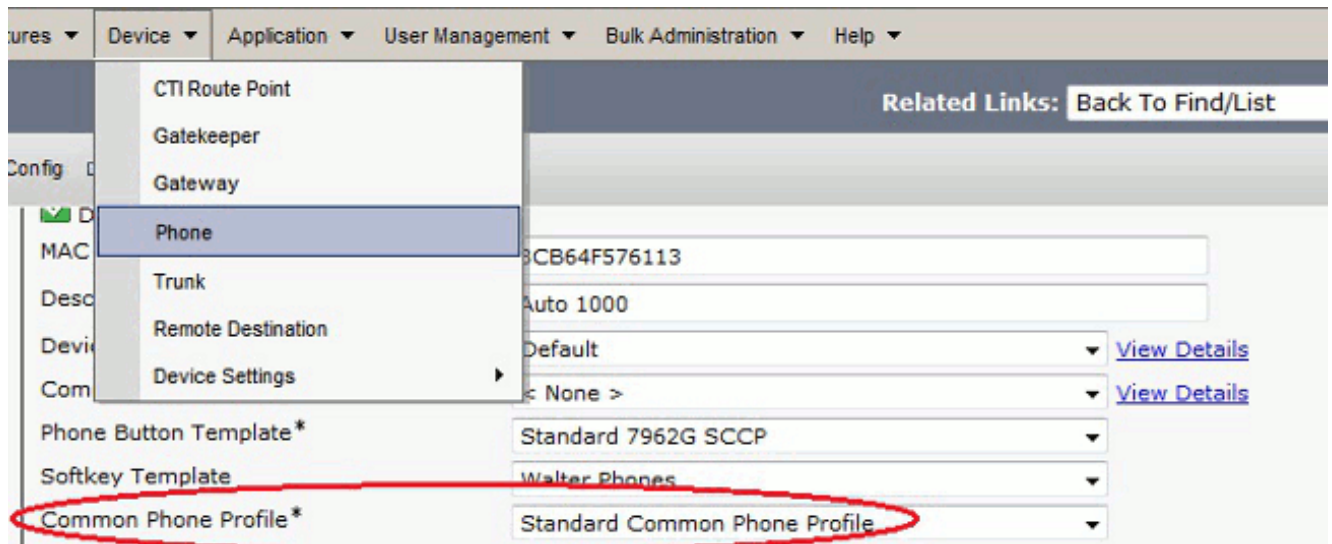
Automatische Netzwerkerkennung aktivieren: Wenn diese Funktion aktiviert ist, pingt das VPN-Telefon den TFTP-Server an, und wenn keine Antwort empfangen wird, initiiert es automatisch eine VPN-Verbindung. **Host-ID-Prüfung aktivieren:** Wenn diese Funktion aktiviert ist, vergleicht das VPN-Telefon den FQDN der VPN Gateway-URL mit dem CN/SAN des Zertifikats. Der Client kann keine Verbindung herstellen, wenn sie nicht übereinstimmen oder wenn ein Platzhalterzertifikat mit einem Sternchen (*) verwendet wird. **Kennwortpersistenz aktivieren:** Dadurch kann das VPN-Telefon den Benutzernamen und das Kennwort für den nächsten VPN-Versuch zwischenspeichern.

8. Klicken Sie im Fenster Konfiguration des allgemeinen Telefonprofils auf **Config anwenden**, um die neue VPN-Konfiguration anzuwenden. Sie können das "Standard Common Phone Profile" (Standardtelefonprofil) verwenden oder ein neues Profil erstellen.

The screenshot displays the Cisco Unified Communications Manager (CUCM) web interface. At the top, a navigation bar includes menus for 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Device' menu is expanded, showing options like 'CTI Route Point', 'Gatekeeper', 'Gateway', 'Phone', 'Trunk', and 'Remote Destination'. The 'Device Settings' option is selected, leading to a sub-menu with 'Device Defaults', 'Firmware Load Information', 'Default Device Profile', 'Device Profile', 'Phone Button Template', 'Softkey Template', 'Phone Services', 'SIP Profile', 'Common Device Configuration', and 'Common Phone Profile'. The 'Common Phone Profile' option is highlighted.

Below the navigation menu, the page title is 'Common Phone Profile Configuration'. A toolbar contains icons for 'Save', 'Delete', 'Copy', 'Reset', 'Apply Config', and 'Add New'. The 'VPN Information' section is visible, featuring two dropdown menus: 'VPN Group' and 'VPN Profile', both set to 'ASA_PhoneVPN'.

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



10. Registrieren Sie das Telefon erneut bei CallManager, um die neue Konfiguration herunterzuladen.





Konfiguration der Zertifikatsauthentifizierung

Führen Sie zum Konfigurieren der Zertifikatsauthentifizierung die folgenden Schritte in CallManager und der ASA aus:


1. Wählen Sie in der Menüleiste **Advanced Features > VPN > VPN Profile (Erweiterte Funktionen > VPN > VPN-Profil)**.
2. Bestätigen Sie, dass das Feld Client Authentication Method (Client-Authentifizierungsmethode) auf **Certificate** festgelegt ist.

