# Configurazione di AnyConnect VPN Phone con autenticazione certificato su un'ASA

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Tipi di certificato telefono Configurazione Configurazioni Verifica Risoluzione dei problemi Informazioni correlate

## Introduzione

In questo documento viene fornito un esempio di configurazione che mostra come configurare le appliance ASA (Adaptive Security Appliance) e i dispositivi CallManager per fornire l'autenticazione dei certificati per i client AnyConnect che vengono eseguiti sui telefoni IP Cisco. Al termine della configurazione, i Cisco IP Phone possono stabilire connessioni VPN all'appliance ASA che usano i certificati per proteggere la comunicazione.

## Prerequisiti

### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Licenza SSL AnyConnect Premium
- Licenza AnyConnect per VPN Phone Cisco

A seconda della versione ASA, viene visualizzato "AnyConnect per Linksys phone" per ASA versione 8.0.x o "AnyConnect per Cisco VPN Phone" per ASA versione 8.2.x o successive.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- ASA versione 8.0(4) o successive
- Modelli IP Phone 7942 / 7962 / 7945 / 7965 / 7975
- Telefoni 8961/9951/9971 con firmware versione 9.1(1)
- Telefono: versione 9.0(2)SR1S Skinny Call Control Protocol (SCCP) o successive
- Cisco Unified Communications Manager (CUCM) Versione 8.0.1.100000-4 o successive

Le versioni utilizzate in questo esempio di configurazione includono:

- ASA release 9.1(1)
- CallManager Release 8.5.1.10000-26

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 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.

### Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

## Tipi di certificato telefono

Cisco utilizza questi tipi di certificati nei telefoni:

- MIC (Manufacturer Installed Certificate) I MIC sono inclusi su tutti i telefoni IP 7941, 7961 e modelli più recenti di Cisco. I MIC sono certificati chiave a 2048 bit firmati da Cisco Certificate Authority (CA). Se è presente un MIC, non è necessario installare un LSC (Locally Significant Certificate). 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.
- LSC LSC protegge la connessione tra CUCM e il telefono dopo aver configurato la modalità di protezione 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). Questo è il metodo preferito (rispetto all'uso dei MIC) perché solo i telefoni IP Cisco forniti manualmente da un amministratore possono scaricare e verificare il file CTL.Nota: 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 che utilizzino i MIC per l'autenticazione Transport Layer Security (TLS) o per qualsiasi altro scopo, lo fanno a proprio rischio.

## Configurazione

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

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

#### Configurazioni

Questo documento descrive le seguenti configurazioni:

- Configurazione ASA
- Configurazione di CallManager
- Configurazione VPN su CallManager
- Installazione certificato su telefoni IP

#### **Configurazione ASA**

La configurazione dell'ASA è pressoché identica a quella usata per connettere un computer client AnyConnect all'ASA. Si applicano tuttavia le seguenti restrizioni:

- Il gruppo di tunnel deve avere un URL di gruppo. Questo URL verrà configurato in CM nell'URL del gateway VPN.
- I Criteri di gruppo non devono contenere un tunnel suddiviso.

Questa configurazione utilizza un certificato ASA (autofirmato o di terze parti) configurato e installato in precedenza nell'trustpoint SSL (Secure Sockets Layer) del dispositivo ASA. Per ulteriori informazioni, fare riferimento a questi documenti:

- Configurazione dei certificati digitali
- Esempio di installazione manuale di certificati di terze parti per ASA 8.x da utilizzare con la configurazione di WebVPN
- ASA 8.x: Accesso VPN con il client VPN AnyConnect utilizzando un esempio di configurazione di un certificato autofirmato

La configurazione rilevante dell'ASA è:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

webvpn enable outside anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside

#### Configurazione di CallManager

Per esportare il certificato dall'ASA e importarlo in CallManager come certificato Phone-VPN-Trust, attenersi alla seguente procedura:

- 1. Registrare il certificato generato con CUCM.
- 2. Controllare il certificato utilizzato per SSL. ASA(config)#**show run ssl** ssl trust-point SSL outside
- 3. Esportare il certificato. ASA(config)#crypto ca export SSL identity-certificate Di seguito è riportato il certificato di identità con codifica PEM (Privacy Enhanced Mail): -----BEGIN CERTIFICATE-----ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTM1MzEwWhcNMjMw MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwN1ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1 NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jc15vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1 wsidpQWq1DDrJD1We83L/oqmhkWJ07QfNrGZh0Lv9x0pR7BFpZd1yFyzwAPkoB11 -----END CERTIFICATE----4. Copiare il testo dal terminale e salvarlo come file .pem.
- Accedere a CallManager e scegliere Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust per caricare il file del certificato salvato nel passaggio precedente.

#### Configurazione VPN su CallManager

- 1. Passare a Cisco Unified CM Administration (Amministrazione Cisco Unified CM).
- 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, immettere l'URL del gruppo definito sull'appliance ASA.Nel campo Certificati VPN in questa posizione selezionare il certificato caricato in precedenza in CallManager per spostarlo dall'archivio trust a questa

#### posizione.

System 👻 Call Routing 👻 Media Reso	urces 🔻 Advanced Features 🗶 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻
VPN Gateway Configuration	
🔜 Save 🗙 Delete 📄 Copy	- Add New
Status	
i Status: Ready	
- VPN Gateway Information	
VPN Gateway Name* ASA_Pho	oneVPN
VPN Gateway Description	
VPN Gateway URL <sup>®</sup> https://d	isa5520-c.disco.com/SSL
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: CN=10.198.16.140,unstructuredName=10.198.16.140 ISSUER: CN=10.198.16.140,unstructuredName= 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.disco.com ISSUER: CN=ASA5510-F-IP-PHON
	**
VPN Certificates in this Location*	SUBJECT: unstructuredNerne=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com [SSUER: DC=com,DC=crtec,DC= *
- Save Delete Copy	Add New

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

System - Call Routing - I	Media Resources 🔻	Ad	vanced Features 🔻	Device 🔻	Applic	ation 🔻	User Management	•	Bulk Adminis
VPN Gateway Configura Save X Delete	ntion Copy 🕂 Add		Voice Mail SAF EMCC Intercompany Media Failback	a Services	) ) ) ) )		N Profile		
<b>VPN Gateway Informati</b> VPN Gateway Name <sup>*</sup> VPN Gateway Description	on ASA_PhoneVPN					VP VP	N Group N Gateway N Feature Configurati	on	
VPN Gateway URL*	https://asa5520-c	.cis	co.com/SSL						

 Nel campo Tutti i gateway VPN disponibili selezionare 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.

System ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼ Device ▼ Application ▼ L	lser Mana <u>c</u>
VPN Group Configuration	
🔚 Save 🗶 Delete 📋 Copy 🕂 Add New	
Status	
(1) Status: Ready	
VPN Group Information	
VPN Group Name* ASA_PhoneVPN	
VPN Group Description	
VPN Gateway Information	
All Available VPN Gateways	*
Move the Gateway down	
	*
Selected VPN Gateways in this VPN Group*	

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

System   Call Routing	Media Resources 🔻	Ad	vanced Features 🔻	Device 🔻	Applic	ation 🔻	User Management	•	Bulk Adminis
VPN Group Configurat Save X Delete	tion 🗋 Copy 🛟 Add		Voice Mail SAF EMCC Intercompany Media Fallback	services					
	•		VPN 🕨			VPN Profile			
VPN Group Informati VPN Group Name* VPN Group Description	on ASA_PhoneVPN					∨PI ∨PI ∨PI	N Group N Gateway N Feature Configurat	ion	

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

System 🔻 Call Roo	uting ▼ Media Resources ▼ Advanced Features ▼ Device ▼ Application ▼
VPN Profile Con	figuration
Save 🗶 🕻	elete [ Copy 🕂 Add New
Status	
i Status: Rea	dy
_ ¥PN Profile Inf	ormation —
Name* ASA	_PhoneVPN
Description	
🗖 Enable Auto M	Vetwork Detect
Tunnel Parame	ters
мти*	1290
Fail to Connect*	30
🗖 Enable Host I	D Check
Client Authenti	cation
Client Authentica	tion Method* Certificate 🗸
🗖 Enable Passw	ord Persistence
- Save Dele	te Copy Add New

Attiva rilevamento automatico rete: Se abilitato, il telefono VPN effettua il ping al server TFTP e, se non riceve alcuna risposta, avvia automaticamente una connessione VPN.Abilita controllo ID host: Se abilitato, il telefono VPN confronta l'FQDN dell'URL del gateway VPN con il CN/SAN del certificato. Il client non riesce a connettersi se 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.

8. 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

Device 🔻	Application -	User Managem	ent	▼ Bulk Administration ▼ Help ▼
CTI Ro	oute Point			
Gatek	eeper			
Gatev	vay			
Phone				
Trunk				
Remot	te Destination			
Devic	e Settings	÷.		Device Defaults
				Firmware Load Information
				Default Device Profile
				Device Profile
				Phone Button Template
				Softkey Template
				Phone Services
				SIP Profile
				Common Device Configuration
).				Common Phone Profile
em 🔻 Call R	outing 🔻 Media	Resources 🔻	Ad	Ivanced Features 👻 Device 👻 🧍
mon Phon	e Profile Conf	iguration		
Save 🗙	Delete [ Co	opy 🎦 Resi	et	🧷 Apply Config 🕂 Add New
Informat	ion —			
Group AS	A_PhoneVPN			-

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

nfig C	CTI Route Point Gatekeeper Gateway	Related Links: E	ack To Find/Lis
	Phone		
Desc	Trunk	Auto 1000	
Devie	Remote Destination	Default	<u>View Details</u>
	Putten Tomolato*	k None >	<ul> <li>View Details</li> </ul>
Softkey	Template	Standard 7962G SCCP	•
Commo	on Phone Profile*	Standard Common Phone Profile	•

10. Registrare nuovamente il telefono in CallManager per scaricare la nuova configurazione. **Configurazione autenticazione certificato** 

Per configurare l'autenticazione dei certificati, attenersi alla seguente procedura in CallManager e sull'appliance ASA:

- 1. Dalla barra dei menu, scegliere Funzioni avanzate > VPN > Profilo VPN.
- 2. Verificare che il campo Metodo di autenticazione client sia impostato su **Certificato.**

System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 💌 Application	י ד
/PN Profile Configuration	
🔚 Save 🗶 Delete 🕞 Copy 🕂 Add New	
Status	
i Status: Ready	
VPN Profile Information	
Name* ASA_PhoneVPN	
Description	
Enable Auto Network Detect	
Tunnel Parameters	
MTU* 1290	
Fail to Connect* 30	
Enable Host ID Check	
Client Authentication	
Client Authentication Method* Certificate	-

- 3. Accedere a CallManager. Dalla barra dei menu, scegliere Unified OS Administration > Security > Certificate Management > Find.
- Esporta i certificati corretti per il metodo di autenticazione certificato selezionato:MIC: Cisco\_Manufacturing\_CA - Autenticazione dei telefoni IP con un MIC

Find Certificate List where File	Name v begins with v	Find Clear Filter				
Certificate Name	Certificate Type	.ºEM Fle				
tomcat	certs	tomcat.sem				
ipsec	certs	ipcec.pem				
tonneat-trust	trust-certs	CUCM85.pen				
ipsec-trust	trust-certs	CUCM85.pem				
CallManager	certs	CallNanager.pem				
CAPF	certs	CAPF.pem				
TVB	certs	TVS.com				
CallManager-trust	trust-cents	Cisco Nanufacturing CAlpern				
CallManager-trust	trust-cents	CAP-RTP-001.pem				
CallManager-trust	trust-certs	Cisco Root CA 2048.pem				
CallManager-trust	trust-certs	CAPF-18cfD46e.pem				
C allMan ager-trust	trust-certs	CAP-PTP-002.pem				

LCS: Cisco Certificate Authority Proxy Function (CAPF) - Autentica i telefoni IP con un LSC

Certificate Name	Certificate Type	.>EN Tile	
comcat	certs	iomcat.pem	tomczt.der
psec	certs	losec.pam	ipeec.der
omcal-trust	trust-certs	CUCM85.pem	OLCM85.der
psec-trust	trust-certs	CUCM85.perr	CLCN85.der
CallManager	certs	CallManacer.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TV5.pem	TVS.der
CalManager-trust	trust-certs	Cisco Manufacturing CA.pem	

- 5. Trovare il certificato, Cisco\_Manufacturing\_CA o CAPF. Scaricare il file .pem e salvarlo come file .txt
- 6. Creare un nuovo trust point sull'appliance ASA e autenticarlo con il certificato salvato in precedenza. 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. Di seguito è

```
riportato un esempio:
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

<base-64 encoded CA certificate>

quit

7. Verificare che l'autenticazione nel gruppo di tunnel sia impostata sull'autenticazione con certificato.

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

#### Installazione certificato su telefoni IP

I telefoni IP possono funzionare con MIC o LSC, ma il processo di configurazione è diverso per ogni certificato.

#### Installazione MIC

Per impostazione predefinita, tutti i telefoni che supportano VPN sono precaricati con MIC. I telefoni 7960 e 7940 non sono forniti con un MIC e richiedono una procedura di installazione speciale per la registrazione sicura di LSC.

**Nota:** Cisco consiglia di utilizzare i MIC solo per l'installazione di LSC. Cisco supporta gli LCS per autenticare la connessione TLS con CUCM. Poiché i certificati principali MIC possono essere compromessi, i clienti che configurano i telefoni per l'utilizzo dei MIC per l'autenticazione TLS o per qualsiasi altro scopo lo fanno a proprio rischio. Cisco non si assume alcuna responsabilità in caso di compromissione dei MIC.

#### Installazione LSC

- 1. Abilita il servizio CAPF in CUCM.
- Una volta attivato il servizio CAPF, assegnare le istruzioni telefoniche per generare un LSC in CUCM. Accedere a Cisco Unified CM Administration e scegliere Dispositivo > Telefono. Selezionare il telefono configurato.
- 3. Nella sezione Informazioni sulla funzione CAPF (Certificate Authority Proxy Function) verificare che tutte le impostazioni siano corrette e che l'operazione sia impostata su una data

futura.

Certificate Operation*	Install/	Install/Upgrade 👻					
Authentication Mode*	By Authentication String 🗸 🗸						
Authentication String	123456						
Generate String							
Key Size (Bits)*	2048					•	
One of the Constant of Dec	2012	3	10	12	(XXXX:MM:DD:HH)		

- 4. Se la modalità di autenticazione è impostata su Stringa null o Certificato esistente, non sono necessarie ulteriori azioni.
- 5. Se la modalità di autenticazione è impostata su una stringa, selezionare manualmente Impostazioni > Configurazione protezione > \*\*# > LSC > Aggiorna nella console telefonica.

### Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

#### Verifica ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1) AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1) SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : OGroup Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
```

Encapsulation: TLSv1.0 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 1759 Bytes Rx : 799 Pkts Tx : 2 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 57.2 Public IP : 172.16.250.15 Encryption : AES128 Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 50529 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : SSL VPN Client Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 835 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 57.3 Assigned IP : 10.10.10.2 Public IP : 172.16.250.15 Encryption : AES128 Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 51096 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : DTLS VPN Client Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 303255 Bytes Rx : 269270 Pkts Tx : 5642 Pkts Rx : 5649 Pkts Tx Drop : 0 Pkts Rx Drop : 0

#### Verifica CUCM

System 💌	Cal Routi	ng 💌 Medio Resources 👻 Adva	naed Features 👻 Devia	e 🐐 Application 👻	User klanagement 💌 Bulk	Administration 👻 Help 💌	
Find and L	ist Pho	nes					Related Links: Actively Log
Add Ne	ew 📕	Select All 🌐 Geer Al 🗮 0	alate Salacted 🛛 🐴 Res	sel Selactad 🧷 App	aly Config to Selected		
Status (1) 4 rect	ords tou	nd					
Find Phone	where	Device Name	★ begins with ★ S	elect item or enter s	Find Clear fil search text 👻	ter 🕹 😑	IP Phone registered with the CUCM using VPN address
		Device Name(Line) *	Description	Device Pool	Desice Protocol	Status	CP Address
E 8		84 <b></b>	Auto 1001	Default	SCOP	Unknown	Unknown
1 2		SEPERATOR	Auto 1000	Default	SCCP (	Registered with 192,168,100.1	10.10.10.2

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

#### Bug correlati

 Cisco bug ID <u>CSCtf09529</u>, aggiungere il supporto per la funzionalità VPN in CUCM per telefoni 8961, 9951, 9971

- Cisco ID bug <u>CSCuc71462</u>, il failover della VPN per telefono IP richiede 8 minuti
- ID bug Cisco CSCtz42052, supporto VPN IP Phone SSL per numeri di porta non predefiniti
- Cisco bug ID <u>CSCth96551</u>, non tutti i caratteri ASCII sono supportati durante il login della VPN del telefono con utente e password.
- ID bug Cisco CSCuj71475, è necessaria una voce TFTP manuale per la VPN IP Phone
- Cisco ID bug <u>CSCum10683</u>, IP phone non registrano chiamate perse, effettuate o ricevute

### Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems