

# Informazioni generali per la registrazione/annullamento della registrazione del telefono IP CUCM

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Domande importanti](#)

[Dati dal telefono](#)

[Dati Dello Switch](#)

[Dati del CUCM](#)

[Esaminare Le Note Telefoniche](#)

[Esaminare i registri CUCM](#)

[Collegamenti aggiuntivi](#)

[Registri e PCAP per applicazioni pratiche](#)

## Introduzione

Questo documento descrive le informazioni generali da raccogliere sui Cisco IP Phone che hanno problemi di registrazione quando vengono integrati con Cisco Unified Communications Manager (CUCM). In questo documento non viene descritta la procedura per la risoluzione di problemi specifici.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo Internet (IP)
- Protocolli di segnalazione VOIP (Voice Over Internet Protocol)
- Il processo di registrazione per i Cisco IP Phone

**NOTA:** Il [processo di registrazione di telefoni IP, SCCP e SIP con CUCM](#) è un ottimo documento da rivedere.

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

# Domande importanti

- I telefoni non registrati sono in grado di effettuare e ricevere chiamate? In caso affermativo, controllare lo stato di registrazione dalla pagina Web degli altri nodi CUCM e lo stato del telefono nel controller di dominio RIS.

**NOTA:** Se i telefoni sono in grado di effettuare e ricevere chiamate, utilizzare il comando seguente su ogni nodo per visualizzare lo stato del telefono nel controller di dominio Servizi di installazione remota.

**show risdb query phone**

Se il problema viene considerato come falso, riavviare il servizio controller di dominio RIS. A causa dell'architettura del controller di dominio RIS potrebbe essere necessario riavviare anche il servizio CallManager.

- Quanti telefoni sono interessati e qual è il numero totale di telefoni?
- Se il problema riguarda solo un sottoinsieme di telefoni, cosa hanno in comune (ad esempio modello, protocollo, versione firmware, sullo stesso switch/blade, nello stesso sito...)?
- Il telefono ha una linea condivisa?
- I telefoni sono collegati alla rete tramite una VPN (Virtual Private Network)?
- Il problema si verifica sempre alla stessa ora del giorno?
- Sono stati eseguiti controlli di sicurezza nella rete (ad esempio scanner delle porte)?
- Avete dei firewall tra il telefono e il CUCM?
- Stai eseguendo un'ispezione SIP su qualsiasi dispositivo nel percorso tra il telefono e il CUCM?
- Quanti telefoni si trovano nella stessa subnet e quanti indirizzi IP sono disponibili per il lease nella subnet?
- È configurato l'utilizzo del SIP (Session Initiation Protocol) sul TCP (Transmission Control Protocol) o UDP (User Datagram Protocol)?
- I telefoni utilizzano un profilo di sicurezza del dispositivo sicuro o non sicuro? Se i telefoni dispongono di un profilo protetto, è stato installato un LSC (Locally Significant Certificate) prima di applicare il profilo protetto alla configurazione del telefono?

**NOTA:** I telefoni non verranno registrati se utilizzano un profilo di sicurezza Decive protetto senza un LSC installato. Per ulteriori informazioni, consultare il documento [CUCM Generating LSC Certificates for Secure Phone](#).

- Qualcuno ha effettuato l'accesso al telefono o ai telefoni con problemi tramite la mobilità degli interni? In caso affermativo, il protocollo (SCCP/SIP) del profilo del dispositivo corrisponde a quello del telefono e si verifica lo stesso comportamento dopo la disconnessione?

- È cambiato qualcosa? Qualunque cosa, a prescindere da quanto possa essere significativo il cambiamento e a prescindere da cosa sia stato. Tutte le nuove modifiche (nuove configurazioni, nuovo software, nuovo hardware) devono essere confermate.