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

- Melden Sie sich bei CallManager an. Wählen Sie in der Menüleiste **Unified OS Administration > Security > Certificate Management > Find** aus.
- Exportieren Sie die richtigen Zertifikate für die ausgewählte Zertifikatsauthentifizierungsmethode: MICs: Cisco_Manufacturing_CA - Authentifizierung von IP-Telefonen mit einer 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

LSCs: Cisco Certificate Authority Proxy Function (CAPF) - Authentifizierung von IP-Telefonen mit einem

LSC

Certificate Name	Certificate Type	.PEM File	
tomcat	certs	tomcat.pem	tomcat.der
psec	certs	lpsec.pem	lpsec.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	

- Suchen Sie das Zertifikat, entweder Cisco_Manufacturing_CA oder CAPF. Laden Sie die .pem-Datei herunter, und speichern Sie sie als TXT-Datei.
- Erstellen Sie einen neuen Trustpoint auf der ASA, und authentifizieren Sie den Trustpoint mit dem zuvor gespeicherten Zertifikat. Wenn Sie zur Eingabe eines Base-64-codierten CA-Zertifikats aufgefordert werden, wählen Sie den Text aus, und fügen Sie ihn zusammen mit den BEGIN- und END-Zeilen in die heruntergeladene .pem-Datei ein. Ein Beispiel wird angezeigt:

```
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
```

- Bestätigen Sie, dass für die Authentifizierung in der Tunnelgruppe die Zertifikatsauthentifizierung festgelegt ist.

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

Zertifikatinstallation auf IP-Telefonen

Die IP-Telefone können entweder mit MICs oder LSCs verwendet werden, aber der Konfigurationsprozess ist für jedes Zertifikat unterschiedlich.

MIC-Installation

Standardmäßig sind alle Telefone, die VPN unterstützen, mit MICs vorinstalliert. Die Telefone der Serien 7960 und 7940 verfügen über kein MIC und erfordern ein spezielles Installationsverfahren, damit sich das LSC sicher registrieren kann.

Hinweis: Cisco empfiehlt, MICs nur für die LSC-Installation zu verwenden. Cisco unterstützt LSCs zur Authentifizierung der TLS-Verbindung mit dem CUCM. Da MIC-Root-Zertifikate kompromittiert werden können, müssen Kunden, die Telefone so konfigurieren, dass sie MICs für die TLS-Authentifizierung oder für andere Zwecke verwenden, dies auf eigenes Risiko tun. Cisco übernimmt keine Haftung, wenn MICs kompromittiert werden.

LSC-Installation

- Aktivieren Sie den CAPF-Service auf CUCM.
- Wenn der CAPF-Dienst aktiviert ist, weisen Sie die Telefonanweisungen zu, um ein LSC in CUCM zu generieren. Melden Sie sich bei Cisco Unified CM Administration an, und wählen Sie **Gerät > Telefon aus**. Wählen Sie das von Ihnen konfigurierte Telefon aus.
- Stellen Sie im Abschnitt CAPF-Informationen (Certificate Authority Proxy Function) sicher,

dass alle Einstellungen korrekt sind und der Vorgang auf ein zukünftiges Datum festgelegt ist.

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. Wenn der Authentifizierungsmodus auf Null String oder Vorhandenes Zertifikat festgelegt ist, ist keine weitere Aktion erforderlich.
5. Wenn der Authentifizierungsmodus auf eine Zeichenfolge festgelegt ist, wählen Sie in der Telefonkonsole manuell **Einstellungen > Sicherheitskonfiguration > **# > LSC > Aktualisieren** aus.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

ASA-Verifizierung

```
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-Verifizierung

The screenshot shows the CUCM 'Find and List Phones' interface. At the top, there are navigation tabs for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below the navigation is a search bar and several action buttons: Add New, Select All, Clear All, Delete Selected, Reset Selected, and Apply Only to Selected. A status bar indicates '4 records found'. The main table displays the following data:

	Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
<input type="checkbox"/>	SEPXXXXXXXXXXXX	Auto 1001	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>	SEPXXXXXXXXXXXX	Auto 1000	Default	SCCP	Registered with: 192.168.100.1	10.10.10.2

A red arrow points from the text 'IP Phone registered with the CUCM using VPN address' to the IP address '10.10.10.2' in the table. A red circle highlights the 'Registered with: 192.168.100.1' and '10.10.10.2' cells.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Fehler

- Cisco Bug ID [CSCtf09529](#), Unterstützung für VPN-Funktion in CUCM für Telefone der Serien 8961, 9951 und 9971 hinzufügen
- Cisco Bug ID [CSCuc71462](#), IP-Telefon-VPN-Failover dauert 8 Minuten
- Cisco Bug ID [CSCtz42052](#), SSL VPN-Unterstützung für IP-Telefon für nicht standardmäßige Portnummern
- Cisco Bug ID [CSCth96551](#), Nicht alle ASCII-Zeichen werden bei der Anmeldung des Telefon-VPN-Benutzers + des Kennworts unterstützt.
- Cisco Bug ID [CSCuj71475](#), manueller TFTP-Eintrag für IP-Telefon-VPN erforderlich
- Cisco Bug-ID [CSCum10683](#), IP-Telefone, die nicht protokolliert werden, verpasste, getätigte oder empfangene Anrufe

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)