

# Esempio di configurazione di una connessione telefonica VPN AnyConnect a un router Cisco IOS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Topologia della rete](#)

[Configurazione server VPN SSL](#)

[Procedura di configurazione comune](#)

[Configurazione con autenticazione AAA](#)

[Configurazione con il certificato LSC \(Locally Significant Certificate\) per l'autenticazione del client del telefono IP](#)

[Configurazione Gestione chiamate](#)

[Esporta il certificato di identità o autofirmato dal router al CUCM](#)

[Configurare il gateway, il gruppo e il profilo VPN in CUCM](#)

[Applicazione del gruppo e del profilo al telefono IP con il profilo telefonico comune](#)

[Applicazione del profilo telefonico comune al telefono IP](#)

[Installare Locally Significant Certificates \(LSC\) sui telefoni IP Cisco](#)

[Registrare nuovamente il telefono per Call Manager e scaricare la nuova configurazione](#)

[Verifica](#)

[Verifica router](#)

[Verifica CUCM](#)

[Risoluzione dei problemi](#)

[Debug sul server VPN SSL](#)

[Debug dal telefono](#)

[Bug correlati](#)

## Introduzione

In questo documento viene descritto come configurare il router e i dispositivi di gestione delle chiamate Cisco IOS® in modo che i Cisco IP Phone possano stabilire connessioni VPN al router Cisco IOS. Queste connessioni VPN sono necessarie per proteggere la comunicazione con uno di questi due metodi di autenticazione client:

- Server di autenticazione, autorizzazione e accounting (AAA) o database locale
- Certificato telefonico

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Cisco IOS 15.1(2)T o versioni successive
- Set funzioni/Licenza: Universal (Data & Security & UC) per Cisco IOS Integrated Service Router (ISR)-G2
- Set funzioni/Licenza: Sicurezza avanzata per Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM) versione 8.0.1.10000-4 o successive
- IP Phone release 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) o successiva

Per un elenco completo dei telefoni supportati nella versione CUCM in uso, attenersi alla seguente procedura:

1. Apri questo URL: **https://<Indirizzo IP server CUCM>:8443/cucreports/systemReports.do**
2. Scegliere **Elenco funzioni telefono CM unificato > Genera un nuovo report > Funzionalità: Rete privata virtuale.**

Le versioni utilizzate in questo esempio di configurazione includono:

- Router Cisco IOS release 15.1(4)M4
- Call Manager release 8.5.1.1000-26
- IP Phone release 9.1(1)SR1S

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.

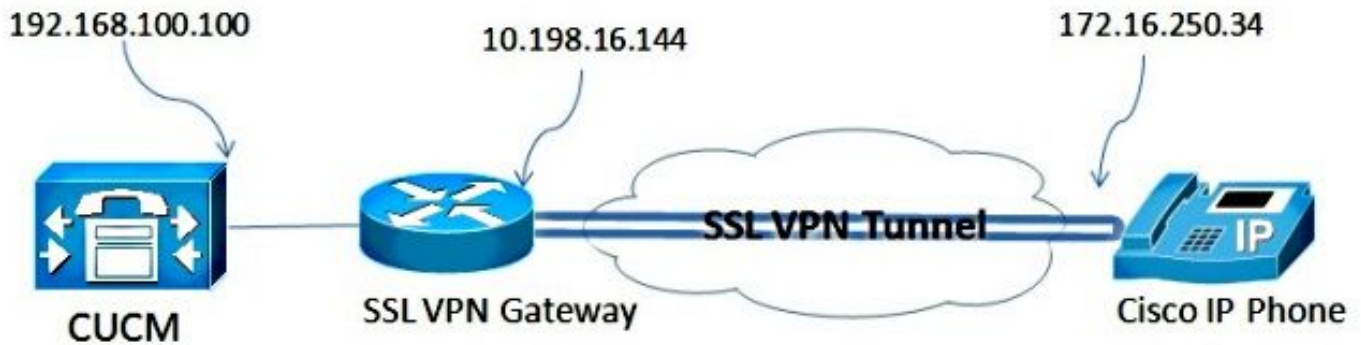
## Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi \(solo utenti registrati\)](#).

## Topologia della rete

La topologia utilizzata in questo documento include un Cisco IP Phone, il router Cisco IOS come gateway VPN Secure Sockets Layer (SSL) e CUCM come gateway vocale.



## Configurazione server VPN SSL

In questa sezione viene descritto come configurare l'headend Cisco IOS in modo da consentire le connessioni VPN SSL in entrata.

### Procedura di configurazione comune

1. Generare la chiave Rivest-Shamir-Adleman (RSA) con una lunghezza di 1024 byte:

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

2. Creare il trust point per il certificato autofirmato e associare la chiave RSA SSL:

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

3. Una volta configurato il trust point, registrare il certificato autofirmato con questo comando:

```
Router(config)#crypto pki enroll server-certificate
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
```

```
Router Self Signed Certificate successfully created
```

4. Abilitare il pacchetto AnyConnect corretto sull'headend. Il telefono stesso non scarica questo pacchetto. Ma, senza il pacchetto, il tunnel VPN non si stabilisce. Si consiglia di utilizzare la versione più recente del software client disponibile su Cisco.com. In questo esempio viene utilizzata la versione 3.1.3103.

Nelle versioni precedenti di Cisco IOS, questo è il comando per abilitare il pacchetto:

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

Tuttavia, nell'ultima versione di Cisco IOS, questo è il comando:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

5. Configurare il gateway VPN. Il gateway WebVPN viene utilizzato per terminare la connessione SSL dall'utente.

```
webvpn gateway SSL
ip address 10.198.16.144 port 443
ssl encryption 3des-sha1 aes-sha1
http-redirect port 80
ssl trustpoint server-certificate
inservice
```

**Nota:** L'indirizzo IP utilizzato qui deve trovarsi sulla stessa subnet dell'interfaccia a cui si connettono i telefoni, oppure il gateway deve essere originato direttamente da un'interfaccia sul router. Il gateway viene anche usato per definire il certificato usato dal router per convalidarsi sul client.

6. Definire il pool locale utilizzato per assegnare gli indirizzi IP ai client quando si connettono:

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

## Configurazione con autenticazione AAA

In questa sezione vengono descritti i comandi necessari per configurare il server AAA o il database locale per autenticare i telefoni. Se si intende utilizzare l'autenticazione basata solo sul certificato per i telefoni, passare alla sezione successiva.

### Configurare il database utenti

Per l'autenticazione è possibile utilizzare il database locale del router o un server AAA esterno:

- Per configurare il database locale, immettere:

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

- Per configurare un server RADIUS AAA remoto per l'autenticazione, immettere:

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

### Configurare il contesto virtuale e i Criteri di gruppo

Il contesto virtuale viene utilizzato per definire gli attributi che governano la connessione VPN, ad esempio:

- L'URL da utilizzare per la connessione
- Il pool da utilizzare per assegnare gli indirizzi del client
- Metodo di autenticazione da utilizzare

Questi comandi sono un esempio di contesto che utilizza l'autenticazione AAA per il client:

```
webvpn context SSL
aaa authenticate list SSL
gateway SSL domain SSLPhones
```

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

## Configurazione con il certificato LSC (Locally Significant Certificate) per l'autenticazione del client del telefono IP

In questa sezione vengono descritti i comandi necessari per configurare l'autenticazione client basata su certificati per i telefoni. Tuttavia, per fare ciò, è necessaria la conoscenza dei vari tipi di certificati telefonici:

- **Certificato di installazione (MIC) del produttore:** i MIC sono inclusi su tutti i telefoni IP Cisco 7941, 7961 e successivi. I MIC sono certificati chiave a 2.048 bit firmati da Cisco Certificate Authority (CA). Affinché CUCM consideri attendibile il certificato MIC, utilizza i certificati CA preinstallati CAP-RTP-001, CAP-RTP-002 e Cisco\_Manufacturing\_CA nel relativo archivio certificati attendibili. Poiché il certificato è fornito dal produttore stesso, come indicato nel nome, non è consigliabile utilizzarlo per l'autenticazione client.
- **LSC -** LSC protegge la connessione tra CUCM e il telefono dopo aver configurato la modalità di sicurezza del dispositivo per l'autenticazione o la crittografia. LSC possiede la chiave pubblica per il telefono IP Cisco, che è firmata dalla chiave privata CUCM Certificate Authority Proxy Function (CAPF). Si tratta del metodo più sicuro (rispetto all'uso degli MIC).