## Dati dal telefono

- Documentare il messaggio sullo schermo del telefono quando si verifica il problema. È normale che un messaggio venga visualizzato sullo schermo del telefono, quindi accertarsi di controllare.
- Verificare se nel telefono è installato un LSC, poiché è necessario se il cliente utilizza un profilo di sicurezza del dispositivo sicuro

**79 XX**

Premere il pulsante delle impostazioni sul telefono > pulsante del tastierino numerico 4 > pulsante del tastierino numerico 4 di nuovo > documentare se LSC dice installato o non installato

**78XX / 88XX / 99XX**

Premere il pulsante Settings (Impostazioni) sul telefono > selezionare Admin Settings (Impostazioni di amministrazione) > premere il tasto Key (Tastierino numerico) numero 2 > documentare se LSC indica installato o meno

- [Acquisisci un pacchetto \(pcap\) dal telefono](#)

**SUGGERIMENTO:** La maggior parte delle informazioni riportate di seguito richiede l'attivazione dell'**accesso Web** tramite telefono. Anche se il telefono non è registrato, è possibile modificarne le impostazioni per abilitare l'accesso al **Web**, **passare alla porta PC** e quindi tentare di accedere alla pagina Web **tramite SSH**.

**NOTA:** Controllare il campo **Expires** (Scadenza) nel messaggio SIP register (registro SIP) trovato nella capsula se i telefoni stanno usando il SIP.

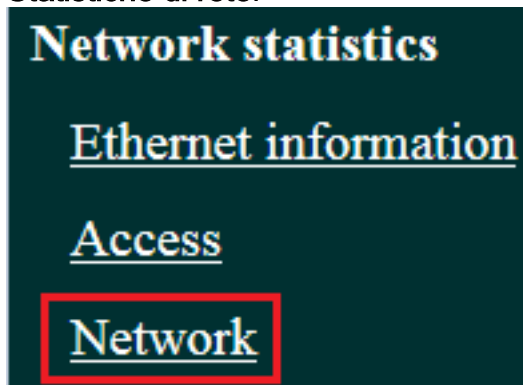
Il valore predefinito per il campo **Scade** quando il messaggio **REGISTER** viene inviato dal telefono al CallManager primario è 120 secondi. Quando il telefono invia un messaggio REGISTER, noto come messaggio keep alive. sul server secondario di CallManager, il campo scade è 0.

- Documentare i messaggi di debug sul telefono
- Cerca core nel telefono e scaricali se ci sono. Assicurarsi inoltre di raccogliere l'output di show **core-dump** dalla CLI del telefono se i core sono stati trovati sull'interfaccia Web del telefono.

**NOTA:** A partire dal 9 novembre 2016 solo gli sviluppatori del telefono hanno accesso allo strumento per la revisione dei file di base del telefono. Se è necessaria un'ulteriore analisi del core, aprire una richiesta TAC (Technical Assistance Center) per coinvolgere gli sviluppatori del telefono.

- Raccogliere le informazioni sui **router adiacenti CDP** dalla pagina **Rete** nella sezione

Statistiche di rete.



CDP Neighbor device ID	rtp12-pkinane-sw.cisco.com
CDP Neighbor IP address	14.48.38.251
CDP Neighbor IPv6 address	
CDP Neighbor port	FastEthernet0/5

- [Scarica i registri della console dal telefono](#). Se il telefono supporta la funzione [Report di problema \(PRT\)](#), si consiglia di utilizzare la PRT.

**NOTA:** Questo [documento del forum di supporto](#) mostra come usare **strace** per stampare i debug sul terminale; tuttavia, potrebbe essere necessario utilizzare **show strace**.

Alcuni telefoni usano **dump** invece di **strace** o **show strace**.

I comandi **strace** o **sdump** sono simili a quelli che si digitano **terminal monitor** su un router Cisco.

**SUGGERIMENTO:** È meglio raccogliere i log della console dall'interfaccia della riga di comando (CLI) del telefono in quanto molti telefoni hanno spazio limitato e i loro log vengono sovrascritti rapidamente.

Se il telefono dispone di una porta ausiliaria, [collegare un cavo console al telefono](#) per acquisire i debug anche se il telefono si riavvia.

**SUGGERIMENTO:** È consigliabile registrare la sessione terminale in un file di testo. Di seguito viene riportata la procedura per accedere a un file di testo con [putty](#) e la procedura per eseguire questa operazione con [SecureCRT](#).

## Dati Dello Switch

Il telefono accede alla rete tramite uno switch. Identificare lo switch a cui è collegato il telefono e raccogliere i dati elencati di seguito.

- Raccogliere la configurazione in esecuzione utilizzando **show run**

- Raccogli **hist CPU proc**.
- Raccogliere l'output di **show log**

## Dati del CUCM

- Ottenere il numero di directory (DN) del telefono.

**NOTA:** Se non è presente alcun DN e il telefono utilizza il SIP (Session Initiation Protocol), il telefono non verrà registrato.

- [Scarica il file di configurazione del telefono](#)
- [Recupera pcaps dai server CUCM](#)
- Utilizzare lo strumento di monitoraggio in tempo reale (RTMT, Real Time Monitoring Tool) per raccogliere i registri e il pcap dai server CUCM. Accertarsi di selezionare tutti i server durante la raccolta dei registri.

**SUGGERIMENTO:** A seconda dell'ambiente o dei sintomi, è possibile raccogliere alcuni o tutti i tipi di log riportati di seguito.

Cisco CallManager, funzione proxy Cisco Certificate Authority, Cisco Tftp, Cisco Trust Verification Service, Event Viewer-Application Log, Event Viewer-System Log e Packet Capture Log.

- Raccogliere l'output di **show itl** e **show ctl** da tutti i server TFTP nel cluster CUCM.
- Raccogliere l'output di questi comandi dall'editore CUCM:  
Determinare se il cluster è in modalità mista:

**eseguire sql select nomeparam,valoreparam da processconfig dove nomeparam='ModalitàProtezioneCluster'**

Determinare se il parametro di rollback è impostato su true:

**esegui sql select nomeparam,valoreparam from processconfig where nomeparam='RollBackToPreGrayback'**

Determinare se la replica del database è integra:

**utilizza proprietà runtime di replica**

**NOTA:** Se il cluster non è in modalità mista, l'output sarà simile al seguente:

```
admin:esegui sql select paramname,paramvalue from processconfig where
paramname='ClusterSecurityMode'
nomeparam valore
=====
ModalitàProtezioneCluster 0
```

**NOTA:** Se il parametro di rollback è impostato su false, l'output sarà simile al seguente:

```
admin:esegui selezione sql nomeparam,valoreparam da processconfig dove
nomeparam='RollBackToPreGrayback'
nomeparam valore
=====
RipristinaPrecedenteGraybackF
```

**SUGGERIMENTO:** Per una spiegazione dell'output di `utils dbreplication runtimestate`, esaminare [Comprensione dell'output di utils dbreplication runtimestate per il documento CUCM](#).

## Esaminare Le Note Telefoniche

- Cerca le seguenti stringhe nelle note telefonate:

Non riuscito

Err

Errore

Eccezione

newUnregReason

Lastoutofservice

Fallback

errore socket=

opvlan

JAVA-sipio-

REGISTRATO

Rilevamento rete attività

tftpAddr1=

Bloccato:

VPN: (NOTA: Accertarsi di cercare con regex questo o il "." sarà analizzato come un carattere letterale anziché speciale)

## Esaminare i registri CUCM

Cercare nei registri CUCM:

- Indirizzo MAC del telefono
- Indirizzo IP del telefono

**SUGGERIMENTO:** Se vengono visualizzati messaggi di errore, è possibile che la spiegazione dei codici motivo sia nei [documenti dei messaggi di errore e di sistema](#).

## Collegamenti aggiuntivi

[Domande frequenti sugli endpoint](#)

[Protezione predefinita](#)

[Policy di supporto del firmware per Cisco IP Phone](#)

[Cerca nel repository Cisco Live](#)

## **Registri e PCAP per applicazioni pratiche**

Ho già registrato alcuni telefoni e raccolto i log/pcaps. Per esaminare i file, [fare clic qui](#).