Configurazione e risoluzione dei problemi dei telefoni VPN

Sommario

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi alla funzionalità VPN Phone di Cisco IP Phone e Cisco Unified Communications Manager.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

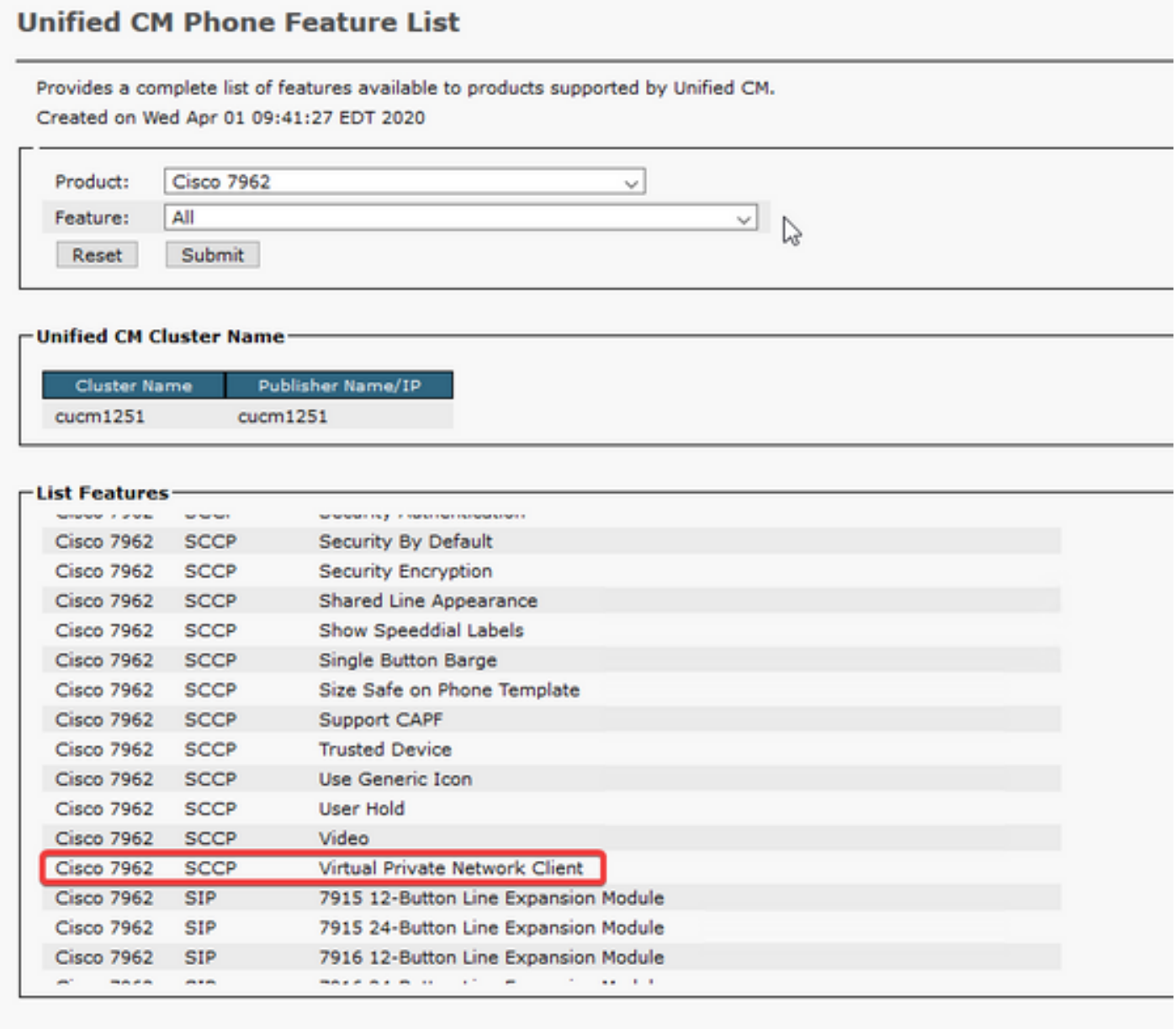
Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'ambiente di test in questo articolo include 8861, ASAv e CUCM 11.5.1, ma è possibile utilizzare diverse varianti di questi prodotti. È necessario controllare l'elenco funzionalità telefono in CUCM per assicurarsi che il modello di telefono in uso supporti la funzionalità VPN. Per utilizzare l'elenco delle funzionalità del telefono, accedere all'editore CUCM nel browser e selezionare **Cisco Unified Reporting > Unified CM Phone Feature List** (Cisco Unified Reporting > Elenco funzionalità telefoniche di CCM unificato). Generare un nuovo report, quindi selezionare il modello di telefono nell'elenco a discesa. Successivamente, è necessario cercare Virtual Private Network Client nella sezione List Features, come mostrato nell'immagine:



Configurazione

I telefoni VPN richiedono la configurazione corretta sulle appliance ASA e CUCM. È possibile iniziare con uno dei due prodotti, ma questo documento descrive prima la configurazione dell'ASA.

Configurazione ASA

Passaggio 1. Verificare che l'appliance ASA sia concessa in licenza per supportare AnyConnect per telefoni VPN. Il comando **show version** sull'appliance ASA può essere usato per verificare che **Anyconnect per Cisco VPN Phone** sia abilitato, come mostrato in questo frammento:

```
[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
```

Se questa funzione non è abilitata, è necessario rivolgersi al team delle licenze per ottenere la licenza appropriata. Dopo aver confermato che l'appliance ASA supporta i telefoni VPN, è possibile iniziare la configurazione.

> **Nota:** Tutti gli elementi sottolineati nella sezione di configurazione sono nomi configurabili che possono essere modificati. Poiché la maggior parte di questi nomi sono menzionati in un'altra posizione della configurazione, è importante ricordare i nomi utilizzati in queste sezioni (Criteri di gruppo, Gruppo tunnel e così via), poiché saranno necessari in seguito.

Passaggio 2. Creare un pool di indirizzi IP per i client VPN. Questa procedura è simile a quella di un pool DHCP, in quanto quando un telefono IP si connette all'appliance ASA riceve un indirizzo IP da questo pool. Il pool può essere creato con questo comando sull'appliance ASA:

ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 maschera 255.255.255.0

Inoltre, se si preferisce una rete o una subnet mask diversa, è possibile modificare anche questa impostazione. Una volta creato il pool, è necessario configurare un criterio di gruppo (un set di parametri per la connessione tra l'ASA e i telefoni IP):

criteri di gruppo vpn-phone-policy internal

attributi criteri gruppo vpn-phone-policy

split-tunnel-policy tunnel

vpn-tunnel-protocol ssl-client

Passaggio 3. Se AnyConnect non è già abilitato, è necessario abilitarlo. A tale scopo, è necessario conoscere il nome dell'interfaccia esterna. In genere, il nome di questa interfaccia è **esterno** (come mostrato nello snippet), ma è configurabile, quindi accertarsi di avere l'interfaccia corretta. Eseguire **show ip** per visualizzare l'elenco delle interfacce:

```
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 questo ambiente, il nome dell'interfaccia esterna è **outside**, quindi questi comandi abilitano AnyConnect su quell'interfaccia.

webvpn
abilita esterno
anyconnect enable

Passaggio 4. Configurare un nuovo gruppo di tunnel per applicare i Criteri di gruppo creati in precedenza a tutti i client che si connettono a un URL specifico. Si noti il riferimento ai nomi del pool di indirizzi IP e dei criteri di gruppo creati in precedenza nella terza e quarta riga dello snippet. Se sono stati modificati i nomi del pool di indirizzi IP o dei criteri di gruppo, è necessario utilizzare la funzione di sostituzione dei valori non corretti con i nomi modificati:

accesso remoto di tipo tunnel group vpn-phone-group
tunnel-group vpn-phone-group general-attributes
pool di indirizzi vpn phone pool
default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attributes
certificato di autenticazione
group-url https://asav.sckiewer.lab/phone enable

Èpossibile utilizzare un indirizzo IP anziché un nome per l'**URL del gruppo**. Questa operazione viene in genere eseguita se i telefoni non hanno accesso a un server DNS in grado di risolvere il nome di dominio completo (FQDN) dell'appliance ASA. In questo esempio viene inoltre utilizzata l'autenticazione basata su certificati. È possibile usare anche l'autenticazione di nome utente/password, ma l'appliance ASA ha altri requisiti che non rientrano nell'ambito di questo documento.

Nell'esempio, il server DNS ha il record A **asav.sckiewer.lab - 172.16.1.250** e l'output **show ip** mostra che la versione 172.16.1.250 è configurata sull'interfaccia **esterna**. La configurazione sarebbe:

crypto ca trustpoint asa-identity-cert

iscrizione self

nome soggetto CN=asav.sckiewer.lab

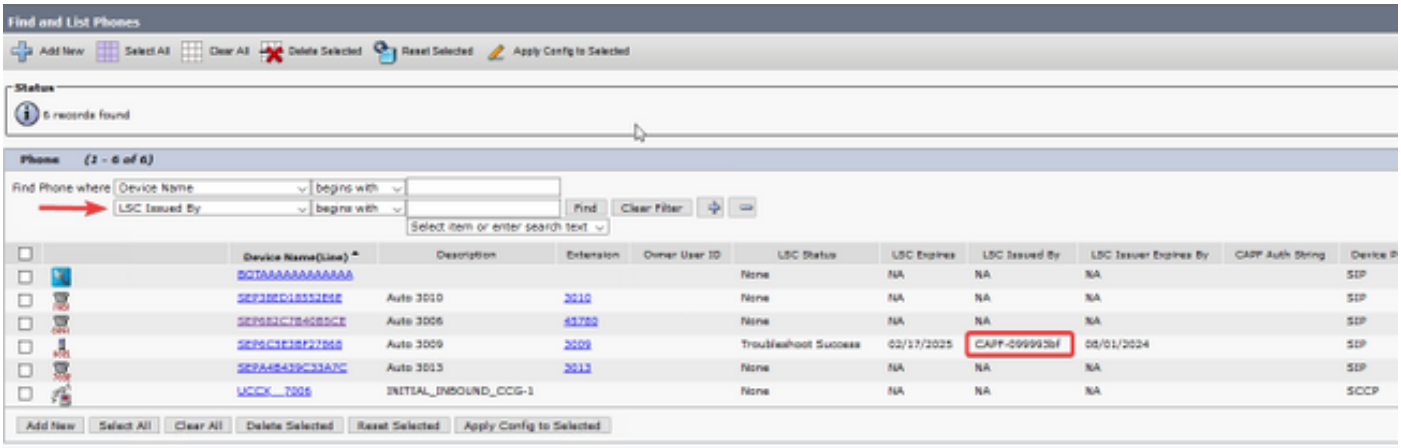
crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert esterno

Ecco alcune cose da notare:

1. Èstato creato un nuovo trust point denominato asa-identity-cert a cui è stato applicato un nome soggetto. In questo modo il certificato generato da questo trust point utilizzerà il nome soggetto specificato
2. Successivamente, il comando 'crypto ca enroll asa-identity-cert' consente all'ASA di generare un certificato autofirmato e di salvarlo in quel trust point
3. Infine, l'ASA presenta il certificato nel trust point a tutti i dispositivi che si connettono all'interfaccia esterna

Passaggio 5. Creare i trust point necessari per consentire all'ASA di considerare attendibile il certificato del telefono IP. Innanzitutto, è necessario determinare se i telefoni IP utilizzano il certificato del produttore installato (MIC) o il certificato di importanza locale (LSC). Per impostazione predefinita, tutti i telefoni utilizzano il microfono per le connessioni protette, a meno che non sia installata una scheda LSC. In CUCM 11.5.1 e versioni successive, è possibile eseguire una ricerca in **Unified CM Administration > Device > Phone (Amministrazione CM unificata)** per verificare se sono installati gli LCS, mentre le versioni precedenti di CUCM richiedono il controllo fisico delle impostazioni di protezione di ciascun telefono. In CUCM 11.5.1, si noti che è necessario aggiungere un filtro (o modificare il filtro predefinito) a **LSC emesso da**. I dispositivi con **NA** nella colonna **LSC emesso da** utilizzano il MIC in quanto non dispongono di un LSC installato.

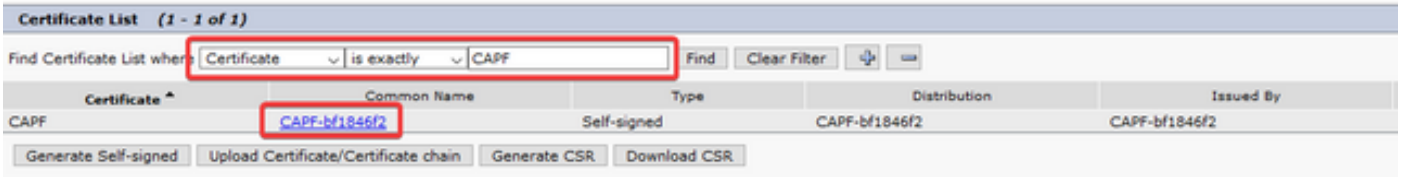


Se il telefono è simile a quello evidenziato nell'immagine, è necessario caricare il certificato CAPF di CUCM Publisher sull'appliance ASA per convalidare il certificato del telefono per la connessione sicura. Se si desidera utilizzare dispositivi senza LSC installato, è necessario caricare i Cisco Manufacturing Certificates sull'appliance ASA. Questi certificati sono disponibili in CUCM Publisher in **Cisco Unified OS Administration > Security > Certificate Management**:

> **Nota:** Alcuni di questi certificati si trovano in più archivi attendibili (CallManager-trust e CAPF-trust). Non importa da quale archivio attendibile si scaricano i certificati, purché si sia certi di selezionare quelli con questi nomi esatti.

- Cisco_Root_CA_2048 < radice MIC SHA-1

- Cisco_Manufacturing_CA < MIC SHA-1 Intermedio
- Cisco_Root_CA_M2 < radice MIC SHA-256
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 intermedio
- CAPF da CUCM Publisher < LSC



Per quanto riguarda il microfono, i modelli di telefoni meno recenti, come la serie 79xx e 99xx, utilizzano la catena di certificati SHA-1, mentre i modelli di telefoni più recenti, come la serie 88xx, utilizzano la catena di certificati SHA-256. Caricare la catena di certificati usata dai telefoni nell'appliance ASA.

Dopo aver ottenuto i certificati richiesti, è possibile creare uno o più punti di trust con:

crypto ca trustpoint cert1

terminale di registrazione

crypto ca authentication cert1

Il primo comando crea un trust point denominato **cert1**, mentre il comando **crypto ca authentication** consente di incollare il certificato codificato base64 nella CLI. È possibile eseguire questi comandi tutte le volte che è necessario per ottenere i trust point appropriati sull'appliance ASA, ma accertarsi di usare un nuovo nome di trust per ogni certificato.

Passaggio 6. Acquisire una copia del certificato di identità ASA usando questo comando:

crypto ca export asa-identity-cert identity-certificate

Esporta il certificato di identità per il trust point denominato asa-identity-cert. Assicurarsi di modificare il nome in modo che corrisponda al trust point creato nel passaggio 4.

Di seguito è riportata la configurazione lab completa per l'appliance 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
```

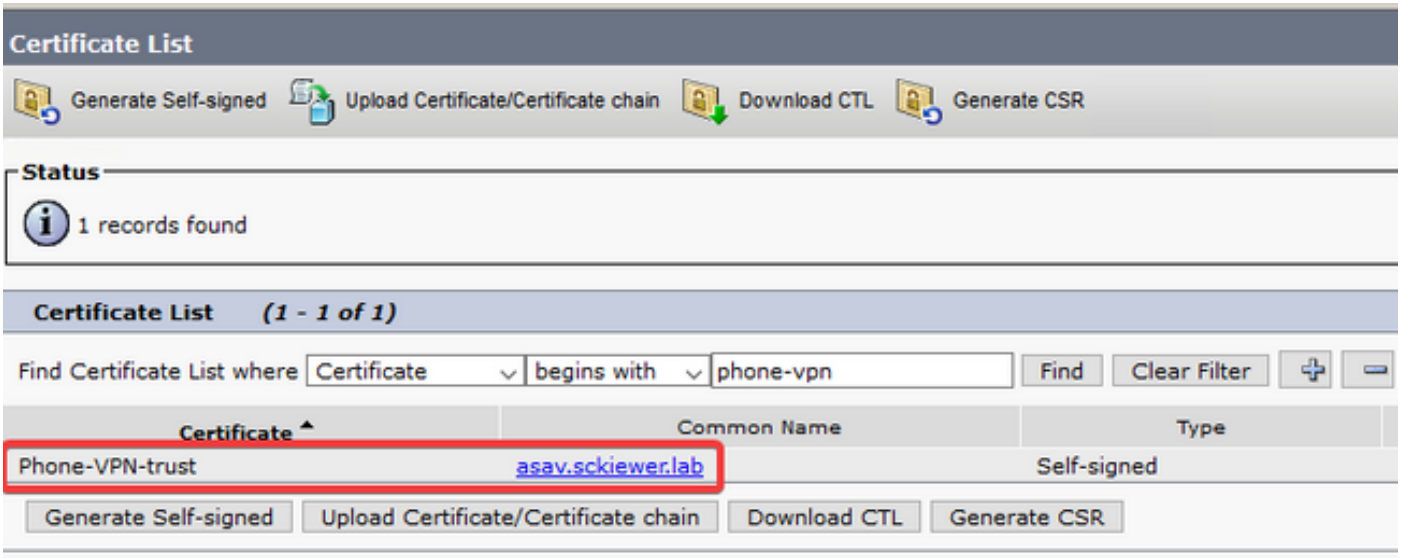
```
    group-url https://asav.sckiewer.lab/phone enable

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

A questo punto, la configurazione dell'ASA è completa e si può procedere con la configurazione di CUCM. È necessario disporre di una copia del certificato ASA appena raccolto e dell'URL configurato nella sezione tunnel-group.

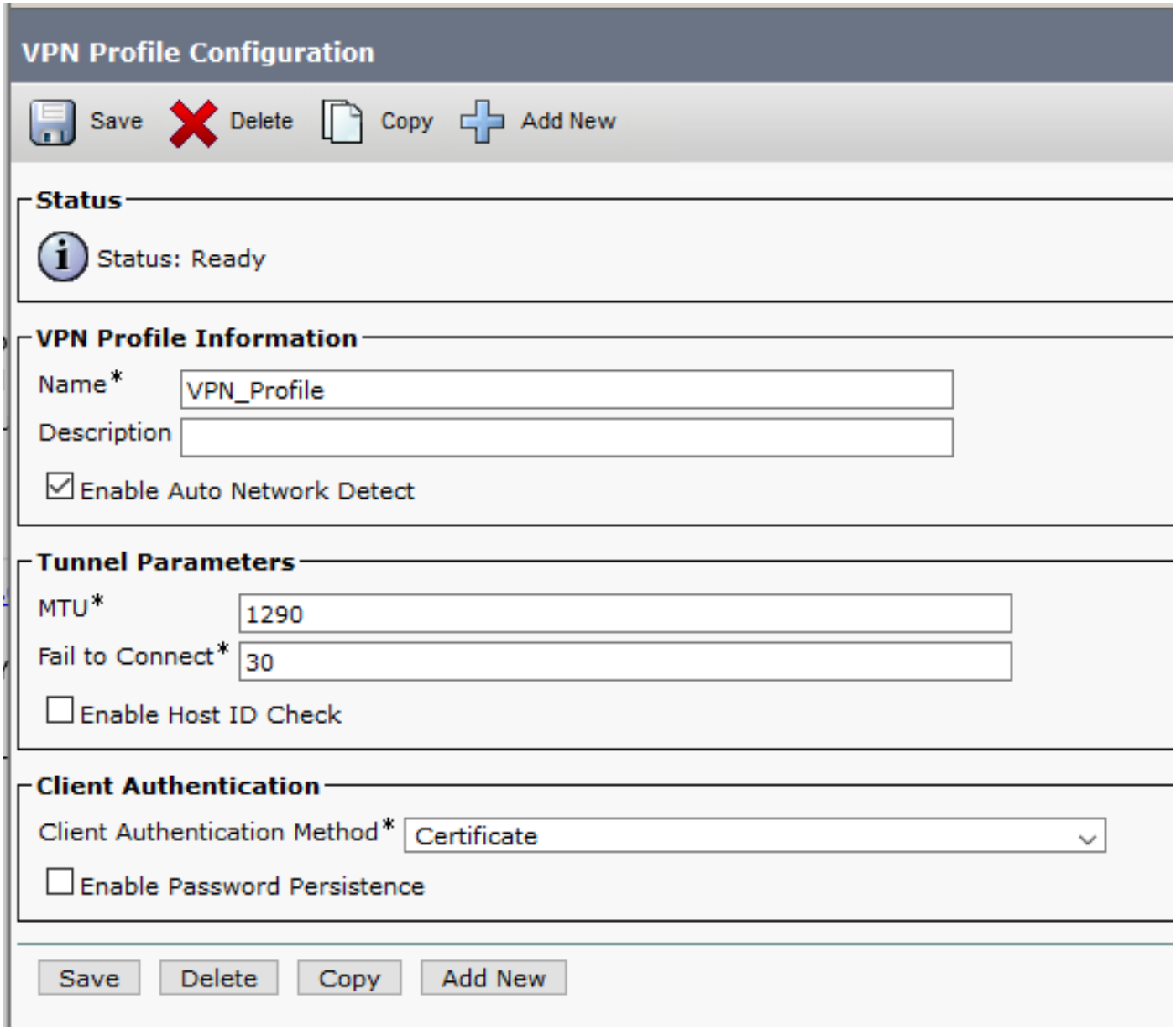
Configurazione CUCM

Passaggio 1. In CUCM, selezionare **Cisco Unified OS Administration > Security > Certificate Management** (Amministrazione del sistema operativo unificato Cisco > Sicurezza > Gestione certificati) e caricare il certificato ASA come **phone-vpn-trust**.

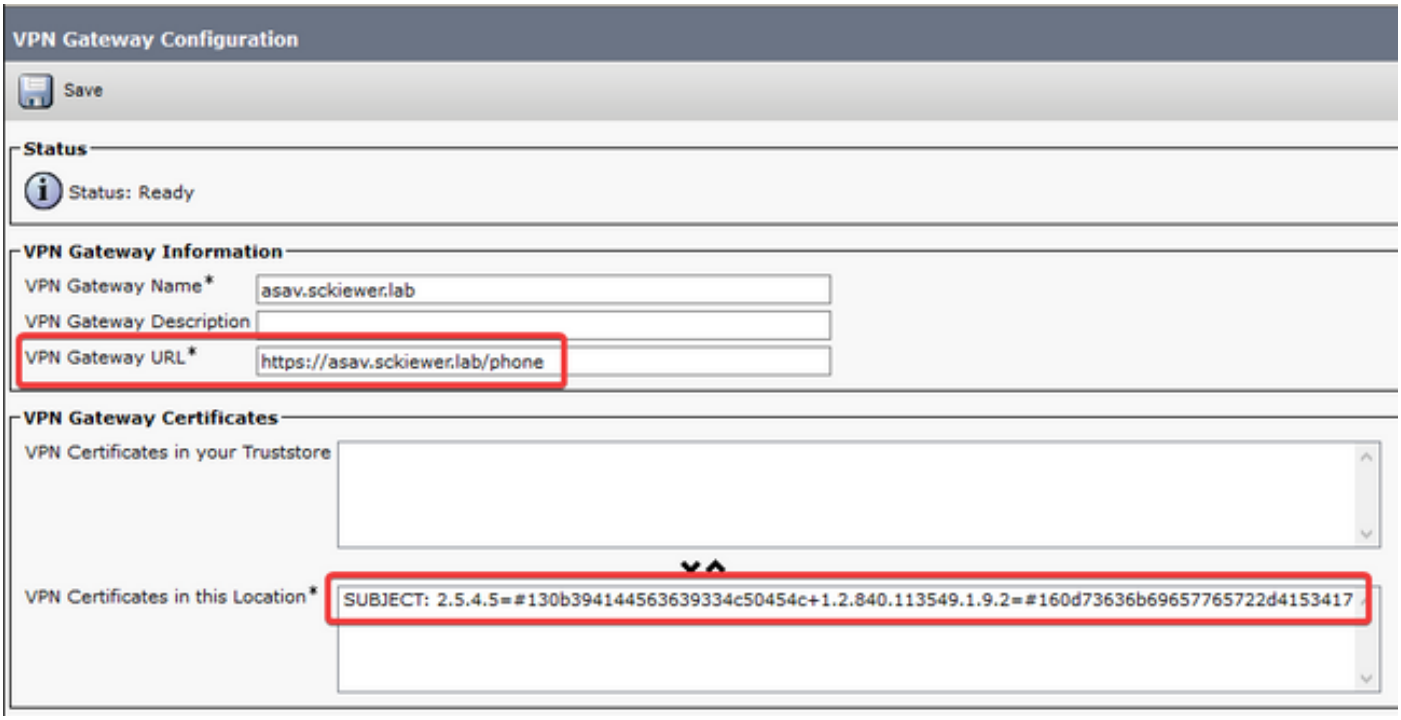


Passaggio 2. Al termine, passare a **Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile** e creare un nuovo profilo. In questa sezione non è presente alcun diritto o errore, ma è importante comprendere lo scopo di ogni impostazione.

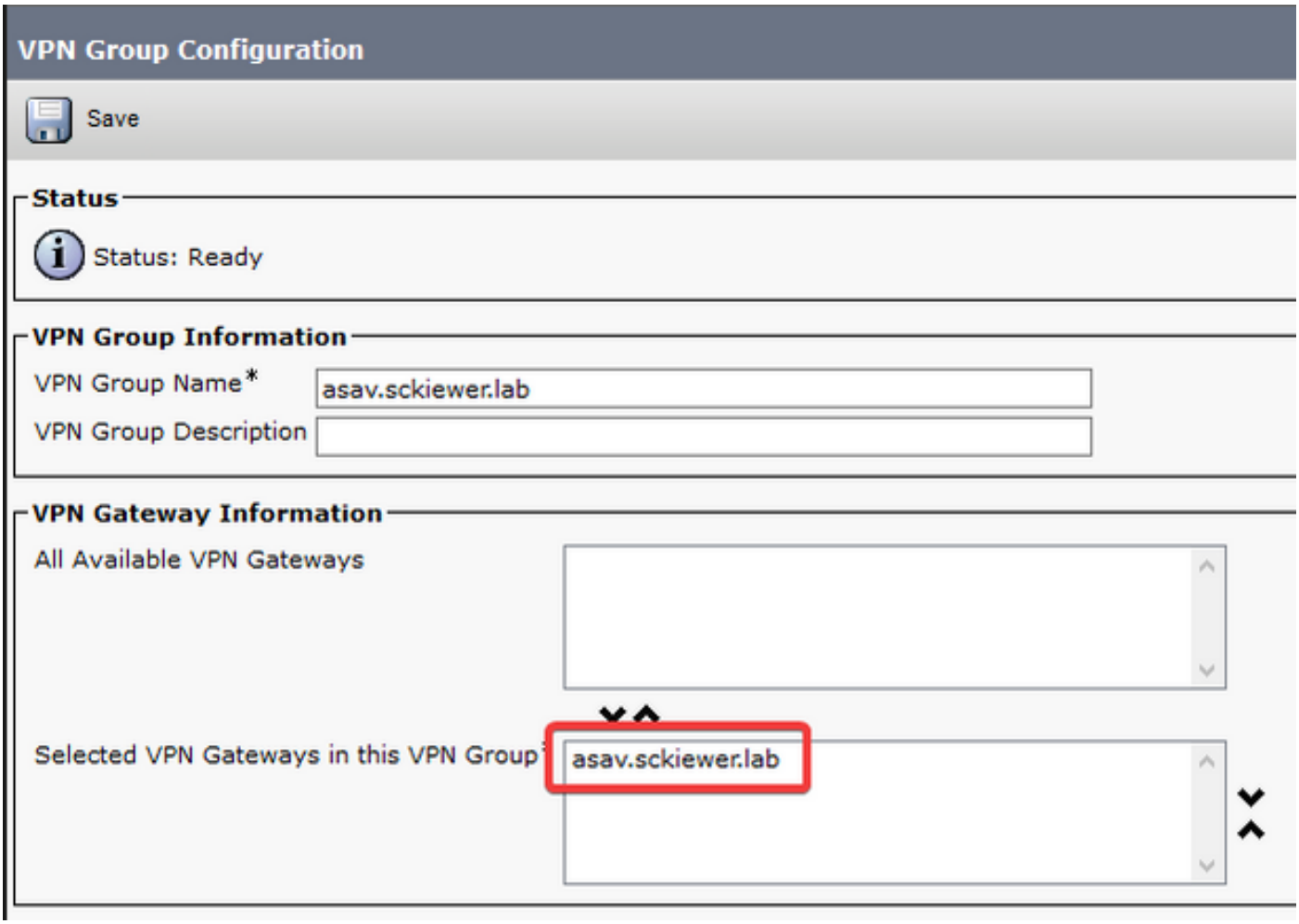
1. **Enable Auto Network Detect (Abilita rilevamento automatico rete)** - quando questa funzione è abilitata, il telefono comunica al server TFTP quando si accende. Se riceve una risposta al ping, non abilita la VPN. Se il telefono non riceve una risposta al ping, abilita la VPN. Quando questa impostazione è abilitata, non è possibile abilitare manualmente la VPN.
2. **Verifica dell'ID host**: quando questa opzione è abilitata, il telefono controlla l'URL della VPN dal file di configurazione (in questo documento, viene usato il sito https://asav.sckiewer.lab/phone) e verifica che il nome host o il nome di dominio completo (FQDN) corrisponda al nome comune (CN) o a una voce SAN nel certificato presentato dall'ASA.
3. **Metodo di autenticazione**: controlla il tipo di metodo di autenticazione utilizzato per la connessione all'appliance ASA. Nell'esempio di configurazione riportato in questo documento viene utilizzata l'autenticazione basata su certificati.
4. **Persistenza password**: se abilitata, la password del client viene memorizzata nel telefono fino a quando non si verifica un tentativo di accesso non riuscito, il client cancella manualmente la password o il telefono viene reimpostato.



Passaggio 3. Quindi, selezionare **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**. Verificare che l'URL del gateway VPN corrisponda alla configurazione ASA e spostare il certificato dalla casella superiore a quella inferiore, come mostrato nell'immagine:

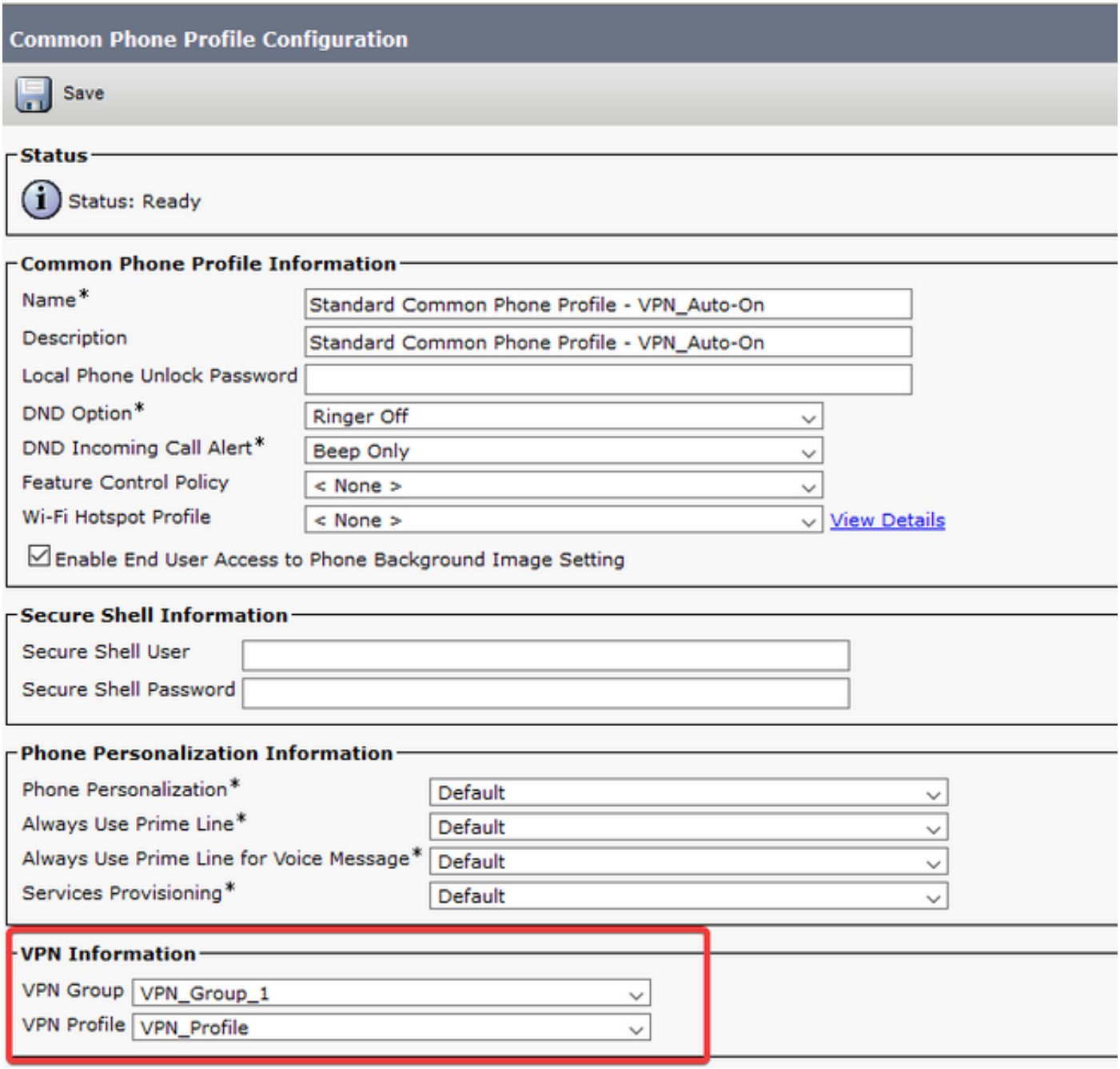


Passaggio 4. Una volta salvato, è necessario passare a **Cisco Unified CM Administration > Advanced Features > VPN Group** e spostare il gateway creato nella casella 'Selected VPN Gateway in this VPN Group' (Gateway VPN selezionati in questo gruppo VPN):



Passaggio 5. Ora che le impostazioni VPN sono state configurate, è necessario passare a **Cisco Unified CM Administration > Device > Device Settings > Common Phone Profile**. È necessario copiare il profilo utilizzato dal telefono VPN desiderato, rinominarlo e selezionare il gruppo VPN e

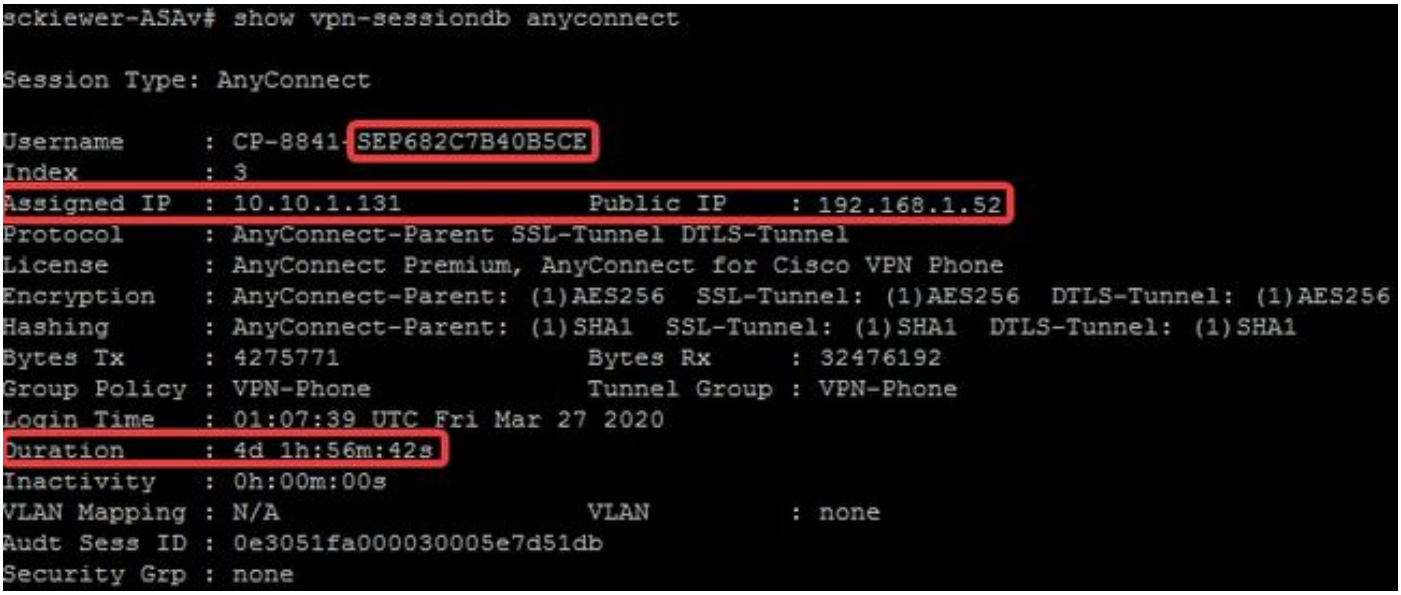
il profilo VPN, quindi salvare il nuovo profilo:



Passaggio 6. Infine, è necessario applicare questo nuovo profilo al telefono, quindi reimpostare il telefono mentre si trova nella rete interna. Questo permette al telefono di ricevere tutta la nuova configurazione, come l'hash del certificato ASA e l'URL della VPN.

> **Nota:** Prima di provare il telefono, è necessario verificare che i telefoni dispongano di un server TFTP alternativo configurato. Poiché l'ASA non fornisce un'opzione 150 ai telefoni, l'IP TFTP deve essere configurato sui telefoni manualmente.

Passaggio 7. Verificare il telefono VPN e verificare che possa connettersi all'ASA e registrarsi. È possibile verificare che il tunnel sia attivo sull'appliance ASA con il comando **show vpn-sessiondb anyconnect**:



Risoluzione dei problemi

Dati da raccogliere

Per risolvere un problema relativo a un telefono VPN, si consiglia di utilizzare i seguenti dati:

- Debug dell'ASA: registrazione del debug nel bufferregistrazione di debug-tracedebug transazioni ca crittografiche 25debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- Registri della console del telefono (o una PRT se il telefono la supporta - qui ulteriori informazioni)

Dopo aver riprodotto il problema con i debug abilitati, è possibile visualizzare l'output con questo comando perché l'output del comando debug contiene sempre 711001:

show log | i 711001

Problemi comuni

> **Nota:** Ai fini di questa sezione, gli snippet di log vengono creati da un telefono 8861 poiché si tratta di una delle serie di telefoni più comuni implementati come telefono VPN. Tenete presente che altri modelli possono scrivere messaggi diversi nei log.

Aggiornamento del certificato di identità ASA autofirmato

Prima della scadenza del certificato di identità ASA, è necessario generare un nuovo certificato e distribuirlo sui telefoni. Per fare questo senza un impatto sui telefoni VPN, utilizzare questo processo:

Passaggio 1. Creare un nuovo trust point per il nuovo certificato di identità:

crypto ca trustpoint asa-identity-cert-2

iscrizione self

nome soggetto CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

Passaggio 2. A questo punto, si avrebbe un nuovo certificato di identità per l'ASA, ma non è ancora stato usato su nessuna interfaccia. È necessario esportare il nuovo certificato e caricarlo in CUCM:

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

Passaggio 3. Dopo aver ottenuto il nuovo certificato di identità, caricarlo in uno dei nodi CUCM come phone-VPN-trust in **Cisco Unified OS Administration > Security > Certificate Management > Upload**.

> **Nota:** Il certificato di attendibilità VPN per telefono corrente è presente solo nel nodo CUCM in cui è stato caricato originariamente (non viene propagato automaticamente ad altri nodi come alcuni certificati). Se la versione CUCM è stata modificata da CSCuo58506, caricare il nuovo certificato ASA su un altro nodo.

Passaggio 4. Una volta caricato il nuovo certificato in uno dei nodi del cluster, passare a **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway** sul server di pubblicazione CUCM

Passaggio 5. Selezionare il gateway appropriato.

Passaggio 6. Selezionare il certificato nella casella in alto (quella appena caricata) e fare clic sulla freccia in giù per spostarlo in basso (in questo modo il TFTP può aggiungere il certificato nei file di configurazione del telefono VPN) e selezionare Salva.

Passaggio 7. Una volta completato, reimpostare tutti i telefoni VPN. A questo punto del processo, l'ASA presenta ancora il vecchio certificato, quindi i telefoni possono connettersi; tuttavia, possono acquisire un nuovo file di configurazione che contiene sia il nuovo certificato sia il vecchio certificato.

Passaggio 8. Ora è possibile applicare il nuovo certificato all'appliance ASA. A tale scopo, sono necessari il nome del nuovo trust point e il nome dell'interfaccia esterna, quindi eseguire questo comando con le informazioni seguenti:

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

> **Nota:** È possibile passare all'URL webvpn nel browser per verificare che l'ASA presenti il nuovo certificato. Poiché l'indirizzo deve essere raggiungibile pubblicamente dai telefoni esterni, anche il PC è in grado di raggiungerlo. È quindi possibile controllare il certificato presentato dall'ASA al browser e confermare che si tratta del nuovo.

Passaggio 9. Dopo aver configurato l'ASA per l'uso del nuovo certificato, reimpostare un telefono di prova e verificare che sia in grado di connettersi all'ASA e registrarsi. Se la registrazione del telefono ha esito positivo, è possibile ripristinare tutti i telefoni e verificare che possano connettersi all'ASA e registrarsi. Questa è la procedura consigliata perché, dopo la modifica del certificato, i

telefoni connessi all'appliance ASA rimangono collegati. Se si esegue il test dell'aggiornamento del certificato su un telefono, si riduce il rischio di problemi di configurazione per un numero elevato di telefoni. Se il primo telefono VPN non riesce a connettersi all'ASA, è possibile raccogliere i log dal telefono e/o dall'ASA per risolvere il problema, mentre gli altri telefoni rimangono connessi.

Passaggio 10. Una volta verificato che i telefoni sono in grado di connettersi e registrarsi con il nuovo certificato, il vecchio certificato può essere rimosso da CUCM.

L'appliance ASA seleziona la cifratura EC (Elliptic Curve)

Le appliance ASA supportano la crittografia a curva ellittica (EC) a partire dalla versione 9.4(x), quindi è comune verificare gli errori dei telefoni VPN che funzionavano in precedenza dopo un aggiornamento dell'ASA alla versione 9.4(x) o successive. Questo si verifica perché l'ASA seleziona una cifratura EC durante l'handshake TLS con i modelli di telefono più recenti. In genere, esiste un certificato RSA associato all'interfaccia a cui si connette il telefono, in quanto la versione ASA precedente non supportava l'EC. A questo punto, poiché l'ASA ha selezionato una cifratura EC, non può usare un certificato RSA per la connessione, quindi genera e invia al telefono un certificato temporaneo autofirmato che crea con l'algoritmo EC piuttosto che con RSA. Poiché questo certificato temporaneo non viene riconosciuto dal telefono, la connessione non riesce. È possibile verificare questo nei registri telefonici 88xx è abbastanza semplice.

```
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
```

Le note telefonate mostrano che l'ASA ha selezionato una cifratura EC per questa connessione, in quanto la linea 'nuova cifratura' contiene cifrature EC, il che provoca il malfunzionamento della connessione.

Nello scenario in cui è stato selezionato AES, viene visualizzato quanto segue:

```
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
```

Per ulteriori informazioni, fare clic qui CSCuu02848.

Per risolvere il problema, disabilitare i cifrari EC sull'appliance ASA per la versione TLS usata dal telefono. Per ulteriori informazioni sulla versione TLS supportata da ogni modello di telefono, fare clic qui:

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

Dopo aver identificato le versioni TLS rilevanti per il proprio ambiente, è possibile eseguire questi comandi sull'appliance ASA per disabilitare le cifrature EC per tali versioni:

```
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"
```

Tenere presente che i telefoni IP utilizzano il protocollo DTLS (Datagram Transport Layer Security) per impostazione predefinita, quindi è necessario eseguire l'istruzione di cifratura per DTLS e la versione TLS appropriata per i telefoni. Inoltre, è importante capire che queste modifiche sono globali sull'appliance ASA, quindi impediscono che le cifrature EC vengano negoziate da altri client AnyConnect che usano quelle versioni TLS.

Errore di connessione DTLS

In alcuni casi, i telefoni VPN non possono stabilire una connessione all'ASA con DTLS. Se il telefono tenta di utilizzare il DTLS ma non riesce, continua a provare il DTLS più volte, senza successo, perché sa che il DTLS è abilitato. Questo si vedrebbe nelle note telefonate 88xx:

```
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
```

Questa condizione può essere causata dallo stesso problema descritto nella sezione Selezione della curva ellittica (EC) dell'appliance ASA, quindi è necessario verificare che i cifrari EC siano disabilitati per le DTLS. Inoltre, è possibile disabilitare del tutto il DTLS che forza i telefoni VPN a utilizzare il TLS. Questa soluzione non è ideale, in quanto implica che tutto il traffico utilizzi il protocollo TCP anziché l'UDP, con un conseguente sovraccarico. Tuttavia, in alcuni scenari si tratta di un test valido, in quanto almeno conferma che la maggior parte della configurazione è corretta e che il problema è specifico delle DTLS. Se si desidera verificarlo, è consigliabile eseguirlo a livello di Criteri di gruppo, in quanto gli amministratori utilizzano in genere criteri di gruppo univoci per i telefoni VPN, che consentono di verificare una modifica senza influire sugli altri client.

attributi criteri gruppo vpn-phone-policy
webvpn
anyconnect ssl dtls none

Un altro problema di configurazione comune che può impedire la riuscita di una connessione DTLS è che il telefono non è in grado di stabilire la connessione TLS e DTLS con la stessa cifratura. Esempio di estratto di registro:

```
%%%%% 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
```

Potete vedere i cifrari TLS offerti nella prima riga del frammento. Viene selezionata l'opzione più sicura supportata da entrambi i lati (i log non mostrano la selezione; tuttavia, è possibile dedurre che è almeno AES-256 dal frammento di log). Si noti inoltre che l'unica cifratura DTLS disponibile è AES128. Poiché la cifratura TLS selezionata non è disponibile per DTLS, la connessione non riesce. Per risolvere questo scenario, è necessario verificare che la configurazione ASA consenta di usare gli stessi cifrari per i protocolli TLS e DTLS.

Telefono: impossibile connettersi all'appliance ASA dopo l'aggiornamento del certificato

Èmolto importante caricare un nuovo certificato di identità ASA come phone-vpn-trust su CUCM in modo che i telefoni possano acquisire l'hash per questo nuovo certificato. Se non si segue questo processo, dopo l'aggiornamento e la successiva connessione di un telefono VPN all'appliance

ASA, al telefono viene presentato un certificato non attendibile, quindi la connessione non riesce. Questa situazione può verificarsi qualche giorno o settimana dopo l'aggiornamento del certificato ASA, in quanto i telefoni non vengono disconnessi quando il certificato viene modificato. Finché l'ASA continua a ricevere pacchetti keepalive dal telefono, il tunnel VPN rimane attivo. Quindi, se è stato confermato che il certificato ASA è stato aggiornato, ma il nuovo certificato non è stato inserito prima su CUCM, sono disponibili due opzioni:

1. Se il vecchio certificato di identità ASA è ancora valido, ripristinare il vecchio certificato dall'ASA e seguire la procedura descritta in questo documento per aggiornare il certificato. Se è già stato generato un nuovo certificato, è possibile ignorare la sezione di generazione del certificato.
2. Se il vecchio certificato di identità ASA è scaduto, è necessario caricare il nuovo certificato ASA in CUCM e riportare i telefoni sulla rete interna per ricevere il file di configurazione aggiornato con il nuovo hash del certificato.

Il telefono non riesce a risolvere l'URL ASA tramite DNS

In alcuni scenari, l'amministratore configura l'URL della VPN con un nome host anziché con un indirizzo IP. Al termine, il telefono deve avere un server DNS per poter risolvere il nome in un indirizzo IP. Nello snippet di codice è possibile notare che il telefono tenta di risolvere il nome con i suoi due server DNS, 192.168.1.1 e 192.168.1.2, ma non riceve risposta. Dopo 30 secondi, il telefono stampa un '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]
```

In genere indica uno dei seguenti elementi:

1. Il telefono ha un server DNS non valido
2. Il telefono non ha ricevuto un server DNS tramite DHCP o non è stato configurato manualmente

Per risolvere il problema, sono disponibili due opzioni:

1. Controllare la configurazione del telefono per assicurarsi che riceva un server DNS dal server DHCP quando è esterno e/o verificare che il server DNS del telefono possa risolvere il nome usato nella configurazione ASA
2. Modificare l'URL nella configurazione ASA e in CUCM in un indirizzo IP in modo che DNS non sia necessario

Il telefono non abilita la VPN

Come accennato in precedenza in questo documento, Auto Network Detect fa sì che il telefono esegua il ping sul server TFTP e verifichi la presenza di una risposta. Se il telefono si trova sulla rete interna, il server TFTP è raggiungibile senza VPN, quindi quando il telefono riceve risposte ai ping, non abilita la VPN. Quando il telefono NON è sulla rete interna, i ping hanno esito negativo, quindi il telefono può abilitare la VPN e connettersi all'ASA. Tenere presente che probabilmente la rete domestica di un client non sarà configurata in modo da fornire al telefono un'opzione 150 tramite DHCP e che anche l'ASA non può fornire un'opzione 150, quindi il 'TFTP alternativo' è un requisito per i telefoni VPN.

Nei registri è possibile verificare alcuni elementi:

1. Il telefono esegue il ping sull'indirizzo IP del server TFTP CUCM?
2. Il telefono riceve una risposta ai ping?
3. Il telefono abilita la VPN dopo che non riceve una risposta ai ping?

Èimportante visualizzare questi elementi nell'ordine indicato. In uno scenario in cui il telefono usa il ping sull'IP sbagliato e riceve una risposta, sarebbe inutile abilitare i debug sull'appliance ASA perché il telefono non abilita la VPN. Convalidare i tre elementi nell'ordine indicato per evitare un'analisi del registro non necessaria. Questo messaggio viene visualizzato nelle note telefonate 88xx se il ping ha esito negativo e la VPN è abilitata:

```
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()
```

Il Telefono Si Registra Ma Non Può Visualizzare La Cronologia Delle Chiamate

Verificare che sul telefono sia abilitato il protocollo TFTP alternativo e che sia configurato l'indirizzo IP TFTP corretto. Il TFTP alternativo è un requisito per i telefoni VPN perché l'ASA non può fornire un'opzione 150.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems