

General Information for CUCM IP Phone Registration/Deregistration Troubleshooting

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Important Questions](#)

[Data From The phone](#)

[Data From The Switch](#)

[Data From The CUCM](#)

[Review The Phone Logs](#)

[Review The CUCM Logs](#)

[Additional Links](#)

[Logs and PCAP For Practical Application](#)

Introduction

This document describes general information to collect for Cisco IP Phones that experience registration issues when integrated with Cisco Unified Communications Manager (CUCM). This document does not explain steps to troubleshoot specific issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Internet Protocol (IP)
- Voice Over Internet Protocol (VOIP) signaling protocols
- The registration process for Cisco IP Phones

NOTE: The [IP Phone, SCCP & SIP Phone Registration Process with CUCM](#) is a great document to review.

Components Used

This document is not restricted to specific software and hardware versions.

Important Questions

- For phones that show unregistered, are they able to make and receive calls? If yes, check the

registration status from the webpage of the other CUCM nodes and check the status of the phone in RIS DC.

NOTE: If the phones are able to make and receive calls use the command below on each node to see the status of the phone in RIS DC.

show risdb query phone

If the issue deemed to be a false status of unregistered, restart the RIS DC service. Due to the architecture of the RIS DC it may be necessary to restart the CallManager service as well.

- How many phones are impacted and what is the total number of phones?
- If only a subset of phones are affected, what do they have in common (i.e. model, protocol, firmware version, on the same switch/blade, at the same site...)?
- Does the phone have a shared line?
- Are the phones connected to the network with a Virtual Private Network (VPN)?
- Does the issue happen at the same time of day each time it happens?
- Are any security checks performed in the network (i.e. port scanners)?
- Do you have any firewalls between the phone and the CUCM?
- Are you doing SIP inspection on any devices in the path between the phone and the CUCM?
- How many phones are in the same subnet and how many IP addresses are available for lease to that subnet?
- Are configured to use Session Initiation Protocol (SIP) over Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)?
- Are the phones using a secure or non-secure Device Security Profile? If the phones have a secure profile, did they have an Locally Significant Certificate (LSC) installed before applying the secure profile to the phone's configuration?

NOTE: Phones will not register if they are using a secure Device Security Profile without an LSC installed. Refer to the [CUCM Generating LSC Certificates for Secure Phones](#) document for more information.

- Is anyone logged into the problem phone(s) via extension mobility? If yes, does the protocol (SCCP/SIP) of the device profile match that of the phone and does the same behavior exist after logging out?
- Did anything change? Anything at all, regardless of how significant the change might be and regardless of what the change was. Any and all new changes (new configurations, new software, new hardware) should be acknowledged.

Data From The phone

- Document the message on the phone's screen when the issue occurs. It is typical for a message to be displayed on the phone's screen so be sure to check this.
- Check to see if the phone has an LSC installed as this is required if the customer is using a secure Device Security Profile

79XX

Press the settings button on the phone > push keypad button number 4 > push keypad button number 4 again > document whether the LSC says installed or not installed

78XX / 88XX / 99XX

Press the settings button on the phone > select Admin Settings > push keypad button number 2 > document whether the LSC says installed or not installed

- [Get a packet capture \(pcap\) from the phone](#)

TIP: Much of the information below this point requires **web access** to be enabled on the phone. Even if a phone isn't registered it may be possible to modify the settings on the phone so enable **webaccess**, **span to pc port**, and **SSH Access** then attempt to access the web page.

NOTE: Check the **Expires** field in the SIP register message found in the pcap if the phones are using SIP.

The default value for the **Expires** field when the **REGISTER** message is sent from the phone to the primary CallManager is 120 seconds. When the phone is sending a REGISTER message, known as a "keep alive" message, to its secondary CallManager server the expires field is 0.

- Document the debug messages on the phone
- Check for cores on the phone and download them if they are there. Be sure to also gather the output of show **show core-dump** from the CLI of the phone if cores were found on the web interface of the phone.

NOTE: As of November 9th, 2016 only the phone developers have access to the tool for reviewing phone core files. If further analysis of the core is needed, open a Technical Assistance Center (TAC) case in order to engage the phone developers.

- Gather the **CDP Neighbor** information from the **Network** page located in the **Network statistics** section

Network statistics

Ethernet information

Access

Network

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

- [Get the console logs from the phone](#). If the phone supports the [Problem Report Tool \(PRT\)](#) feature it is recommended to use the PRT.

NOTE: This [support forum document](#) displays how to use **strace** to print the debugs to the terminal; however, you may need to use **show strace**.

Some phones use **sdump** instead of **strace** or **show strace**.

strace or **sdump** commands are like typing **terminal monitor** on a Cisco router.

TIP: It is best to gather the console logs from the Command Line Interface (CLI) of the phone as many phones have limited space and their logs are overwritten quickly.

If the phone has an auxiliary port, [plug a console cable into the phone](#) for capturing debugs even if the phone reboots.

TIP: It is best to log your terminal session to a text file. Here is how to do log to a text file with [putty](#) and here is how to do it with [SecureCRT](#).

Data From The Switch

The phone accesses the network via a switch. Identify the switch the phone is attached to and gather the data listed below.

- Gather **running configuration** using **show run**
- Gather **show proc cpu hist**
- Gather the output of **show log**

Data From The CUCM

- Get the directory number (DN) of the phone.

NOTE: If there is no DN and the phone uses the Session Initiation Protocol (SIP), the phone will not register.

- [Get the phone's configuration file](#)

- [Get pcaps from the CUCM servers](#)

- Use the Real Time Monitoring Tool (RTMT) to collect logs and the pcap from the CUCM servers. Be sure to select all servers when collecting the logs.

TIP: Depending on the environment/symptoms you may want to collect some or all of the following log types:

Cisco CallManager, Cisco Certificate Authority Proxy Function, Cisco Tftp, Cisco Trust Verification Service, Event Viewer-Application Log, Event Viewer-System Log, and Packet Capture Logs.

- Gather the output of **show itl** and **show ctl** from all TFTP servers in the CUCM cluster.

- Gather the output of these commands from the CUCM publisher:

Determine if the cluster is in mixed-mode:

```
run sql select paramname,paramvalue from processconfig where  
paramname='ClusterSecurityMode'
```

Determine if the rollback parameter is set to true:

```
run sql select paramname,paramvalue from processconfig where  
paramname='RollBackToPreGrayback'
```

Determine if database replication is healthy:

```
utils dbreplication runtimestate
```

NOTE: If the cluster is not in mixed-mode, the output will look like this:

```
admin:run sql select paramname,paramvalue from processconfig where  
paramname='ClusterSecurityMode'  
paramname paramvalue  
===== =====  
ClusterSecurityMode 0
```

NOTE: If the rollback parameter is set to false, the output will look like this:

```
admin:run sql select paramname,paramvalue from processconfig where  
paramname='RollBackToPreGrayback'  
paramname paramvalue
```

=====
RollBackToPreGrayback F

TIP: For an explanation of the output from `utils dbreplication runtimestate` review the [Understanding the output of utils dbreplication runtimestate for CUCM](#) document.

Review The Phone Logs

- Search the phone logs for these strings:

Fail

Err

Error

Exception

newUnregReason=

Lastoutofservice

Fallback

socket error=

opvvlan

JAVA-sipio-

REGISTERED

Network_detect_change_task

tftpAddr1=

Locked out:

VPN.: (NOTE: Make sure you are searching with regex for this one or the "." will be analyzed as a literal instead of a special character)

Review The CUCM Logs

Search the CUCM logs for the following:

- The MAC address of the phone
- The IP address of the phone

TIP: If you see error messages the explanation of the reason codes may be in the [Error and System Messages Documents](#).

Additional Links

[Endpoints FAQ](#)

[Security By Default](#)

[Cisco IP Phone Firmware Support Policy](#)

[Search the Cisco Live repository](#)

Logs and PCAP For Practical Application

I already registered some phones and collected the logs/pcaps. To review the files [click here](#).