**Attenzione:** A causa dell'aumento dei rischi per la sicurezza, Cisco consiglia di usare gli MIC solo per l'installazione di LSC e non per continuare a usarli. I clienti che configurano i telefoni IP Cisco in modo da utilizzare i MIC per l'autenticazione Transport Layer Security (TLS) o per qualsiasi altro scopo, lo fanno a proprio rischio.

Nell'esempio di configurazione, viene usata la LSC per autenticare i telefoni.

**Suggerimento:** Il modo più sicuro per collegare il telefono è usare l'autenticazione doppia, che combina l'autenticazione certificato e AAA. È possibile configurare questa impostazione se si combinano i comandi utilizzati per ognuno in un contesto virtuale.

## Configurare il punto di fiducia per convalidare il certificato client

Per convalidare il protocollo LSC dal telefono IP, sul router deve essere installato il certificato CAPF. Per ottenere il certificato e installarlo sul router, procedere come segue:

1. Andare alla pagina Web Amministrazione sistema operativo (OS) CUCM.
2. Scegliere **Protezione > Gestione certificati**.  
**Nota:** Questa posizione potrebbe cambiare in base alla versione CUCM.
3. Individuare il certificato **CAPF** e scaricare il file **.pem**. Salvarlo come file **.txt**
4. Una volta estratto il certificato, creare un nuovo trust point sul router e autenticare il trust point con CAPF, come mostrato di seguito. Quando viene richiesto il certificato CA codificato in base 64, selezionare e incollare il testo nel file .pem scaricato insieme alle righe BEGIN e END.

```
Router(config)#crypto pki trustpoint CAPF
```

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

```
quit
```

## Note importanti:

- Il metodo di registrazione è terminale perché il certificato deve essere installato manualmente sul router.
- Il comando **authorization username** è necessario per comunicare al router cosa usare come nome utente quando il client effettua la connessione. In questo caso utilizza il nome comune (CN).
- È necessario disabilitare una verifica di revoca perché per i certificati telefonici non è definito un elenco di revoche di certificati (CRL). Pertanto, a meno che non sia disabilitata, la connessione non riesce e i debug PKI (Public Key Infrastructure) visualizzano questo output:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilities request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

## Configurare il contesto virtuale e i Criteri di gruppo

Questa parte della configurazione è simile a quella utilizzata in precedenza, ad eccezione di due punti:

- Metodo di autenticazione
- Il trust point utilizzato dal contesto per autenticare i telefoni

Di seguito sono riportati i comandi disponibili:

```
webvpn context SSL
gateway SSL domain SSLPhones
authentication certificate
ca trustpoint CAPF
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonenvpn" netmask 255.255.255.0
svc keep-client-installed
```

default-group-policy phones

## Configurazione Gestione chiamate

In questa sezione vengono descritti i passaggi di configurazione di Call Manager.

### Esporta il certificato di identità o autofirmato dal router al CUCM

Per esportare il certificato dal router e importarlo in Call Manager come certificato Phone-VPN-Trust, attenersi alla seguente procedura:

1. Controllare il certificato utilizzato per SSL.

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

2. Esportare il certificato.

```
Router(config)#crypto pki export server-certificate pem terminal
The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
-----BEGIN CERTIFICATE-----

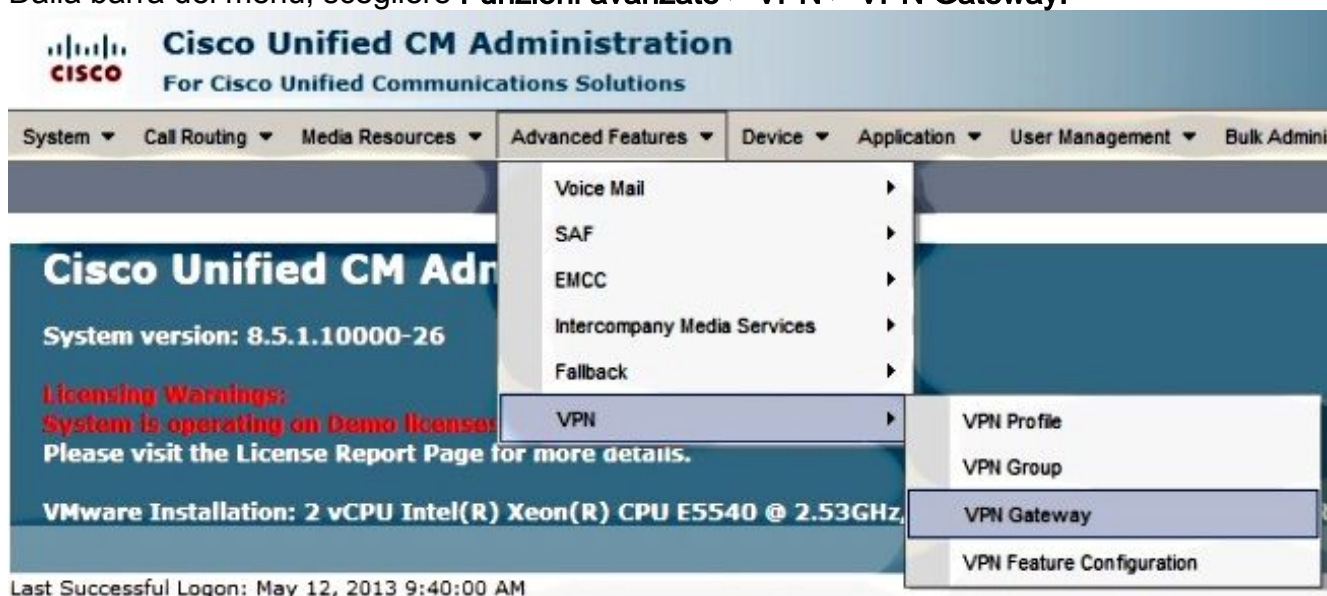
<output removed>

-----END CERTIFICATE-----
```

3. Copiare il testo dal terminale e salvarlo come file .pem.
4. Accedere a Call Manager e scegliere **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust** per caricare il file del certificato salvato nel passaggio precedente.

### Configurare il gateway, il gruppo e il profilo VPN in CUCM

1. Passare a **Cisco Unified CM Administration**.
2. Dalla barra dei menu, scegliere **Funzioni avanzate > VPN > VPN Gateway**.



3. Nella finestra Configurazione gateway VPN, eseguire i seguenti passaggi:  
Nel campo Nome gateway VPN immettere un nome. Può essere un nome qualsiasi. Nel campo Descrizione gateway VPN immettere una descrizione (facoltativo). Nel campo VPN Gateway URL (URL gateway VPN), immettere l'URL del gruppo definito sul router. Nel campo

Certificati VPN in questa posizione scegliere il certificato caricato in Gestione chiamate in precedenza per spostarlo dall'archivio di attendibilità a questa posizione.

**-VPN Gateway Information-**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

---

**-VPN Gateway Certificates-**

VPN Certificates in your Truststore

- SUBJECT: CN=10.198.16.136,unstructuredName=10.198.16.136 ISSUER: CN=10.198.16.136,unstructuredName=
- SUBJECT: unstructuredName=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com ISSUER: DC=com,DC=certac,DC=
- SUBJECT: C=CR,O=Cisco,OU=VPN,CN=ASA5520-C.cisco.com,unstructuredName=ASA5520-C.cisco.com ISSUER:
- SUBJECT: CN=10.198.16.140:8443 ISSUER: CN=10.198.16.140:8443 S/N: e7:e2:72:4f
- SUBJECT: CN=ASA5510-F-IP-PHONE,unstructuredName=ASA5510-F.cisco.com ISSUER: CN=ASA5510-F-IP-PHON

VPN Certificates in this Location\*

- SUBJECT: CN=10.198.16.144,SERIALNUMBER=FTX1309A406+unstructuredName=R2811.vpn.cisco-tac.com ISSU

4. Dalla barra dei menu, scegliere **Funzioni avanzate > VPN > Gruppo VPN**.

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

**VPN Gateway Configuration**

**Status**

Status: Ready

**VPN Gateway Information**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

- Voice Mail ▶
- SAF ▶
- EMCC ▶
- Intercompany Media Services ▶
- Fallback ▶
- VPN ▶**
  - VPN Profile
  - VPN Group**
  - VPN Gateway
  - VPN Feature Configuration

5. Nel campo Tutti i gateway VPN disponibili, scegliere il **gateway VPN** definito in precedenza. Fare clic sulla freccia in giù per spostare il gateway selezionato nei gateway VPN selezionati nel campo Gruppo VPN.



### 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

Selected VPN Gateways in this VPN Group\*

6. Dalla barra dei menu, scegliere **Funzioni avanzate > VPN > Profilo VPN**.

The screenshot shows the 'VPN Group Configuration' page with the 'Advanced Features' menu open. The 'VPN' option is selected, and the 'VPN Profile' sub-option is highlighted. The background shows the configuration form with 'VPN Group Name' set to 'IOS\_SSL\_Phones'.

7. Per configurare il profilo VPN, completare tutti i campi contrassegnati da un asterisco (\*).

## VPN Profile Configuration



Save



Delete



Copy



Add New

### Status



Status: Ready

### VPN Profile Information

Name\*

IOS\_SSL\_Phones

Description

Enable Auto Network Detect

### Tunnel Parameters

MTU\*

1290

Fail to Connect\*

30

Enable Host ID Check

### Client Authentication

Client Authentication Method\* Certificate

Enable Password Persistence

Save

Delete

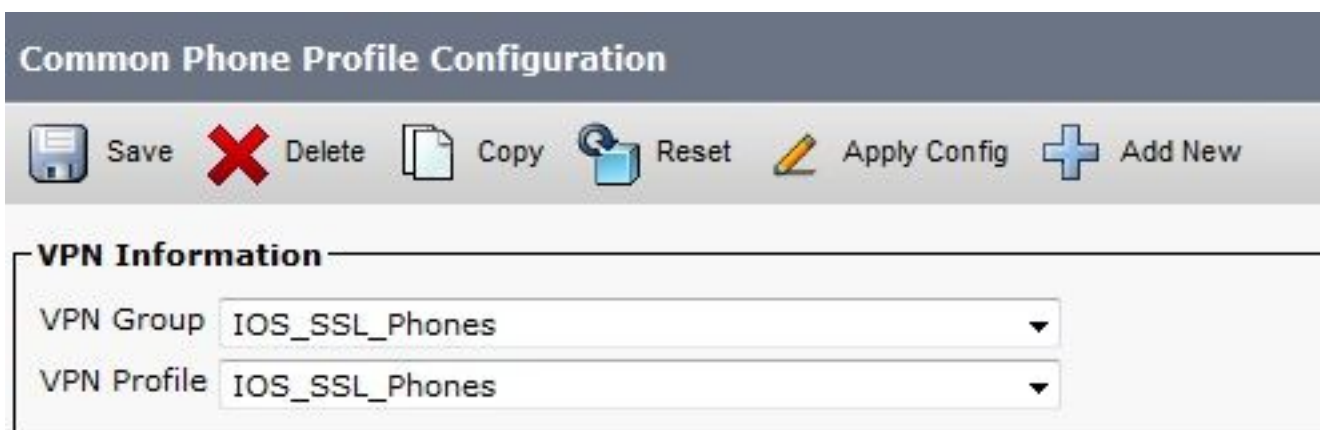
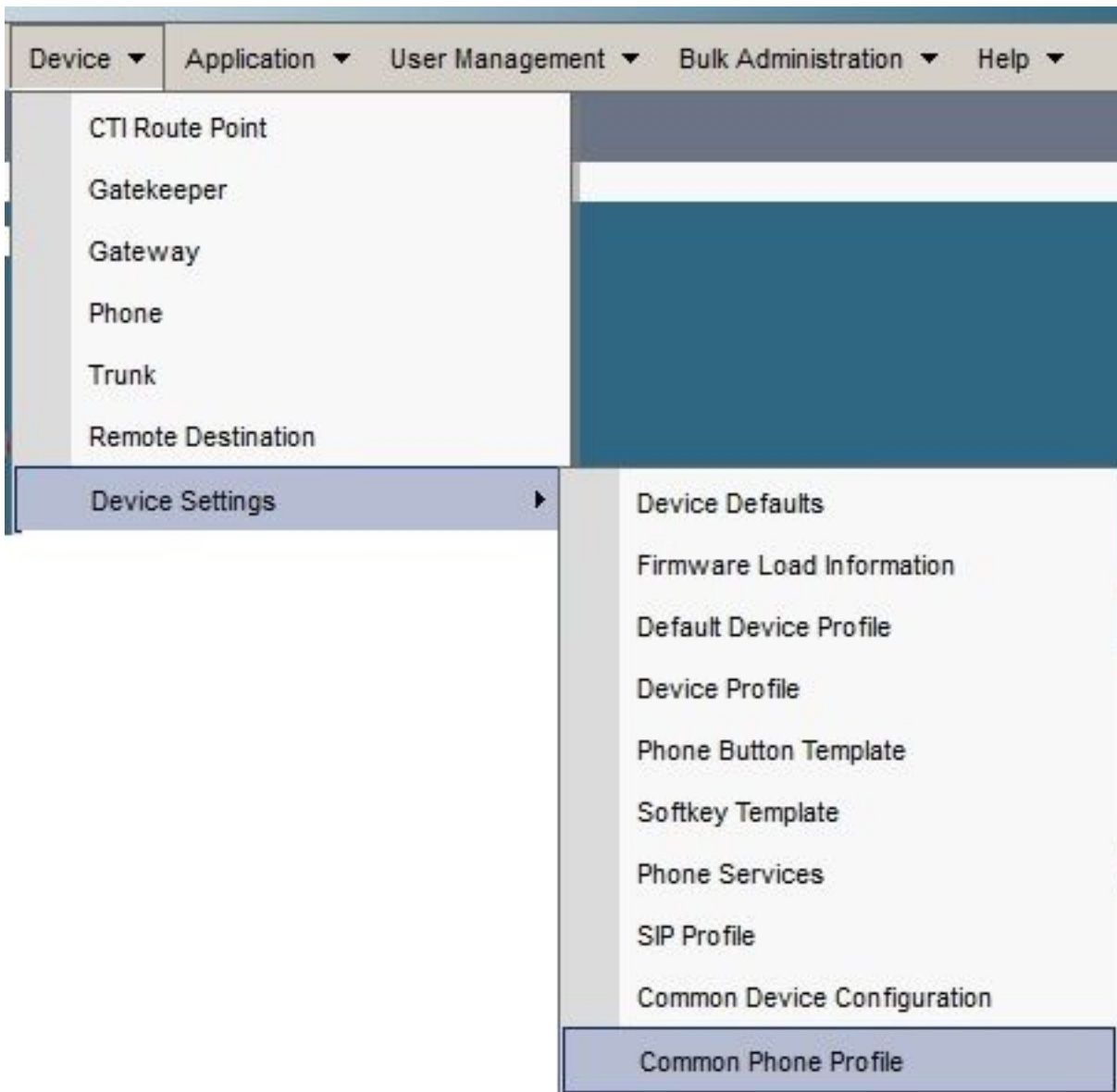
Copy

Add New

**Attiva rilevamento automatico rete:** Se abilitata, il telefono VPN effettua il ping al server TFTP. Se non si riceve alcuna risposta, viene avviata automaticamente una connessione VPN.**Abilita controllo ID host:** Se abilitato, il telefono VPN confronta il nome di dominio completo (FQDN) dell'URL del gateway VPN con la rete CN/SAN (Storage Area Network) del certificato. Il client non riesce a connettersi se questi elementi non corrispondono o se viene utilizzato un certificato con caratteri jolly con un asterisco (\*).**Abilita persistenza password:** Questo consente al telefono VPN di memorizzare nella cache il nome utente e la password per il successivo tentativo VPN.

### Applicazione del gruppo e del profilo al telefono IP con il profilo telefonico comune

Nella finestra Configurazione profilo telefonico comune, fare clic su **Apply Config** (Applica configurazione) per applicare la nuova configurazione VPN. È possibile utilizzare il **profilo telefonico comune** standard o creare un nuovo profilo.



### Applicazione del profilo telefonico comune al telefono IP

Se è stato creato un nuovo profilo per telefoni/utenti specifici, passare alla finestra **Configurazione telefono**. Nel campo Profilo telefono comune, scegliere il profilo **Standard Common Phone**.



## Installare Locally Significant Certificates (LSC) sui telefoni IP Cisco

La seguente guida può essere utilizzata per installare Locally Significant Certificates sui telefoni IP Cisco. Questo passaggio è necessario solo se viene utilizzata l'autenticazione tramite LSC. L'autenticazione tramite il certificato di installazione del produttore (MIC) o il nome utente e la password non richiede l'installazione di un LSC.

[Installare un LSC in un telefono con la modalità di protezione cluster CUCM impostata su Non protetto.](#)

## Registrare nuovamente il telefono per Call Manager e scaricare la nuova configurazione

Questo è il passaggio finale del processo di configurazione.

## Verifica

### Verifica router

Per controllare le statistiche della sessione VPN nel router, è possibile utilizzare questi comandi e verificare le differenze tra gli output (evidenziati) per l'autenticazione del nome utente e del certificato:

### Per l'autenticazione di nome utente/password:

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones                Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
```

```

Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

```

```
Router#show webvpn session context all
```

```

WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones            172.16.250.34          1                00:30:38  00:00:20

```

### Per l'autenticazione dei certificati:

```
Router#show webvpn session user SEP8CB64F578B2C context all
```

```

Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

```

```

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932

```

```
Router#show webvpn session context all
```




```

WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C  172.16.250.34          1                3d04h    00:00:16

```

### Verifica CUCM

Confermare che il telefono IP sia registrato con Gestione chiamate con l'indirizzo assegnato dal router alla connessione SSL.

Phone (1 - 4 of 4)							
Find Phone where Device Name begins with <input type="text"/> Find Clear Filter <input type="button" value="↕"/> <input type="button" value="←"/>							
Select item or enter search text ▼							
<input type="checkbox"/>		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
<input type="checkbox"/>		SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B13	Auto 1000	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

# Risoluzione dei problemi

## Debug sul server VPN SSL

Router#**show debug**

WebVPN Subsystem:

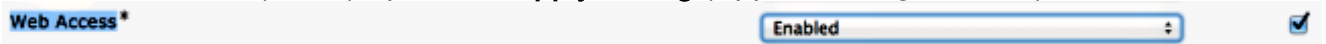
WebVPN (verbose) debugging is on  
WebVPN HTTP debugging is on  
WebVPN AAA debugging is on  
WebVPN tunnel debugging is on  
WebVPN Tunnel Events debugging is on  
WebVPN Tunnel Errors debugging is on  
Webvpn Tunnel Packets debugging is on

PKI:

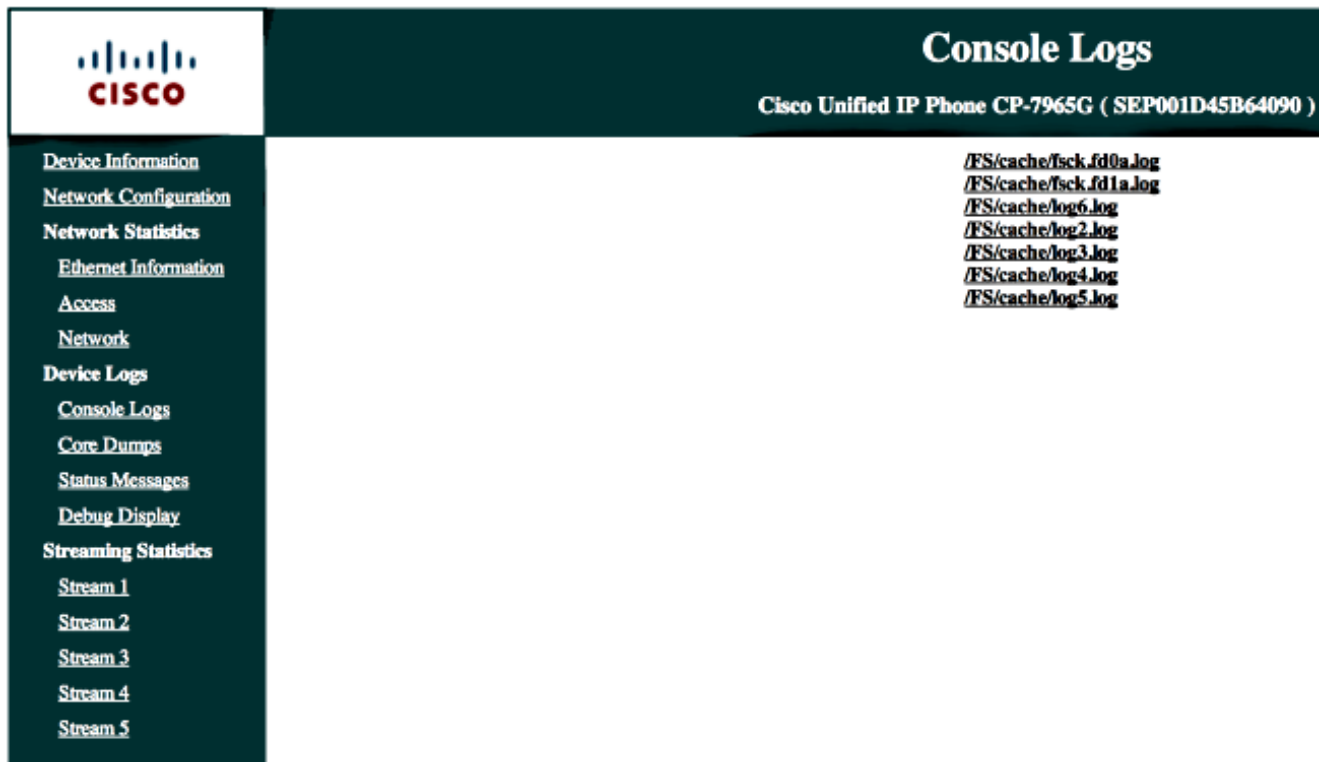
Crypto PKI Msg debugging is on  
Crypto PKI Trans debugging is on  
Crypto PKI Validation Path debugging is on

## Debug dal telefono

1. Selezionare **Periferica > Telefono** da CUCM.
2. Nella pagina di configurazione del dispositivo, impostare Accesso Web su **Abilitato**.
3. Fare clic su **Save** (Salva), quindi su **Apply Config** (Applica configurazione).



4. Da un browser, immettere l'indirizzo IP del telefono e scegliere **Console Logs** dal menu a sinistra.



5. Scaricare tutti i file **/FS/cache/log\*.log**. I file di registro della console contengono informazioni sul motivo per cui il telefono non riesce a connettersi alla VPN.

## Bug correlati

ID bug Cisco [CSCty46387](#) , IOS SSLVPN: Miglioramento per impostare un contesto come predefinito

ID bug Cisco [CSCty46436](#) , IOS SSLVPN: Miglioramento del comportamento di convalida dei certificati client