VPN-Telefone konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung der VPN-Telefonfunktion von Cisco IP-Telefonen und Cisco Unified Communications Manager.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM)
- Cisco Adaptive Security Appliance (ASA)
- AnyConnect Virtual Private Network (VPN)
- Cisco IP-Telefone

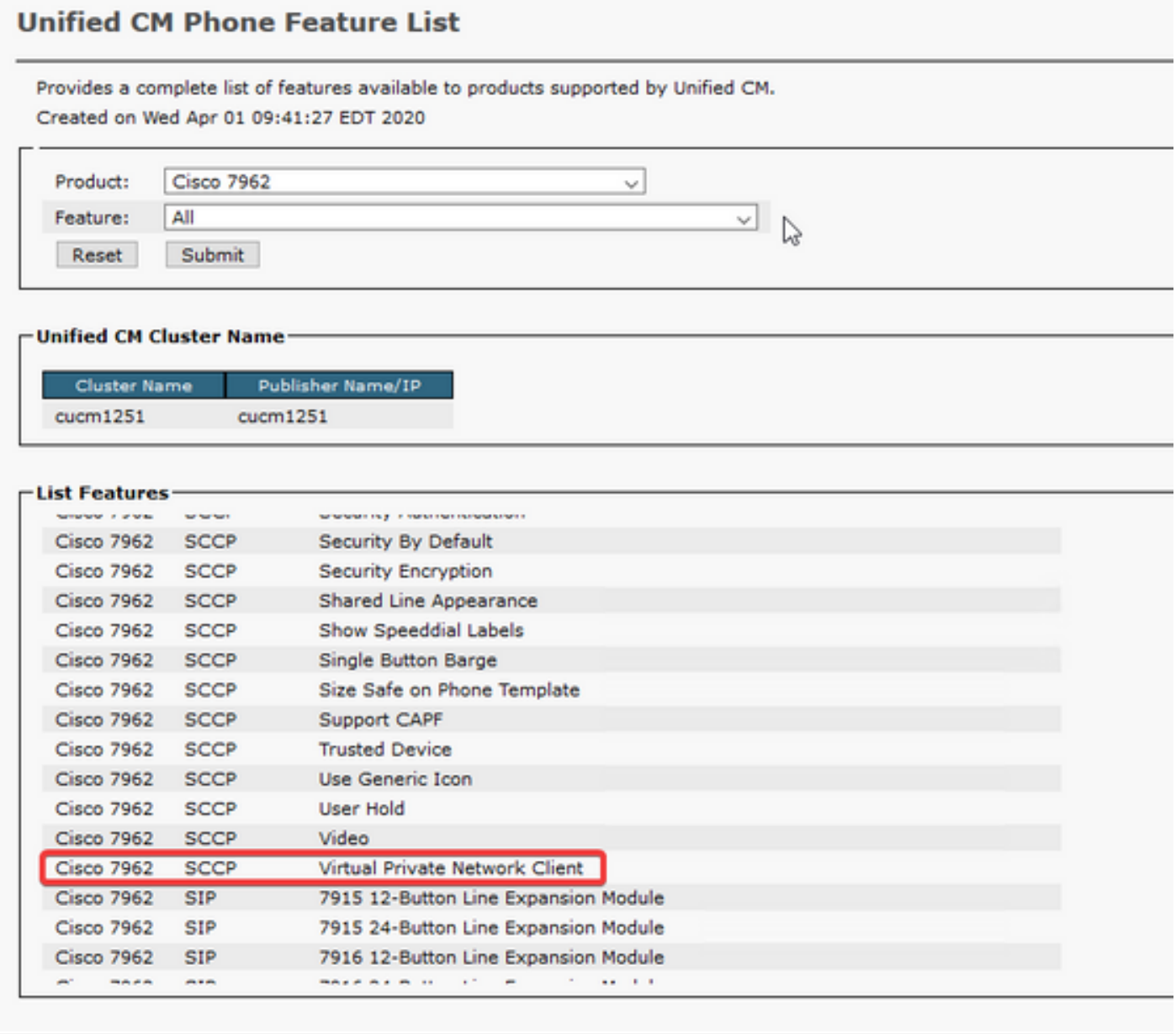
Verwendete Komponenten

- 8861 14-0-1-0101-145
- ASAv 9.12(2)9
- CUCM 11.5.1.21900-40

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Testumgebung in diesem Artikel umfasst eine Version 8861, ASAv und CUCM 11.5.1. Es gibt jedoch viele verschiedene Varianten dieser Produkte, die Sie verwenden können. Sie müssen die Telefonfunktionsliste auf CUCM überprüfen, um sicherzustellen, dass Ihr Telefonmodell die VPN-Funktion unterstützt. Um die Funktionsliste des Telefons zu verwenden, rufen Sie Ihren CUCM-Publisher in Ihrem Browser auf, und navigieren Sie zur **Funktionsliste von Cisco Unified Reporting > Unified CM Phone**. Erstellen Sie einen neuen Bericht, und wählen Sie dann im Dropdown-Menü Ihr Telefonmodell aus. Als Nächstes müssen Sie den Abschnitt List Features (Funktionen auflisten) für Virtual Private Network Client durchsuchen, wie im Bild gezeigt:



Konfigurieren

Für VPN-Telefone müssen Sie die richtige Konfiguration auf Ihrer ASA und Ihrem CUCM haben. Sie können mit jedem Produkt zuerst beginnen, aber dieses Dokument behandelt zuerst die ASA-Konfiguration.

ASA-Konfiguration

Schritt 1: Überprüfen Sie, ob die ASA lizenziert ist, um AnyConnect für VPN-Telefone zu unterstützen. Der Befehl **show version** auf der ASA kann verwendet werden, um zu überprüfen, ob **AnyConnect für Cisco VPN Phone** aktiviert ist, wie in diesem Ausschnitt gezeigt:

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

Wenn diese Funktion nicht aktiviert ist, müssen Sie mit dem Lizenzteam zusammenarbeiten, um die entsprechende Lizenz zu erhalten. Nachdem Sie bestätigt haben, dass Ihre ASA VPN-Telefone unterstützt, können Sie mit der Konfiguration beginnen.

> **Anmerkung:** Alle unterstrichenen Elemente im Konfigurationsabschnitt sind konfigurierbare Namen, die geändert werden können. Da auf die meisten dieser Namen an anderer Stelle in der Konfiguration verwiesen wird, ist es wichtig, sich die Namen zu merken, die Sie in diesen Abschnitten verwenden (Gruppenrichtlinie, Tunnelgruppe usw.), da Sie sie später benötigen.

Schritt 2: Erstellen Sie einen IP-Adresspool für VPN-Clients. Dies ähnelt einem DHCP-Pool, wenn ein IP-Telefon eine Verbindung zur ASA herstellt, erhält es von diesem Pool eine IP-Adresse. Der Pool kann mit dem folgenden Befehl auf der ASA erstellt werden:

ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254, Maske 255.255.255.0

Wenn Sie eine andere Netzwerk- oder Subnetzmaske bevorzugen, kann dies ebenfalls geändert werden. Nachdem der Pool erstellt wurde, müssen Sie eine Gruppenrichtlinie konfigurieren (eine Reihe von Parametern für die Verbindung zwischen ASA und IP-Telefonen):

Gruppenrichtlinie VPN-Phone-Policy intern

Gruppenrichtlinien-VPN-Telefon-Richtlinienattribute

Tunnelverbindung

vpn-tunnel-protocol ssl-client

Schritt 3: Sie müssen AnyConnect aktivieren, wenn es noch nicht aktiviert ist. Dazu müssen Sie den Namen der externen Schnittstelle kennen. In der Regel ist diese Schnittstelle **extern** benannt (wie im Ausschnitt gezeigt), sie ist jedoch konfigurierbar. Stellen Sie daher sicher, dass Sie die richtige Schnittstelle haben. Führen Sie **show ip aus**, um die Liste der Schnittstellen anzuzeigen:

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

In dieser Umgebung wird die externe Schnittstelle **außerhalb** benannt, sodass diese Befehle AnyConnect für diese Schnittstelle aktivieren.

Webpn
Aktivieren von außen
anyconnect-fähig

Schritt 4: Konfigurieren Sie eine neue Tunnelgruppe, um die zuvor erstellte Gruppenrichtlinie auf alle Clients anzuwenden, die eine Verbindung mit einer bestimmten URL herstellen. Beachten Sie den Verweis auf die Namen des IP-Adresspools und der Gruppenrichtlinie, die Sie zuvor in der dritten und vierten Zeile des Ausschnitts erstellt haben. Wenn Sie die Namen des IP-Adresspools oder der Gruppenrichtlinie geändert haben, müssen Sie die falschen Werte durch die geänderten Namen ersetzen:

Tunnel-Group vpn-phone-group Typ Remote-Zugriff
tunnel-group vpn-phone-group - allgemeine Attribute
address-pool vpn-phone-pool
default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attribute
Authentifizierungszertifikat
group-url https://asav.sckiewer.lab/phone aktivieren

Sie können eine IP-Adresse anstelle eines Namens für die **Gruppen-URL** verwenden. Dies geschieht in der Regel, wenn die Telefone keinen Zugriff auf einen DNS-Server haben, der den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der ASA auflösen kann. Außerdem wird in diesem Beispiel die zertifikatsbasierte Authentifizierung verwendet. Sie haben die Möglichkeit, auch Benutzername/Kennwort-Authentifizierung zu verwenden. Es gibt jedoch auch weitere Anforderungen an die ASA, die nicht in diesem Dokument enthalten sind.

In diesem Beispiel verfügt der DNS-Server über den A-Eintrag **asav.sckiewer.lab - 172.16.1.250**, und in der **show ip**-Ausgabe wird angezeigt, dass 172.16.1.250 auf der **externen** Schnittstelle konfiguriert ist. Die Konfiguration lautet also:

crypto ca trustpoint asa-identity-cert

Einschreibung selbst

subject-name CN=asav.sckiewer.lab

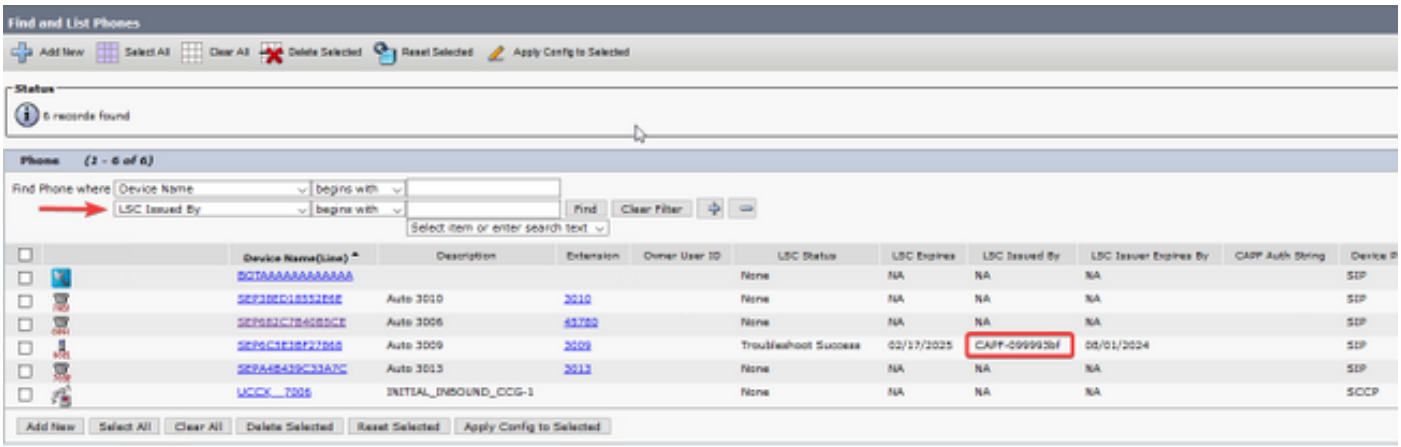
crypto kann sich als "asa-identity-cert" registrieren

ssl trust-point asa-identity-cert extern

Einige wichtige Punkte:

1. Es wurde ein neuer Vertrauenspunkt mit dem Namen asa-identity-cert erstellt, auf den ein Betreffname angewendet wurde. Dadurch wird das von diesem Vertrauenspunkt generierte Zertifikat zur Verwendung des angegebenen Betreffnamens verwendet.
2. Als Nächstes ermöglicht der Befehl "crypto ca enroll asa-identity-cert" der ASA, ein selbstsigniertes Zertifikat zu generieren und es an diesem Vertrauenspunkt zu speichern.
3. Schließlich stellt die ASA das Zertifikat im Vertrauenspunkt jedem Gerät zur Verfügung, das eine Verbindung zur externen Schnittstelle herstellt.

Schritt 5: Erstellen Sie die erforderlichen Trustpoints, damit die ASA dem Zertifikat des IP-Telefons vertrauen kann. Zunächst müssen Sie feststellen, ob Ihre IP-Telefone das MIC (Manufacturer Installed Certificate) oder das LSC (Locally Significant Certificate) verwenden. Standardmäßig verwenden alle Telefone ihre MIC für sichere Verbindungen, es sei denn, auf ihnen ist ein LSC installiert. In CUCM 11.5.1 und höher können Sie eine Suche unter **Unified CM Administration > Device > Phone** ausführen, um festzustellen, ob LSCs installiert sind, während ältere Versionen von CUCM eine physische Überprüfung der Sicherheitseinstellungen auf jedem Telefon erfordern. Beachten Sie in CUCM 11.5.1, dass Sie in **LSC Issued By** einen Filter hinzufügen (oder den Standardfilter ändern) müssen. Geräte mit **NA** in der Spalte **"LSC Issued By" (Ausgestellt von** LSC) verwenden das MIC, da auf ihnen kein LSC installiert ist.

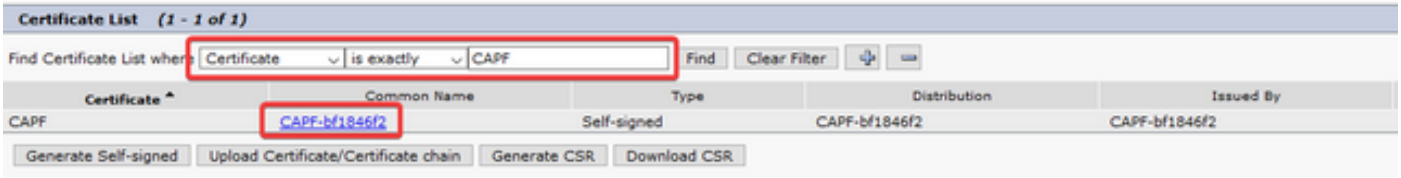


Wenn Ihr Telefon wie das im Bild hervorgehobene aussieht, müssen Sie das CAPF-Zertifikat des CUCM Publisher auf die ASA hochladen, damit die ASA das Telefonzertifikat für die sichere Verbindung validieren kann. Wenn Sie Geräte ohne installierte LSC verwenden möchten, müssen Sie die Cisco Manufacturing Certificates auf die ASA hochladen. Diese Zertifikate finden Sie im CUCM Publisher unter **Cisco Unified OS Administration > Security > Certificate Management**:

Anmerkung: Sie sehen, dass einige dieser Zertifikate in mehreren Trusted-Stores (CallManager-trust und CAPF-trust) vorhanden sind. Es spielt keine Rolle, von welchem vertrauenswürdigen Speicher Sie die Zertifikate herunterladen, solange Sie sicherstellen,

dass Sie die Zertifikate mit diesen genauen Namen auswählen.

- Cisco_Root_CA_2048 < MIC SHA-1 Root
- Cisco_Manufacturing_CA < MIC SHA-1 Intermediate
- Cisco_Root_CA_M2 < MIC SHA-256 Root
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 Intermediate
- CAPF vom CUCM Publisher < LSC



Bei älteren Telefonmodellen wie den Serien 79xx und 99xx wird die Zertifikatskette SHA-1 verwendet, während neuere Telefonmodelle wie die Serie 88xx die Zertifikatskette SHA-256 verwenden. Die Zertifikatskette, die von Ihrem Telefon bzw. Ihren Telefonen verwendet wird, muss auf die ASA hochgeladen werden.

Wenn Sie über die erforderlichen Zertifikate verfügen, können Sie die Vertrauenspunkte wie folgt erstellen:

crypto ca trustpoint cert1

Anmeldeterminal

crypto ca authentifizieren cert1

Der erste Befehl erstellt einen Vertrauenspunkt mit dem Namen **cert1**, und der Befehl **crypto ca authentication** ermöglicht es Ihnen, das Base64-codierte Zertifikat in die CLI einzufügen. Sie können diese Befehle so oft ausführen, wie Sie müssen, um die entsprechenden Vertrauenspunkte auf der ASA zu erhalten. Achten Sie jedoch darauf, für jedes Zertifikat einen neuen Trustpoint-Namen zu verwenden.

Schritt 6: Sichern Sie sich eine Kopie des ASA-Identitätszertifikats, indem Sie den folgenden Befehl ausstellen:

crypto kann als Identitätszertifikat asa-identity-cert exportieren

Dadurch wird das Identitätszertifikat für den Vertrauenspunkt mit der Bezeichnung "a-identity-cert" exportiert. Passen Sie den Namen so an, dass er mit dem in Schritt 4 erstellten Trustpoint übereinstimmt.

Nachfolgend finden Sie die vollständige Laborkonfiguration für die ASA:

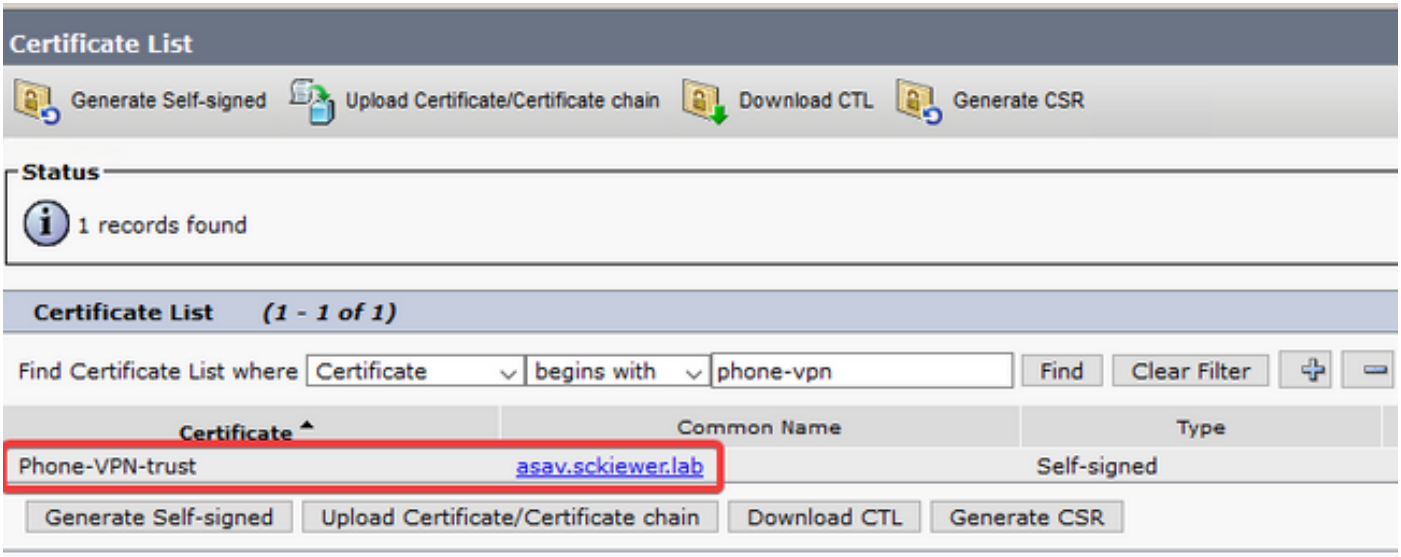
```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
     split-tunnel-policy tunnelall
     vpn-tunnel-protocol ssl-client

webvpn
     enable outside
```

```
     anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
     address-pool vpn-phone-pool
     default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
     authentication certificate
     group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

An diesem Punkt ist die ASA-Konfiguration abgeschlossen, und Sie können mit der CUCM-Konfiguration fortfahren. Sie benötigen eine Kopie des gerade gesammelten ASA-Zertifikats und der im Tunnelgruppenabschnitt konfigurierten URL.

CUCM-Konfiguration

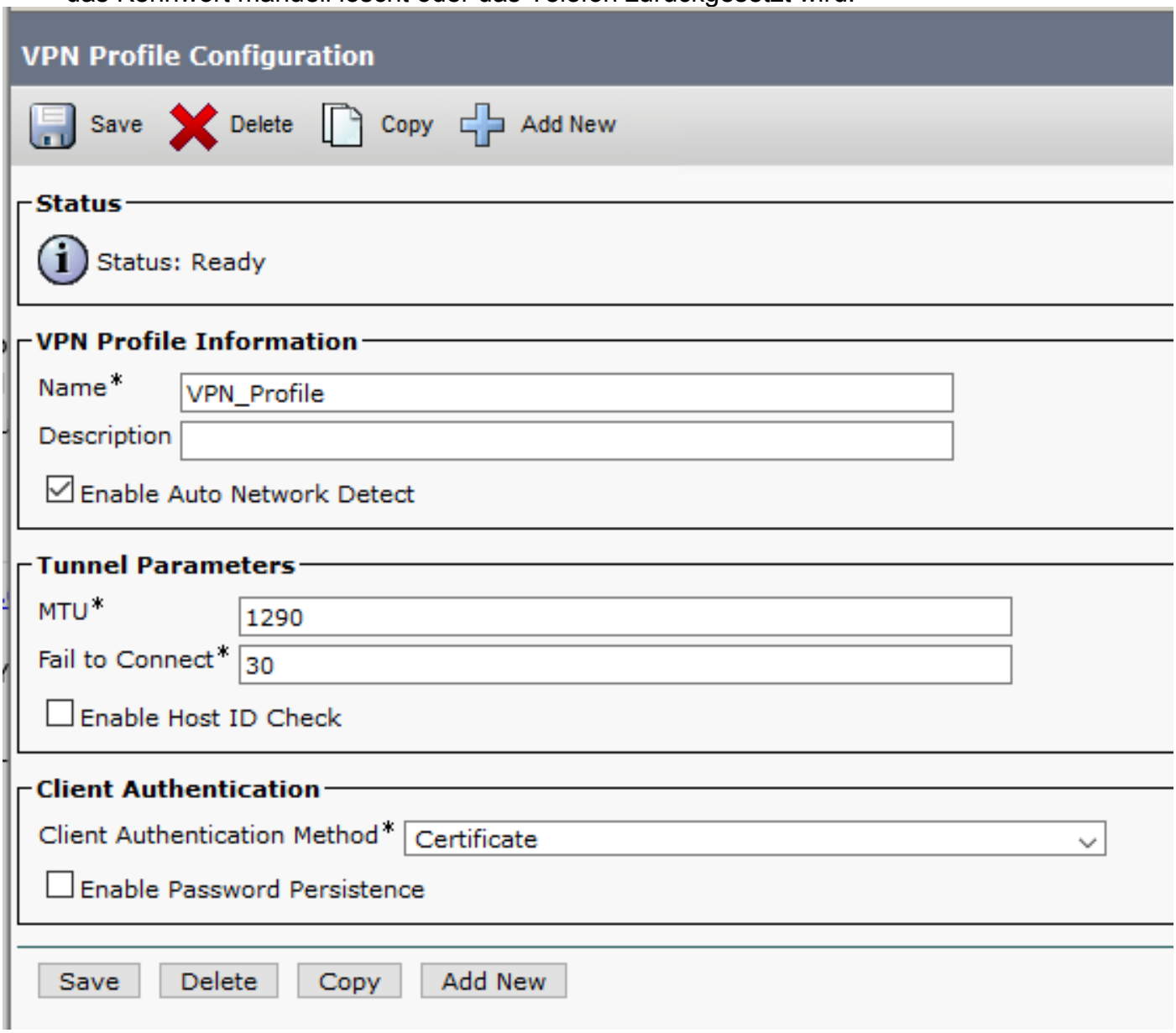
Schritt 1: Navigieren Sie auf dem CUCM zu **Cisco Unified OS Administration > Security > Certificate Management**, und laden Sie das ASA-Zertifikat als **phone-vpn-trust** hoch.



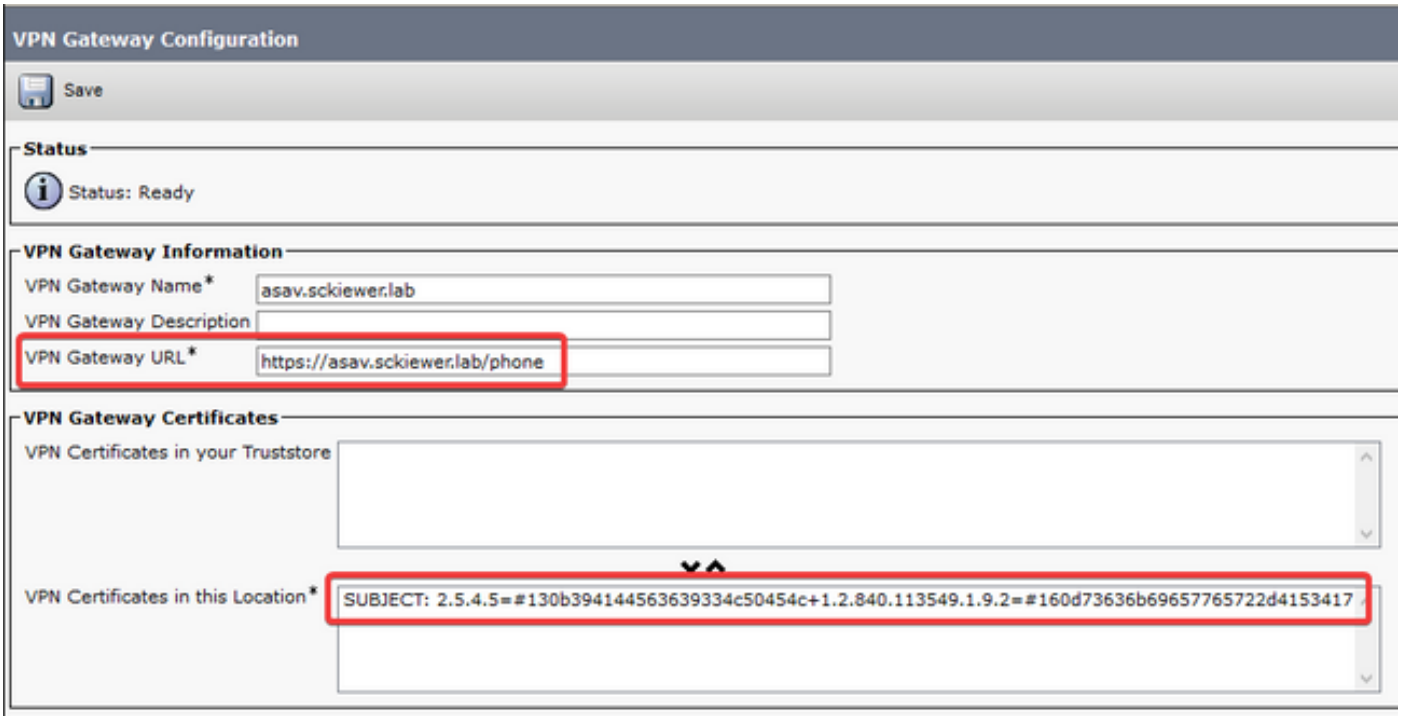
Schritt 2: Navigieren Sie anschließend zu **Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile**, und erstellen Sie ein neues Profil. In diesem Abschnitt gibt es weder Recht noch Unrecht. Es ist nur wichtig, den Zweck jeder Einstellung zu verstehen.

1. **Auto Network Detect (Automatische Netzwerkerkennung aktivieren)**: Wenn diese Funktion aktiviert ist, pingt das Telefon beim Einschalten den TFTP-Server an. Wenn eine Antwort auf diesen Ping-Befehl empfangen wird, wird VPN nicht aktiviert. Wenn das Telefon keine Antwort auf diesen Ping empfängt, aktiviert es VPN. Wenn diese Einstellung aktiviert ist, kann VPN nicht manuell aktiviert werden.
2. **Host-ID-Prüfung**: Wenn diese Funktion aktiviert ist, prüft das Telefon die VPN-URL aus seiner Konfigurationsdatei (https://asav.sckiewer.lab/phone wird in diesem Dokument verwendet) und stellt sicher, dass der Hostname oder der FQDN mit dem Common Name (CN) oder einem SAN-Eintrag im von der ASA präsentierten Zertifikat übereinstimmt.
3. **Authentication Method** - steuert, welcher Authentifizierungstyp für die Verbindung mit der ASA verwendet wird. Im Konfigurationsbeispiel dieses Dokuments wird die zertifikatsbasierte Authentifizierung verwendet.

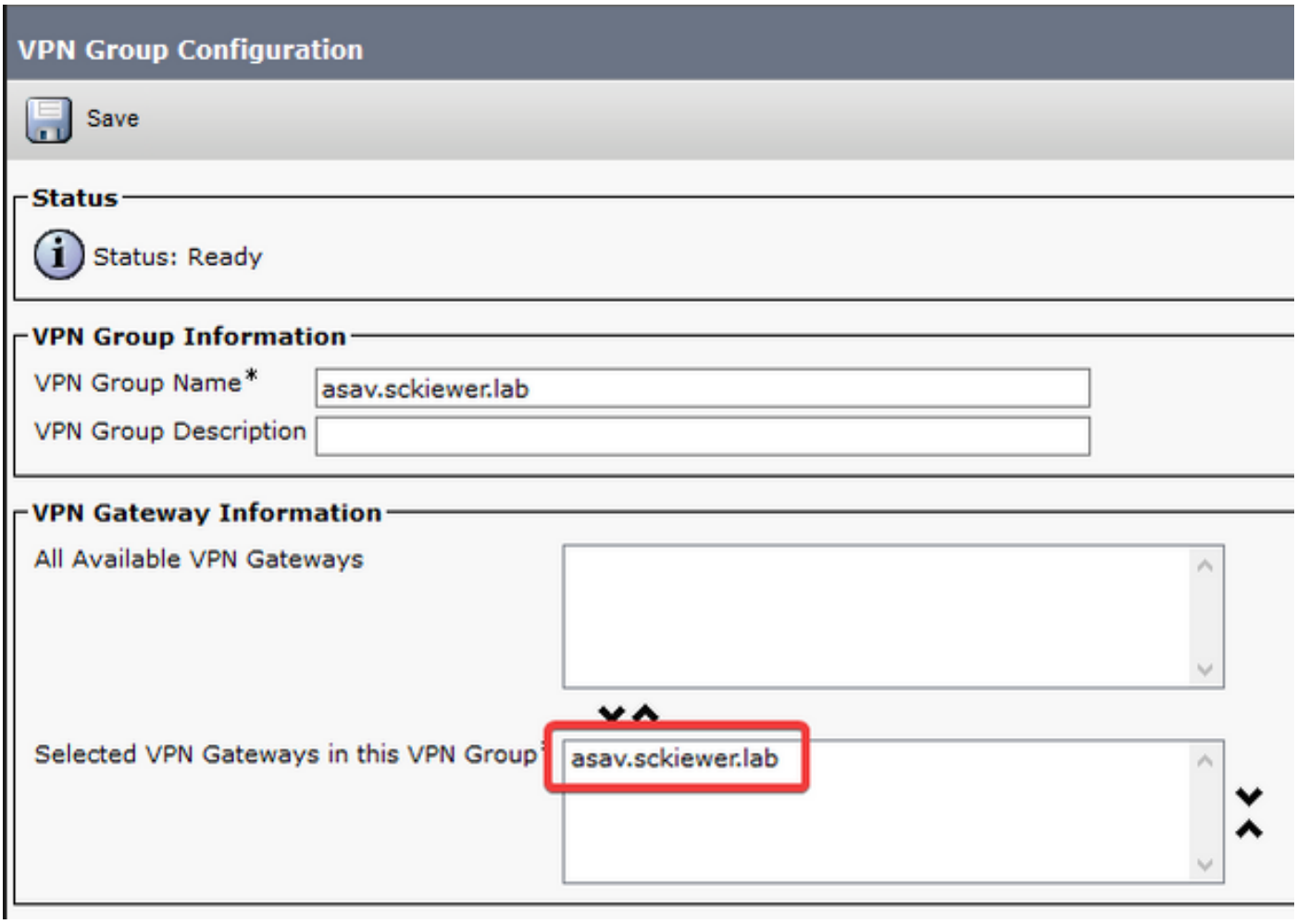
4. **Kennwortpersistenz**: Wenn diese Option aktiviert ist, wird das Kennwort des Clients auf dem Telefon gespeichert, bis ein fehlgeschlagener Anmeldeversuch durchgeführt wird, der Client das Kennwort manuell löscht oder das Telefon zurückgesetzt wird.



Schritt 3: Navigieren Sie anschließend zu **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**. Sie müssen sicherstellen, dass Ihre VPN Gateway-URL der ASA-Konfiguration entspricht und dass Sie das Zertifikat vom oberen Feld zum unteren Feld verschieben, wie in der Abbildung gezeigt:

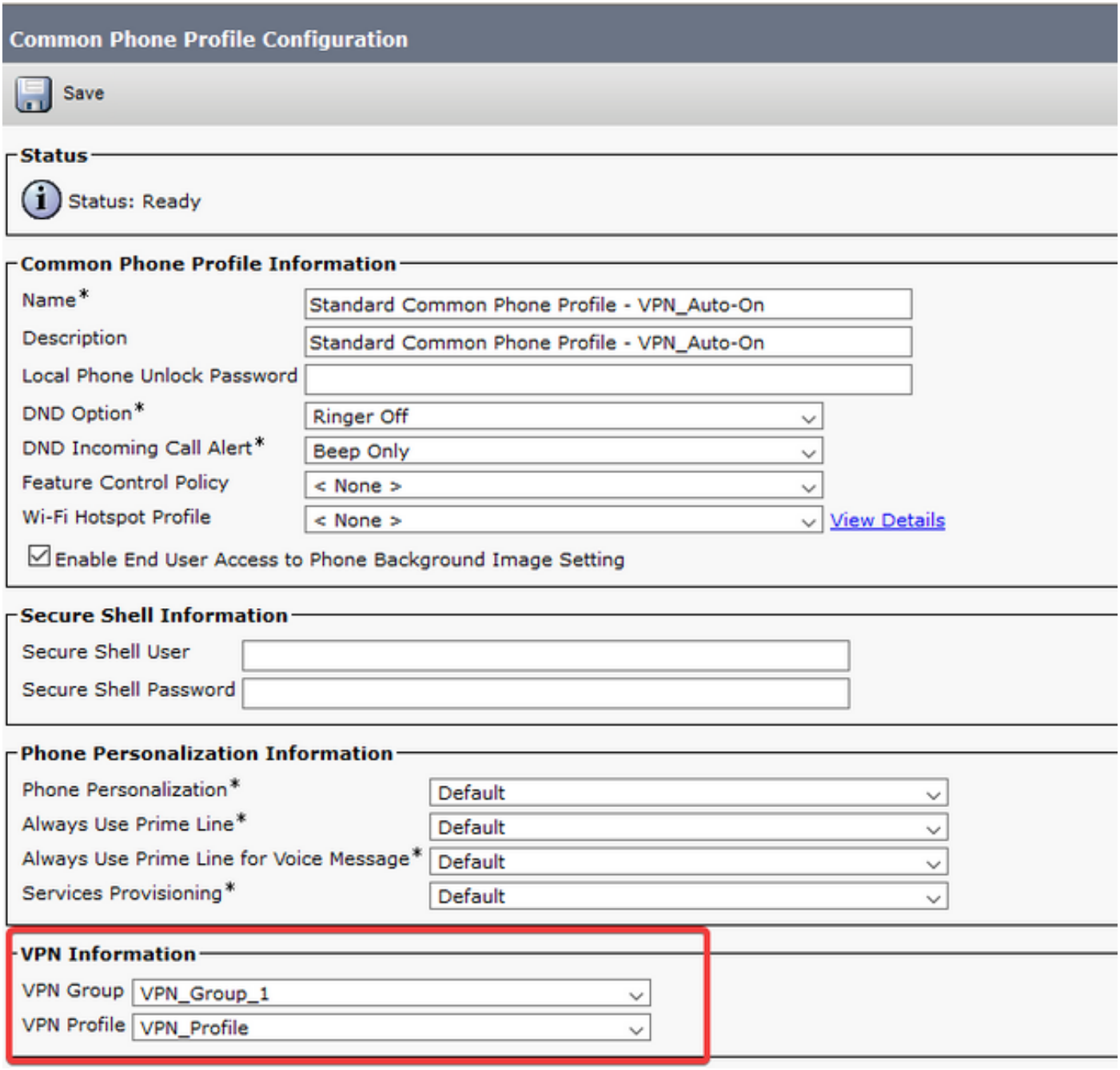


Schritt 4: Sobald diese gespeichert sind, müssen Sie zu **Cisco Unified CM Administration > Advanced Features > VPN > VPN Group** navigieren und das erstellte Gateway in das Feld "Selected VPN Gateways in this VPN Group" (Ausgewählte VPN-Gateways in dieser VPN-Gruppe) verschieben:



Schritt 5: Nachdem die VPN-Einstellungen konfiguriert wurden, navigieren Sie zu **Cisco Unified CM Administration > Device Settings > Common Phone Profile**. Hier müssen Sie das Profil

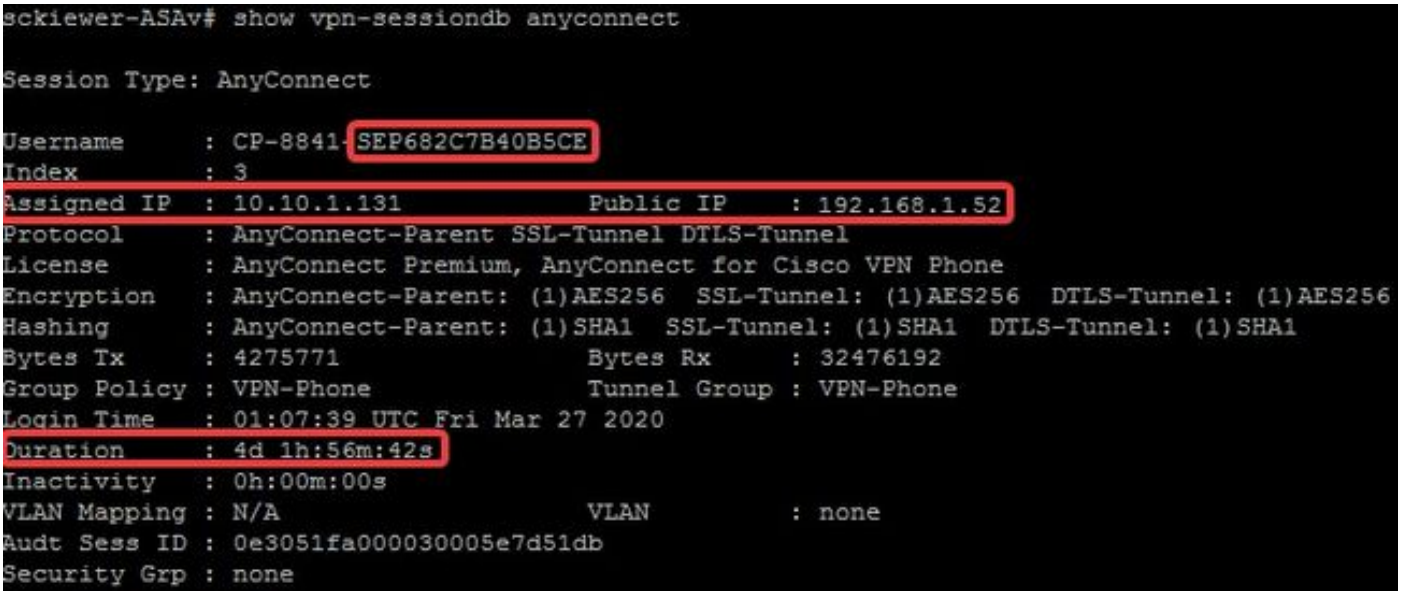
kopieren, das von Ihrem gewünschten VPN-Telefon verwendet wird, umbenennen und Ihre VPN-Gruppe und Ihr VPN-Profil auswählen. Speichern Sie anschließend das neue Profil:



Schritt 6: Schließlich müssen Sie dieses neue Profil auf Ihr Telefon anwenden und dann das Telefon zurücksetzen, während es sich im internen Netzwerk befindet. Dadurch kann das Telefon die gesamte neue Konfiguration wie den ASA-Zertifikat-Hash und die VPN-URL erhalten.

> **Anmerkung:** Bevor Sie das Telefon testen, müssen Sie sicherstellen, dass für die Telefone ein alternativer TFTP-Server konfiguriert ist. Da die ASA den Telefonen keine Option 150 bereitstellt, muss die TFTP-IP-Adresse auf den Telefonen manuell konfiguriert werden.

Schritt 7: Testen Sie das VPN-Telefon, und stellen Sie sicher, dass es erfolgreich eine Verbindung zur ASA herstellen und sich registrieren kann. Sie können überprüfen, ob der Tunnel auf der ASA verfügbar ist. Zeigen Sie **vpn-sessiondb anyconnect an**:



Fehlerbehebung

Zu erfassende Daten

Zur Fehlerbehebung bei einem VPN-Telefon werden folgende Daten empfohlen:

- ASA-Debugger: gepufferte ProtokollierungProtokollierung von Debug-Tracedebug crypto ca transaktionen 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- Telefonkonsolenprotokolle (oder ein PRT, wenn das Telefon es unterstützt - weitere Informationen hier)

Nachdem Sie das Problem bei aktiviertem Debuggen reproduziert haben, können Sie die Ausgabe mit diesem Befehl anzeigen, da die Debugausgabe immer 711001 enthält:

show log | i 711001

Häufige Probleme

> **Anmerkung:** Für die Zwecke dieses Abschnitts werden Protokollausschnitte von einem Telefon mit der Nummer 8861 gesendet, da dies eine der gebräuchlichsten Telefonserien ist, die als VPN-Telefon bereitgestellt werden. Beachten Sie, dass andere Modelle unterschiedliche Meldungen in die Protokolle schreiben können.

Aktualisieren des selbst signierten ASA-Identitätszertifikats

Bevor das ASA-Identitätszertifikat abläuft, muss ein neues Zertifikat erstellt und an die Telefone weitergeleitet werden. Gehen Sie folgendermaßen vor, um dies ohne Auswirkungen auf die VPN-Telefone zu tun:

Schritt 1: Erstellen Sie einen neuen Vertrauenspunkt für das neue Identitätszertifikat:

crypto ca trustpoint asa-identity-cert-2

Einschreibung selbst

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

Schritt 2: Zu diesem Zeitpunkt hätten Sie ein neues Identitätszertifikat für die ASA, das jedoch noch nicht für eine Schnittstelle verwendet wird. Sie müssen dieses neue Zertifikat exportieren und in CUCM hochladen:

crypto ca export asa-identity-cert-2 identity-certificate

Schritt 3: Wenn Sie das neue Identitätszertifikat haben, laden Sie es als phone-VPN-trust in einen Ihrer CUCM-Knoten unter **Cisco Unified OS Administration > Security > Certificate Management > Upload hoch**.

> **Anmerkung:** Das aktuelle "phone-VPN trust"-Zertifikat ist nur auf dem CUCM-Knoten vorhanden, auf den es ursprünglich hochgeladen wurde (es wird nicht automatisch an andere Knoten wie einige Zertifikate weitergeleitet). Wenn Ihre CUCM-Version von CSCuo58506 betroffen ist, müssen Sie das neue ASA-Zertifikat auf einen anderen Knoten hochladen.

Schritt 4: Sobald das neue Zertifikat auf einen der Knoten im Cluster hochgeladen wurde, navigieren Sie zu **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway** auf dem CUCM Publisher.

Schritt 5: Wählen Sie das entsprechende Gateway aus.

Schritt 6: Wählen Sie im oberen Feld das Zertifikat aus (dies ist das Zertifikat, das Sie gerade hochgeladen haben), und klicken Sie auf den Abwärtspfeil, um es nach unten zu verschieben (damit TFTP dieses Zertifikat in die Konfigurationsdateien Ihres VPN-Telefons einfügen kann), und wählen Sie Speichern aus.

Schritt 7: Setzen Sie anschließend alle VPN-Telefone zurück. Zu diesem Zeitpunkt des Prozesses präsentiert die ASA noch das alte Zertifikat, sodass die Telefone eine Verbindung herstellen können. Sie erwerben jedoch eine neue Konfigurationsdatei, die sowohl das neue Zertifikat als auch das alte Zertifikat enthält.

Schritt 8: Jetzt können Sie das neue Zertifikat auf die ASA anwenden. Dazu benötigen Sie den Namen des neuen Vertrauenspunkts und den Namen der externen Schnittstelle. Führen Sie dann diesen Befehl mit den folgenden Informationen aus:

ssl trust-point asa-identity-cert-2 extern

> **Anmerkung:** Sie können zur webvpn-URL in Ihrem Browser navigieren, um zu überprüfen, ob die ASA das neue Zertifikat vorlegt. Da diese Adresse für externe Telefone öffentlich erreichbar sein muss, kann Ihr PC sie auch erreichen. Sie können dann das Zertifikat überprüfen, das die ASA Ihrem Browser vorlegt, und bestätigen, dass es sich um das neue Zertifikat handelt.

Schritt 9: Wenn die ASA für die Verwendung des neuen Zertifikats konfiguriert ist, setzen Sie ein

Testtelefon zurück, und überprüfen Sie, ob es eine Verbindung zur ASA herstellen und sich registrieren kann. Wenn das Telefon erfolgreich registriert wird, können Sie alle Telefone zurücksetzen und überprüfen, ob sie eine Verbindung zur ASA herstellen und sich registrieren können. Dies ist der empfohlene Prozess, da die Telefone, die mit der ASA verbunden sind, nach dem Ändern des Zertifikats weiterhin verbunden sind. Wenn Sie die Zertifikatsaktualisierung zuerst an einem Telefon testen, verringern Sie das Risiko, dass ein Konfigurationsproblem eine große Anzahl von Telefonen betrifft. Wenn das erste VPN-Telefon keine Verbindung zur ASA herstellen kann, können Sie Protokolle vom Telefon und/oder der ASA sammeln, um eine Fehlerbehebung durchzuführen, während die anderen Telefone verbunden bleiben.

Schritt 10: Nachdem Sie überprüft haben, ob die Telefone eine Verbindung herstellen und sich für das neue Zertifikat registrieren können, kann das alte Zertifikat aus dem CUCM entfernt werden.

ASA wählt Elliptic Curve (EC)-Chiffre

ASAs unterstützen die Elliptic Curve (EC)-Verschlüsselung ab Version 9.4(x). Daher ist es üblich, dass bereits funktionierende VPN-Telefone nach einem ASA-Upgrade auf Version 9.4(x) oder höher ausfallen. Dies liegt daran, dass die ASA jetzt beim TLS-Handshake mit neueren Telefonmodellen eine EC-Chiffre auswählt. In der Regel ist der Schnittstelle, mit der das Telefon verbunden ist, ein RSA-Zertifikat zugeordnet, da die vorherige ASA-Version EC nicht unterstützt. Da die ASA jetzt einen EC-Chip ausgewählt hat, kann für die Verbindung kein RSA-Zertifikat verwendet werden. Daher generiert und sendet sie ein temporäres, selbstsigniertes Zertifikat, das sie mit dem EC-Algorithmus und nicht mit RSA erstellt. Da dieses temporäre Zertifikat vom Telefon nicht erkannt wird, schlägt die Verbindung fehl. Sie können überprüfen, dass dies in den 88xx-Telefonprotokollen ziemlich einfach ist.

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

Die Telefonprotokolle zeigen, dass die ASA einen EC-Chiffre für diese Verbindung ausgewählt hat, da die "neue Chiffre"-Leitung EC-Chiffren enthält, die zum Ausfall der Verbindung führen.

In einem Szenario, in dem AES ausgewählt wurde, wird Folgendes angezeigt:

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-
SHA:AES128-SHA
```

Weitere Informationen hierzu finden Sie hier, CSCuu02848.

Die Lösung dafür wäre, die EC-Chiffre auf der ASA für die TLS-Version zu deaktivieren, die Ihr Telefon verwendet. Weitere Informationen darüber, welche TLS-Version von den einzelnen Telefonmodellen unterstützt wird, finden Sie hier:

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

	Phone Models			
Version	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
** With 12.5 firmware

https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf

Sobald Sie wissen, welche TLS-Versionen für Ihre Umgebung relevant sind, können Sie diese Befehle auf der ASA ausführen, um EC-Chiffren für diese Versionen zu deaktivieren:

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
```

Beachten Sie, dass IP-Telefone standardmäßig DTLS (Datagram Transport Layer Security) verwenden. Daher müssen Sie die Verschlüsselungsanweisung für DTLS und die entsprechende TLS-Version für Ihre Telefone ausführen. Außerdem ist es wichtig zu verstehen, dass es sich bei diesen Änderungen um globale Änderungen auf der ASA handelt, sodass sie verhindern, dass EC-Chiffren von einem anderen AnyConnect-Client verhandelt werden, der diese TLS-Versionen verwendet.

DTLS-Verbindungsfehler

In einigen Fällen können VPN-Telefone keine Verbindung zur ASA mit DTLS herstellen. Wenn das Telefon versucht, DTLS zu verwenden, aber es fehlschlägt, versucht es weiterhin, DTLS zu wiederholen, und zwar erfolglos, da es weiß, dass DTLS aktiviert ist. Dies wird in den 88xx-Telefonprotokollen angezeigt:

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000
status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal
parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1,
```

```
error 1
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

Dies kann durch dasselbe Problem verursacht werden, das auch im Abschnitt ASA Selecting Elliptic Curve (EC) Cipher erwähnt wurde. Daher müssen Sie sicherstellen, dass die EC-Chiffren für DTLS deaktiviert sind. Darüber hinaus können Sie DTLS vollständig deaktivieren, wodurch die Verwendung von TLS durch VPN-Telefone erzwungen wird. Dies wäre nicht ideal, da der gesamte Datenverkehr TCP anstelle von UDP nutzen würde, was einen gewissen Overhead bedeutet. In einigen Szenarien ist dies jedoch ein guter Test, da zumindest bestätigt wird, dass die meisten Konfigurationen in Ordnung sind, und das Problem sich auf DTLS bezieht. Wenn Sie dies testen möchten, empfiehlt es sich, dies auf Gruppenrichtlinienebene zu tun, da Administratoren in der Regel eine eindeutige Gruppenrichtlinie für VPN-Telefone verwenden. Auf diese Weise können wir Änderungen testen, ohne andere Clients zu beeinträchtigen.

Gruppenrichtlinien-VPN-Telefon-Richtlinienattribute
Webpn
anyconnect ssl dtl none

Ein weiteres häufiges Konfigurationsproblem, das eine erfolgreiche DTLS-Verbindung verhindern kann, besteht darin, dass das Telefon keine TLS- und DTLS-Verbindung mit demselben Chip herstellen kann. Beispiel für Protokollauszug:

```
%%%%% TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

%%%%% DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

%%%%% DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

Sie können die TLS-Chiffren in der ersten Zeile des Ausschnitts sehen. Die sicherste Option, die von beiden Seiten unterstützt wird, ist ausgewählt (die Protokolle zeigen die Auswahl nicht an, Sie können jedoch davon ausgehen, dass es sich bei mindestens AES-256 aus dem Protokollausschnitt handelt). Sie können auch sehen, dass AES128 die einzige angebotene DTLS-Verschlüsselung ist. Da die ausgewählte TLS-Verschlüsselung für DTLS nicht verfügbar ist, schlägt die Verbindung fehl. Das Problem in diesem Szenario besteht darin, sicherzustellen, dass die ASA-Konfiguration die Verwendung derselben Chiffren für TLS und DTLS ermöglicht.

Telefon kann nach Zertifikatupdate keine Verbindung zur ASA herstellen

Es ist sehr wichtig, dass Sie das neue ASA-Identitätszertifikat als phone-vpn-trust auf CUCM

hochladen, damit die Telefone den Hash für dieses neue Zertifikat abrufen können. Wenn dieser Vorgang nicht befolgt wird, wird dem Telefon nach der Aktualisierung und beim nächsten Versuch, eine Verbindung mit der ASA herzustellen, ein Zertifikat angezeigt, dem es nicht vertraut, sodass die Verbindung fehlschlägt. Dies kann einige Tage oder Wochen nach dem Update des ASA-Zertifikats auftreten, da die Telefone nicht getrennt werden, wenn sich das Zertifikat ändert. Solange die ASA weiterhin Keepalives vom Telefon empfängt, bleibt der VPN-Tunnel bestehen. Wenn Sie also bestätigt haben, dass das ASA-Zertifikat aktualisiert wurde, das neue Zertifikat jedoch nicht zuerst für den CUCM bereitgestellt wurde, haben Sie zwei Möglichkeiten:

1. Wenn das alte ASA-Identitätszertifikat noch gültig ist, setzen Sie die ASA wieder in das alte Zertifikat zurück und befolgen Sie anschließend den in diesem Dokument beschriebenen Prozess zur Aktualisierung des Zertifikats. Wenn Sie bereits ein neues Zertifikat generiert haben, können Sie den Abschnitt zur Zertifikatgenerierung überspringen.
2. Wenn das alte ASA-Identitätszertifikat abgelaufen ist, müssen Sie das neue ASA-Zertifikat in CUCM hochladen und die Telefone wieder in das interne Netzwerk bringen, um die aktualisierte Konfigurationsdatei mit dem neuen Zertifikats-Hash zu erhalten.

Telefon kann ASA-URL nicht über DNS auflösen

In einigen Szenarien konfiguriert der Administrator die VPN-URL mit einem Hostnamen anstatt einer IP-Adresse. Anschließend muss das Telefon über einen DNS-Server verfügen, um den Namen in eine IP-Adresse auflösen zu können. Im Ausschnitt sehen Sie, dass das Telefon versucht, den Namen mit seinen zwei DNS-Servern, 192.168.1.1 und 192.168.1.2, aufzulösen, aber keine Antwort erhält. Nach 30 Sekunden druckt das Telefon ein 'DnsLookupErr:'

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

Dies weist in der Regel auf einen der folgenden Aspekte hin:

1. Das Telefon verfügt über einen ungültigen DNS-Server.
2. Das Telefon hat keinen DNS-Server über DHCP erhalten oder wurde nicht manuell konfiguriert.

Zur Behebung dieses Problems gibt es zwei Optionen:

1. Überprüfen Sie die Konfiguration des Telefons, um sicherzustellen, dass ein DNS-Server vom DHCP-Server empfangen wird, wenn dieser extern ist, und/oder überprüfen Sie, ob der DNS-Server des Telefons den in der ASA-Konfiguration verwendeten Namen auflösen kann.
2. Ändern Sie die URL in der ASA-Konfiguration und in CUCM in eine IP-Adresse, sodass kein DNS erforderlich ist.

VPN wird vom Telefon nicht aktiviert

Wie bereits zuvor in diesem Dokument erwähnt, veranlasst die automatische Netzwerkerkennung das Telefon, einen Ping an den TFTP-Server zu senden und nach einer Antwort zu suchen. Wenn sich das Telefon im internen Netzwerk befindet, ist der TFTP-Server ohne VPN erreichbar. Wenn das Telefon also Antworten auf die Pings empfängt, aktiviert es kein VPN. Wenn sich das Telefon NICHT im internen Netzwerk befindet, schlagen die Pings fehl, sodass das Telefon VPN aktiviert und eine Verbindung zur ASA herstellt. Beachten Sie, dass das Heimnetzwerk eines Clients wahrscheinlich nicht so konfiguriert wird, dass dem Telefon die Option 150 via DHCP zur Verfügung gestellt wird. Die ASA kann auch keine Option 150 bereitstellen. Daher ist "Alternate TFTP" für VPN-Telefone erforderlich.

In den Protokollen sollten Sie einige Punkte überprüfen:

1. Ping das Telefon an den CUCM-TFTP-Server-IP?
2. Erhält das Telefon eine Antwort auf die Pings?
3. Ermöglicht das Telefon VPN, nachdem es keine Antwort auf die Pings erhält?

Es ist wichtig, diese Posten in dieser Reihenfolge anzuzeigen. In einem Szenario, in dem das Telefon die falsche IP pingt und eine Antwort empfängt, wäre es sinnlos, Debug auf der ASA zu aktivieren, da das Telefon VPN nicht aktiviert. Validieren Sie diese drei Dinge in dieser Reihenfolge, um unnötige Protokollanalysen zu vermeiden. Dies wird in den 88xx-Telefonprotokollen angezeigt, wenn der Ping-Befehl fehlschlägt und anschließend das VPN aktiviert ist:

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

Telefonregister können Anrufsverlauf nicht anzeigen

Überprüfen Sie, ob auf dem Telefon Alternate TFTP aktiviert ist und die richtige TFTP-IP konfiguriert ist. Für VPN-Telefone ist ein alternatives TFTP erforderlich, da die ASA die Option 150 nicht bereitstellen kann.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme