Troubleshoot MPP Phone in WxC for Provision and Registration

Contents

Introduction

This document describes how to troubleshoot MPP phones in WxC for provision and registration issues when the device is added by MAC Address.

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Network knowledge
- MPP phones

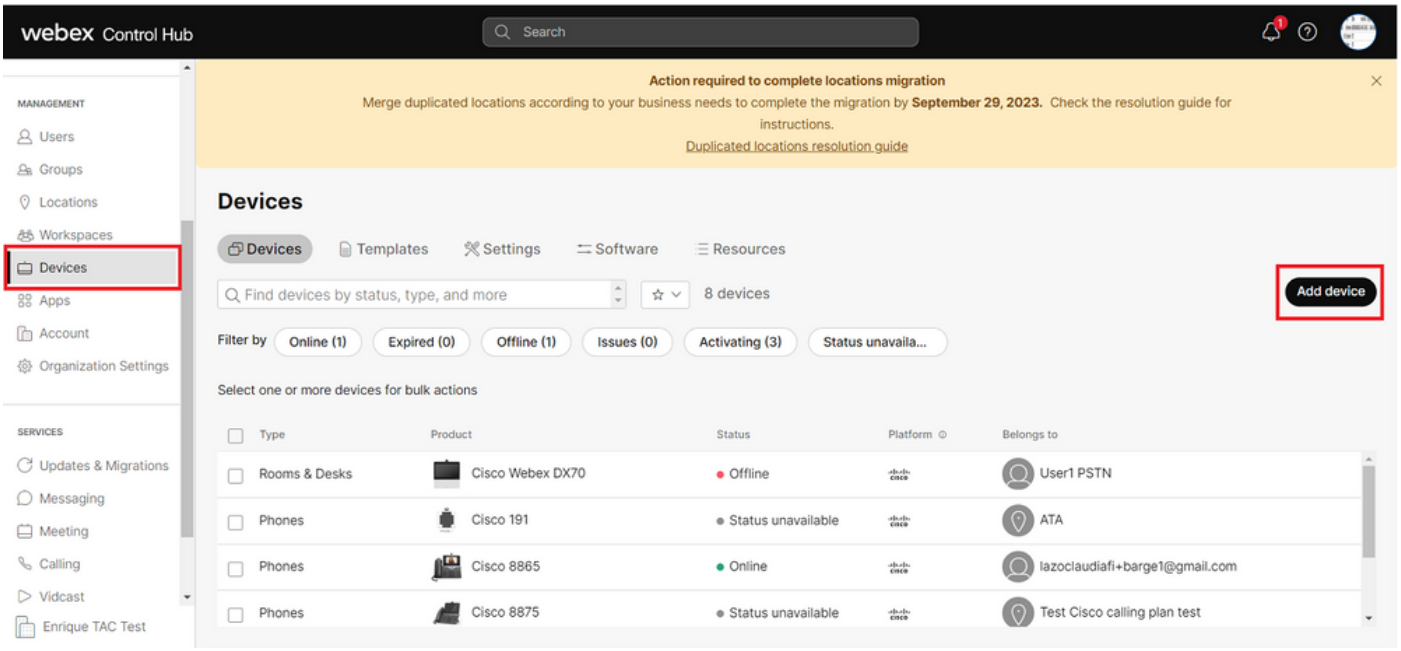
Components Used

The information in this document is based only on MPP Phones such as 78XX, 88XX.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

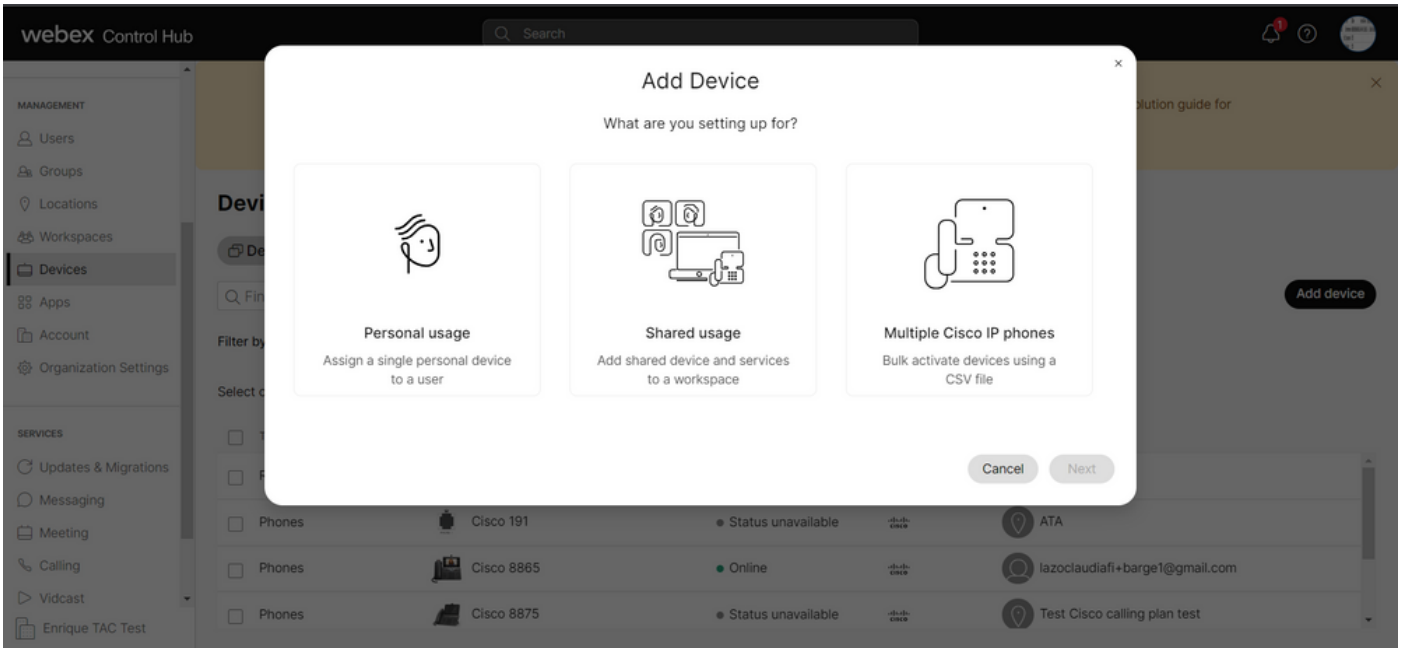
Add the Device in Control Hub

Step 1. Navigate to admin.webex.com and use the admin credentials. In the organization, navigate to **Devices > Add device**:



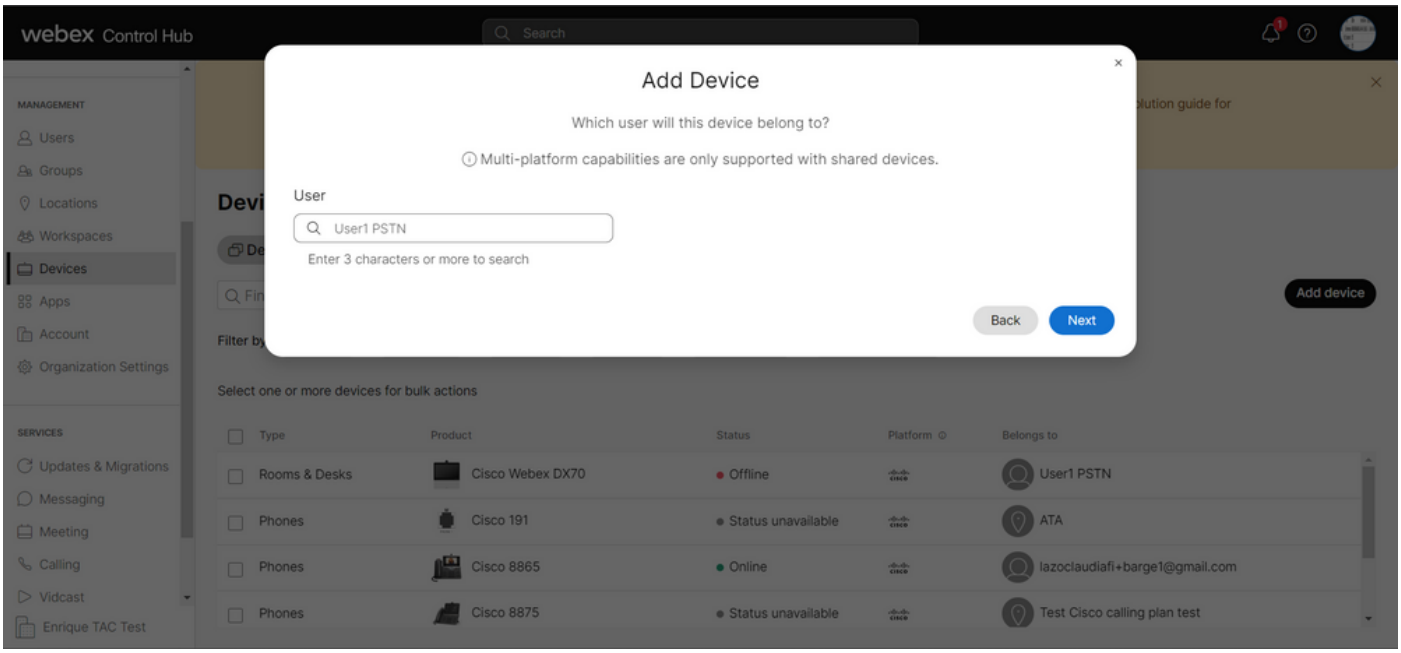
Devices tab

Step 2. Select **Personal usage** to be assigned to a user or select **Shared Usage** to be assigned for a workspace. (In this scenario a user is used.)



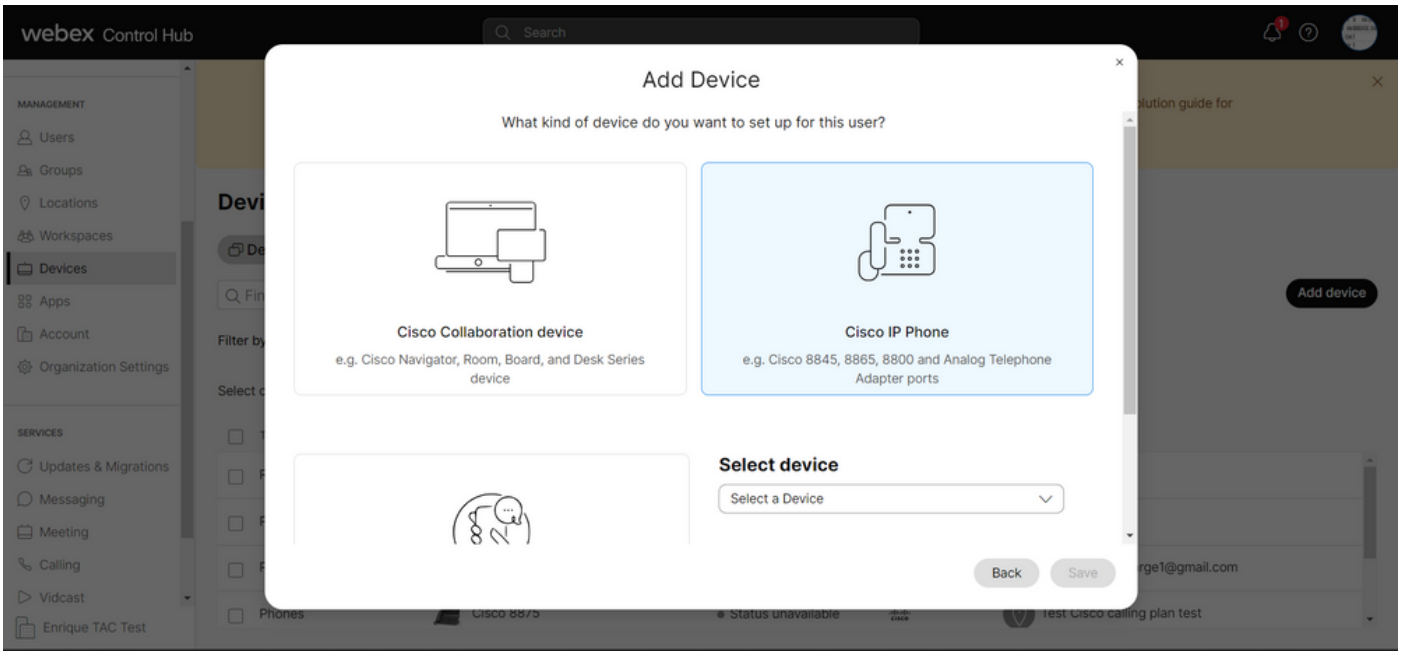
Add device

Step 3. Search and select the user that you want to assign to this device and click on **Next**:



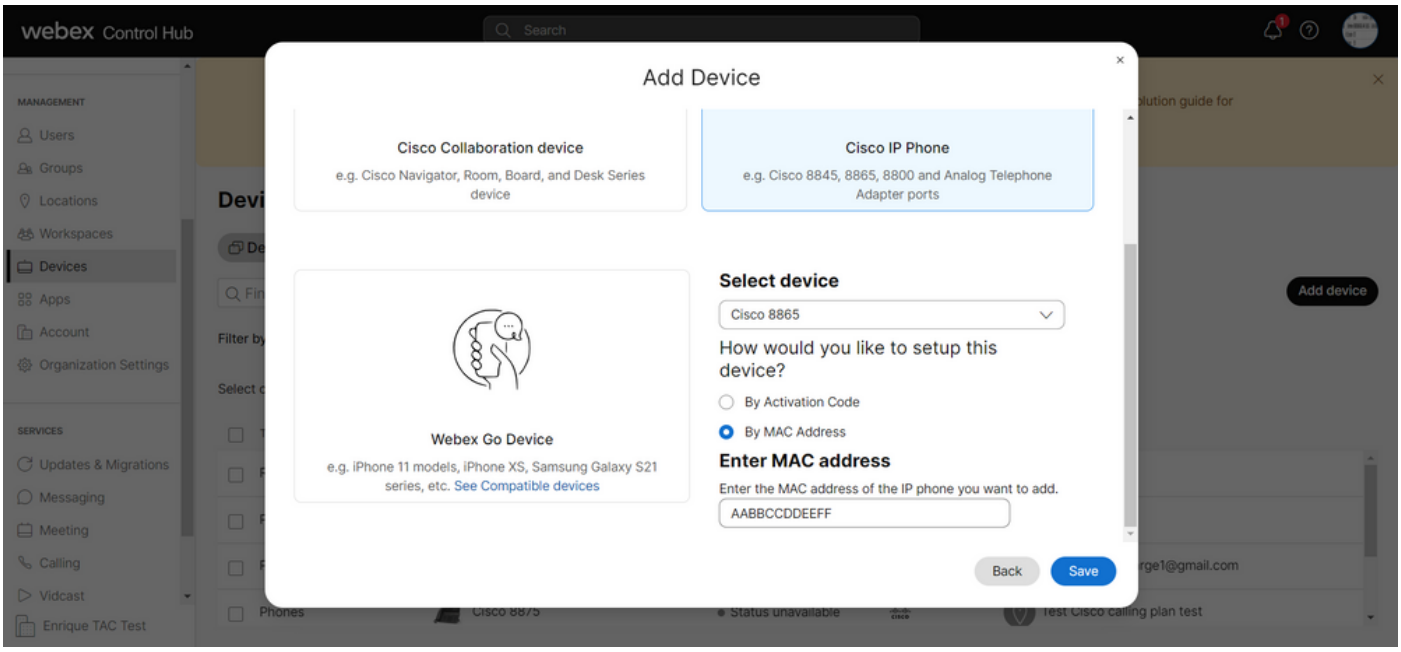
Search for a user

Step 4. Select **Cisco IP Phone** and search for your device model:



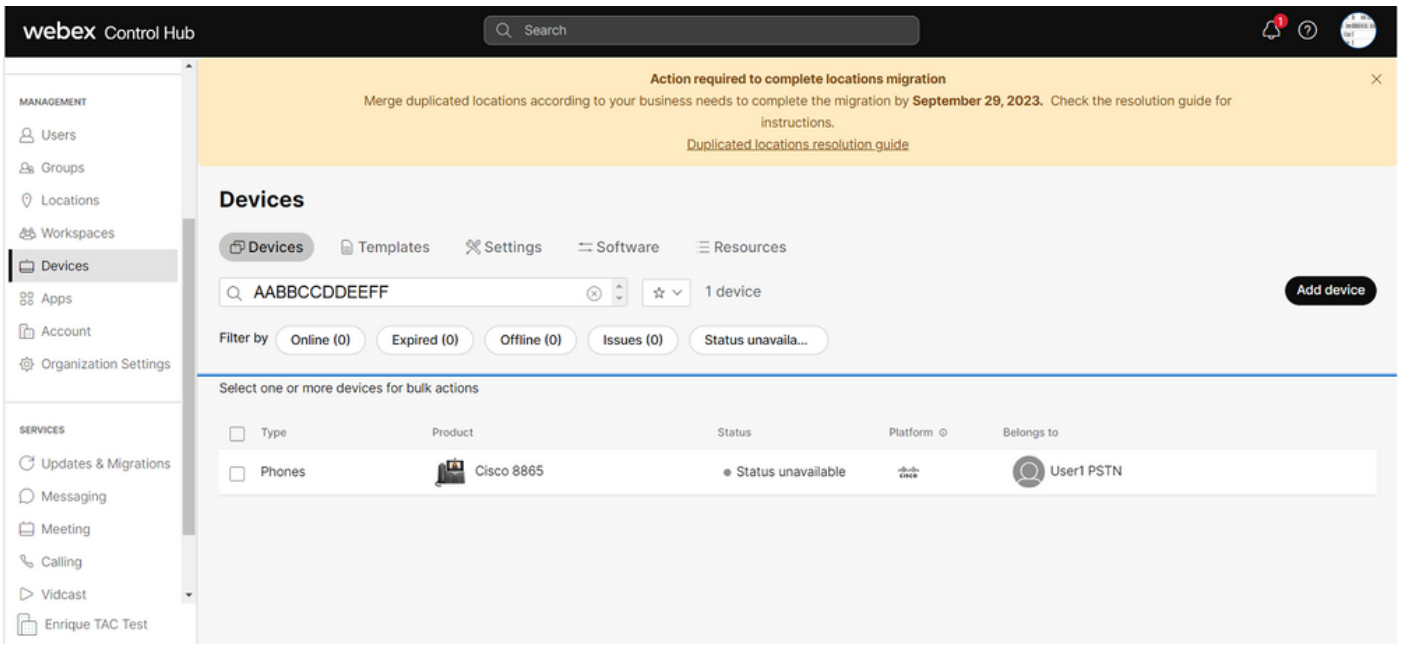
Select model of device

Step 5. Once the device is selected, select the option **By MAC Address** and enter the MAC Address of the device and click **Save**:



Add MAC Address

Step 6. Once the device is in Control Hub, you can verify that was added correctly when you search the MAC Address in the search bar:

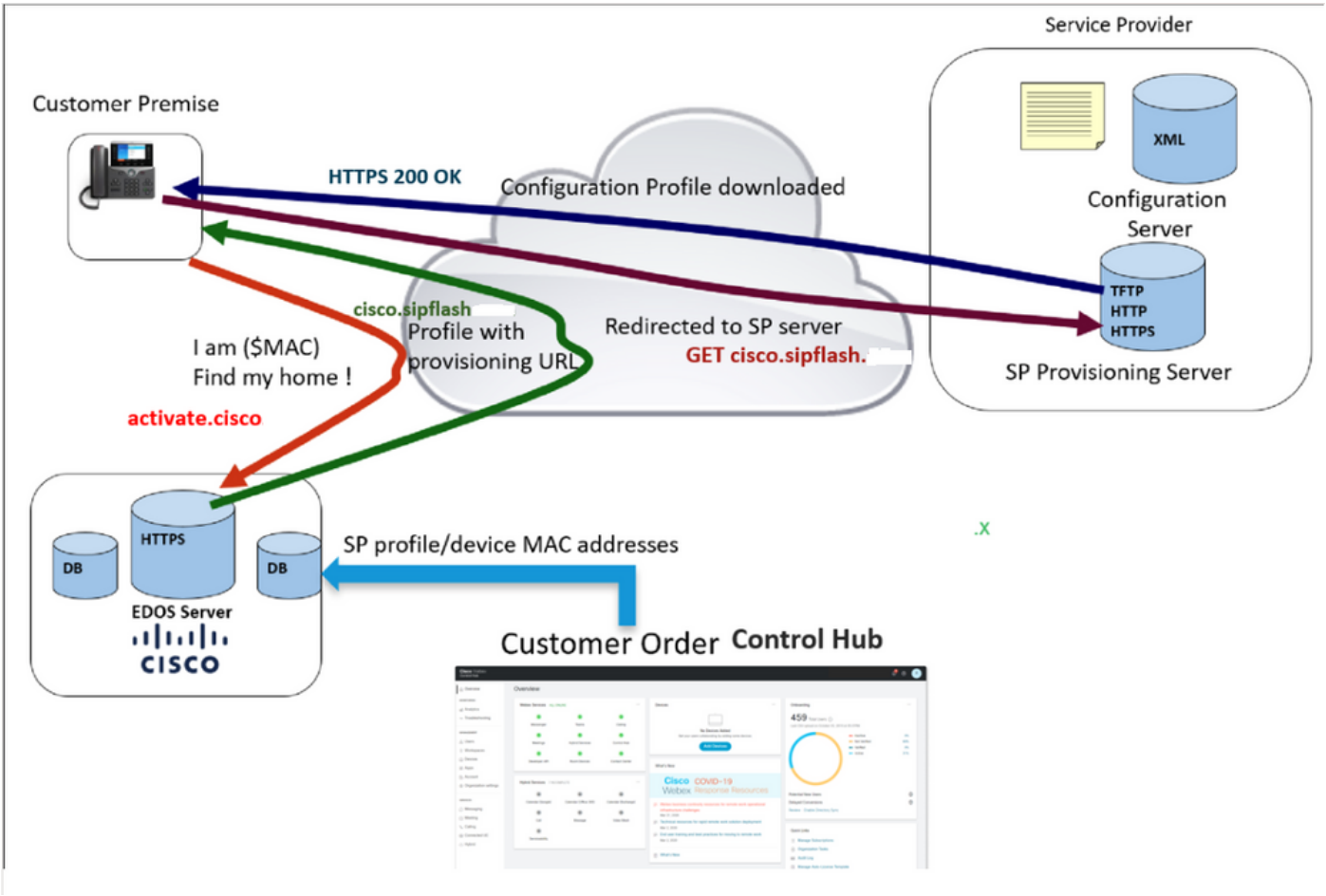


Verification of device

The status shows as "Unavailable" since the device is still not provisioned. Once the device is in Control Hub, the next step is to factory reset the device. After the factory reset, the device must make a request to the WxC servers to get config files. (That is the provision process.) The device is provisioned successfully when the device displays the phone number and/or the extension in the screen.

If you see that the device is not showing the proper configuration, the process for provision the device failed.

Brief Summary of the Process for Provision a Device in WxC



Provisioning diagram

Troubleshoot the process for Provision a Device in WxC

The MPP device can not provision with WxC if it is configured with:

- A TFTP server configured in the DHCP server
- If Option (OPT66, OPT160, OPT159 or OPT150) is configured and provided by the DHCP Server

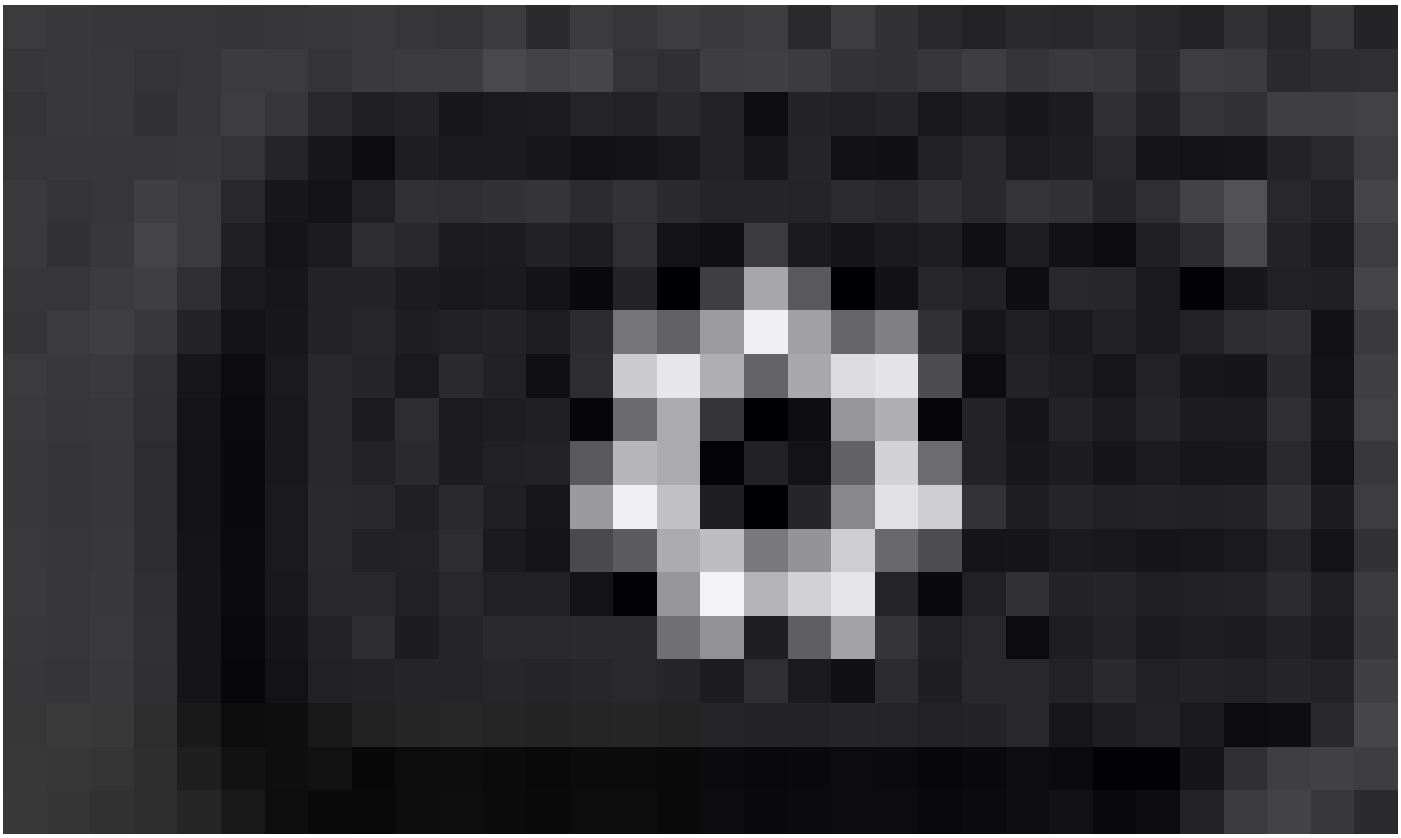
To see if the phone took a TFTP configuration from a DHCP server, the PRT logs are needed.

Genereate the PRT logs from an MPP device

Submit from the PRT logs from the phone. The next steps shows how to generate the PRT logs.

Generate the PRT from the Device

Step 1.On the device, press the**Applications**button



Settings button

.

Step 2.Go to**Status > Report Problem.**

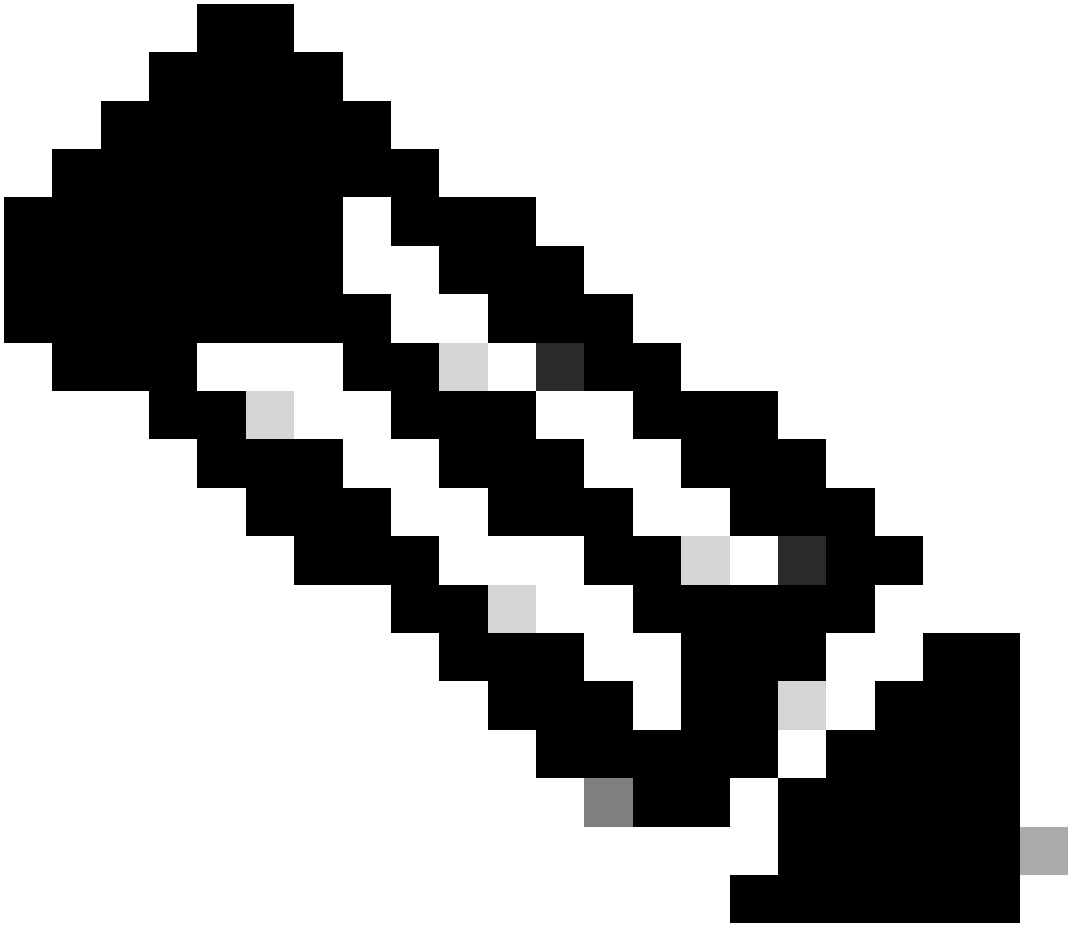
Step 3**.**Enter Date and Time of the problem.

Step 4.Select a Description from the list.

Step 5.Press**Submit.**

Once the logs are submitted, see the next steps to download the PRT logs:

Step 1. Login to https://IP_ADDRESS_PHONE/



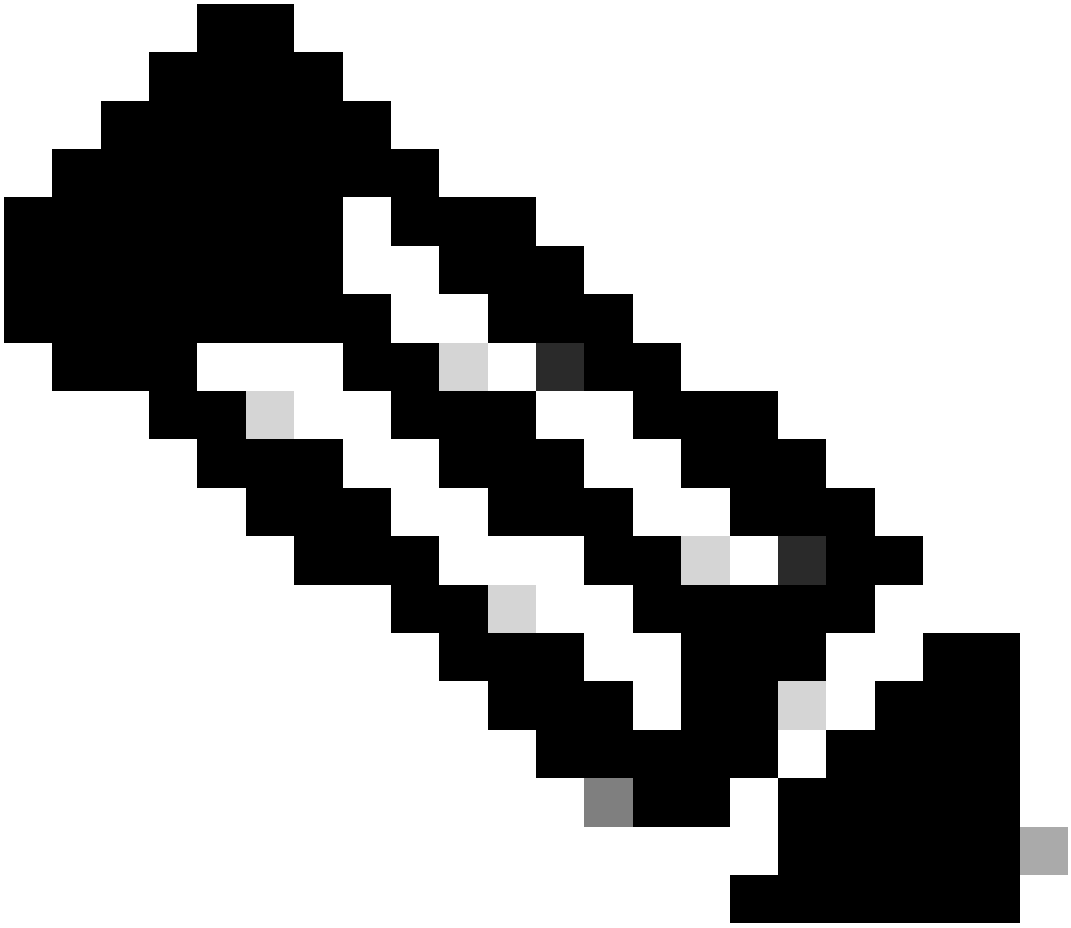
Note: Note: If the IP Address is unknown, it can be obtained from **Settings > Status > Network Status > IPv4 Status**

Step 2. Navigate to **Info > Debug Info >** Download the PRT log (Right click on the link and select **Save As...**)

Web GUI

PRT logs

When you open the logs, you can see a view like this:



Note: You can open the logs with a program like WinRAR since the logs are compressed.

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
.	774,619	?	File folder	5/10/2023 11:0...	
.\cert	1,627	?	File folder	5/10/2023 11:0...	
.\archive.tar.gz	133	?	WinRAR archive	5/10/2023 11:0...	
.\backtraces.tar.gz	75	?	WinRAR archive	5/10/2023 11:0...	
.\messages.tar.gz	74,437	?	WinRAR archive	5/10/2023 11:0...	
.\cfg.xml	126,544	?	XML Document	5/10/2023 11:0...	
.\description-20230510-100139.log	344	?	Text Document	5/10/2023 11:0...	
.\logcat-20230510-170152.log	427,496	?	Text Document	5/10/2023 11:0...	
.\net.cfg	1,001	?	CFG File	5/10/2023 11:0...	
.\show-output-20230510-100139.log	65,669	?	Text Document	5/10/2023 11:0...	
.\status.xml	13,594	?	XML Document	5/10/2023 11:0...	
.\usrlog_kernel_cur_boot.log	32,343	?	Text Document	5/10/2023 11:0...	
.\usrlog_kernel_prev_boot.log	31,000	?	Text Document	5/10/2023 11:0...	
.\webex_service_status.json	356	?	JSON File	5/10/2023 11:0...	

PRT Log view

In order to analyze the process for provision the device, the log called **logcat** needs to be opened. It can be

opened with a text editor like **Notepad** or **Notepad++**.
The function "Find" from the text editor can be used in order to find if the phone has an TFTP server configured. Use **DHCP-tftpsvr1** or **DHCP-tftpsvr2** to find the specific line for that log. If you take a look and the other lines of the logs, more information about the DHCP configuration can be found:

```
2154 NOT Aug 10 16:58:12.226653 (689-695) DHCP-IP Address: 192.168.238.1
2155 NOT Aug 10 16:58:12.226688 (689-695) DHCP-Subnet Mask: 255.255.255.0
2156 NOT Aug 10 16:58:12.226702 (689-695) DHCP-Default Gwy: 192.168.238.240
2157 NOT Aug 10 16:58:12.226734 (689-695) DHCP- ******** dhcpConvConfToExtOptionFile(): Usin
2158 NOT Aug 10 16:58:12.226790 (689-695) DHCP-hostname:SEP14A2A0E0837A
2159 NOT Aug 10 16:58:12.226835 (689-695) DHCP-ipaddr:192.168.238.1
2160 NOT Aug 10 16:58:12.226858 (689-695) DHCP-netmask:255.255.255.0
2161 NOT Aug 10 16:58:12.226878 (689-695) DHCP-router1:192.168.238.240
2162 NOT Aug 10 16:58:12.226894 (689-695) DHCP-domain:
2163 NOT Aug 10 16:58:12.226911 (689-695) DHCP-ntpsvr1:0.0.0.0
2164 NOT Aug 10 16:58:12.226929 (689-695) DHCP-ntpsvr2:0.0.0.0
2165 NOT Aug 10 16:58:12.226947 (689-695) DHCP-tftpsvr1:192.168.150.20
2166 NOT Aug 10 16:58:12.226966 (689-695) DHCP-tftpsvr2:0.0.0.0
2167 NOT Aug 10 16:58:12.226983 (689-695) DHCP-dns1:172.25.6.14
2168 NOT Aug 10 16:58:12.227001 (689-695) DHCP-dns2:172.25.10.31
2169 NOT Aug 10 16:58:12.227017 (689-695) DHCP-option160:
2170 NOT Aug 10 16:58:12.227032 (689-695) DHCP-option159:
2171 NOT Aug 10 16:58:12.227047 (689-695) DHCP-option125:
2172 NOT Aug 10 16:58:12.227061 (689-695) DHCP-option66:
```

As you can see in the log, a TFTP IP Address is configured in the DHCP server. This cause that the phone tried to provision to this TFTP server instead of the Webex Calling servers.

```
3677 NOT Aug 10 16:58:50.718451 (823-940) voice-fapp-Provisioning using DHCP..
3678 NOT Aug 10 16:58:50.718479 (823-940) voice-FUNCTION:fprv_update, proxy_Config:0
3679 NOT Aug 10 16:58:50.718507 (823-940) voice-fprv_eval_profile_rule assemble url=tftp://192.168.150.
3680 NOT Aug 10 16:58:50.718521 (823-940) voice-DHCP pending acquired=1
3681 NOT Aug 10 16:58:50.718772 (823-940) voice-fapp-[resync] fprv_eval_profile_rule - must resync
3682 NOT Aug 10 16:58:50.721954 (823-940) voice-fapp-CP-8851-3PCC 14:a2:a0:e0:83:7a -- Requesting resyn
```

After remove any TFTP configuration and any OPT configuration from the DHCP server, you must factory reset the device in order to start the process to provision the device with WxC again.
The first attempt that the phone do with the process for provisiong the device is to make a request to the URL activate.cisco.com. The phone makes a query to the DNS server in order to resolve the domain. If the DNS Resolution fail, it can look like this:

<#root>

```
1753 NOT Aug 10 16:56:46.129550 (975-1286) voice-reqByCurlInternal sending http request out..., url: ht
1754 INF Aug 10 16:56:46.142687 dnsmasq[564]: query[A] activate.cisco.com from 127.0.0.1
1755 INF Aug 10 16:56:46.142742 dnsmasq[564]: forwarded activate.cisco.com to 192.168.100.3
1774 NOT Aug 10 16:56:54.146585
```

Couldn't resolve host 'activate.cisco.x'

```
1777 NOT Aug 10 16:56:54.146325 (975-1286) voice-reqByCurlInternal return from http request, [res] = 6
1780 NOT Aug 10 16:56:54.147416 (975-1286) voice-fapp-CP-8865-3PCC <MAC_ADDRESS> -- Resync failed: Down
1781 ERR Aug 10 16:56:54.148845 (975-1286) voice-fapp-fprv_eval_profile_rule return status=FPRV_ERR_SER
```

If the phone can resolve the domain, it can look like this:

```
1664 NOT Aug 10 16:56:35.440901 (968-1290) voice-reqByCurlInternal sending http request out..., url: ht
1666 INF Aug 10 16:56:35.454585 dnsmasq[560]: forwarded activate.cisco.x to 192.168.100.1
1669 INF Aug 10 16:56:35.488147 dnsmasq[560]: reply activate.cisco.x is <CNAME>
1670 INF Aug 10 16:56:35.488194 dnsmasq[560]: [cache_insert] activate.cisco.x[4008]: Wed May 10 17:21:4
1671 INF Aug 10 16:56:35.488219 dnsmasq[560]: reply activate.xglb.cisco.com is 173.36.XXX.XXX
1683 NOT Aug 10 16:56:36.018143 GET /software/edos/callhome/rc?id=<MAC_ADDRESS>:FCH2305DMH0:CP-8865-3PC
 User-Agent: Cisco-CP-8865-3PCC/12.0.2 (MAC_ADDRESS)^M
 Host: activate.cisco.x^M
 Accept-Encoding: deflate, gzip^M
 Accept: */*^M
 Accept-Language: en^M
 Accept-Charset: iso-8859-1^M
 ^M
1684 NOT May 10 16:56:36.137337 <
1685 NOT May 10 16:56:36.137446 HTTP/1.1 200 ^M
1760 NOT Sep 04 22:49:25.017943 (968-1290) voice-fapp-pal data updated for property name: Profile Rule
```

After receiveing the 200 OK from the GET request to activate.cisco.com the phone makes a request to cisco.siplash.com. It is the same process, the phone tries to resolve the domain and if it fails it can look like this:

```
2460 NOT May 10 17:03:14.644821 (975-975) voice-QPE:RESYNC profile=[https://cisco.sipflash.x/ ]
2487 NOT May 10 17:03:14.924347 (975-1286) voice-reqByCurlInternal sending http request out..., url: ht
2488 INF May 10 17:03:14.925286 dnsmasq[564]: query[A] cisco.sipflash.x from 127.0.0.1
2489 INF May 10 17:03:14.925318 dnsmasq[564]: forwarded cisco.sipflash.x to 192.168.100.3
2503 NOT May 10 17:03:22.926249 "Couldn't resolve host 'cisco.sipflash.x"
```

If the phone can resolve the domain, it can look like this:

```
1980 NOT Sep 04 22:49:28.832733 (968-1290) voice-reqByCurlInternal sending http request out..., url: ht
1981 INF Sep 04 22:49:28.833577 dnsmasq[560]: query[A] cisco.sipflash.x from 127.0.0.1
1982 INF Sep 04 22:49:28.833628 dnsmasq[560]: forwarded cisco.sipflash.x to 192.168.100.1
1985 INF Sep 04 22:49:28.844068 dnsmasq[560]: reply cisco.sipflash.x is 199.59.XXX.XXX
1993 NOT Sep 04 22:49:29.189918 (968-1290) voice-sec_set_min_TLS_version: min_TLS_verson is TLS 1.1,ret
1994 NOT Sep 04 22:49:29.428716 >
1995 NOT Sep 04 22:49:29.428776 GET / HTTP/1.1^M
User-Agent: Cisco-CP-8865-3PCC/12.0.2 (MAC_ADDRESS)^M
Host: cisco.sipflash.x^M
Accept-Encoding: deflate, gzip^M
Accept: */*^M
Accept-Language: en^M
Accept-Charset: iso-8859-1^M
^M
1996 NOT Sep 04 22:49:29.506969 <
1997 NOT Sep 04 22:49:29.507037 HTTP/1.1 200 OK^M
```

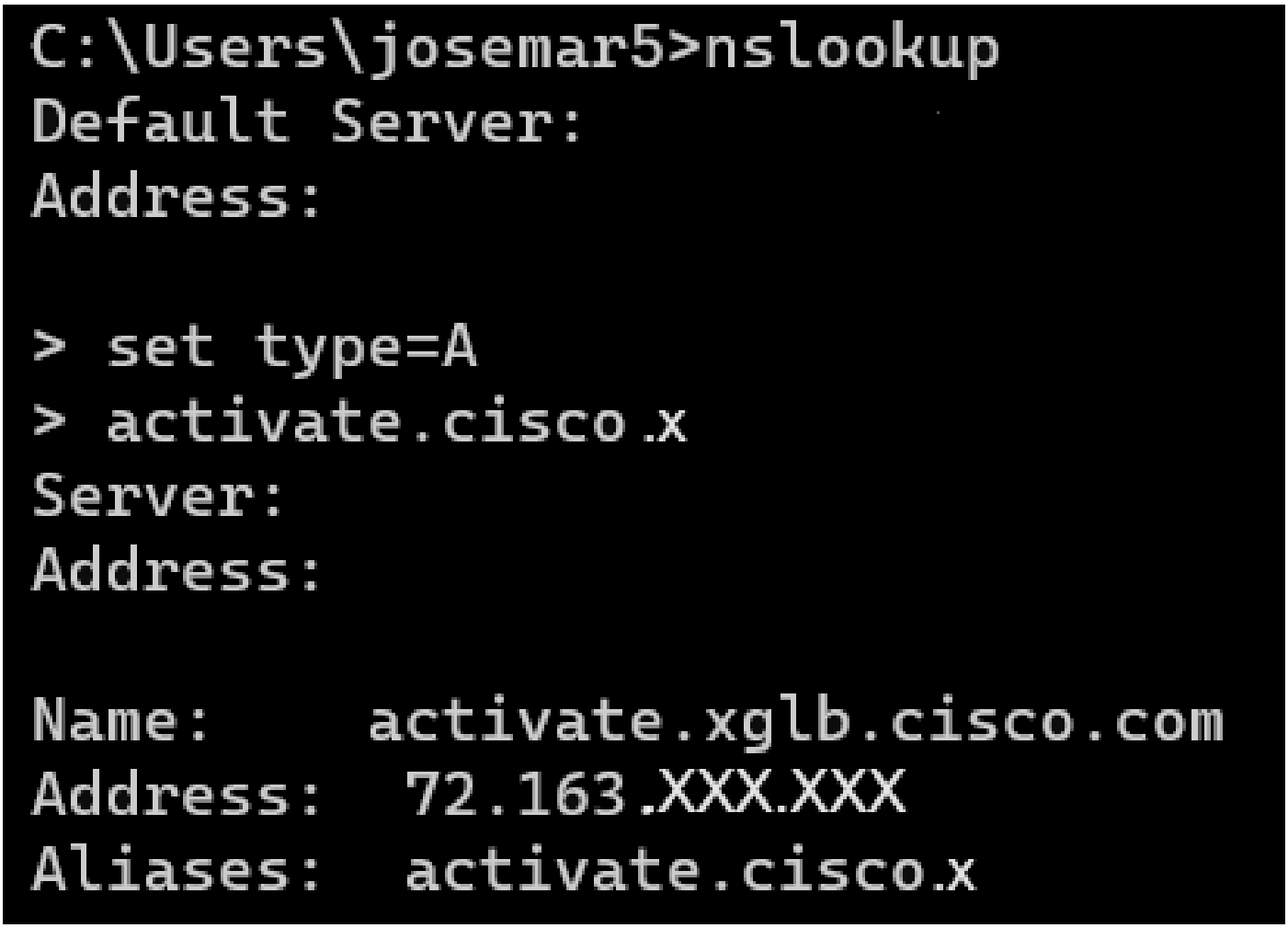
Trobuleshoot DNS (Provision URLs)

If you are in the same network where the devices has problems with the DNS resolution, an nslookup can be used to check if the DNS server is able to resolve the domain. Open the command line interface and do the next steps:

- nslookup -> Enter

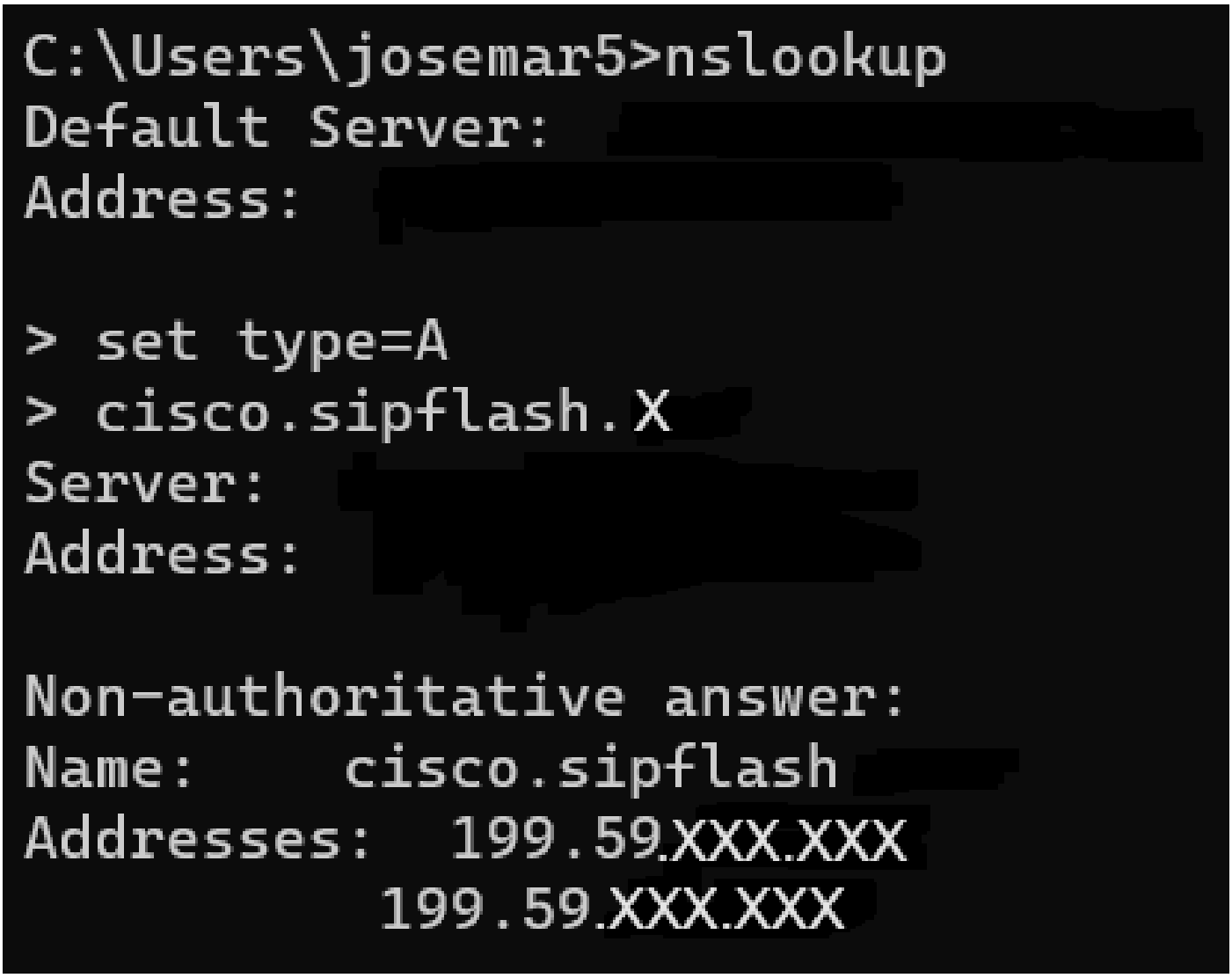
- set type=A -> Enter
- activate.cisco.com

If the PC can resolve the domain, it can look like this:



nslookup activate.cisco

The same process can be made for cisco.sipflash.x to resolve the domain:



nslookup cisco sipflash

If the PC is unable to resolve the domains, look at your DNS server.

Trobleshoot the Registration for an MPP device in WxC

For this example, the outbound proxy is da02.hosted-us10.bcld.webex.com. The phone tries to resolve the SRV domain:

```
1721 NOT Sep 04 22:50:32.068857 (2059-2271) voice-[SIP_resolveHostName] host=da02.hosted-us10.bcld.webe
1722 NOT Sep 04 22:50:32.068912 (2059-2271) voice-RSE_DEBUG: rse_unref context: 0x5213bab8
1723 NOT Sep 04 22:50:32.068933 (2059-2271) voice-RSE_DEBUG: rse_unref ref_cnt:0
1724 NOT Sep 04 22:50:32.068950 (2059-2271) voice-RSE_DEBUG: rse_get_server_addr, name: _sips._tcp.da02
1725 NOT Sep 04 22:50:32.068975 (2059-2271) voice-RSE_DEBUG: rse_refresh_addr_list target:_sips._tcp.da
1726 NOT Sep 04 22:50:32.069001 (2059-2271) voice-RSE_DEBUG: RR[0], name:_sips._tcp.da02.hosted-us10.bc
1727 INF Sep 04 22:50:32.069517 dnsmasq[560]: query[SRV] _sips._tcp.da02.hosted-us10.bcld.webex.com fro
1728 INF Sep 04 22:50:32.069549 dnsmasq[560]: forwarded _sips._tcp.da02.hosted-us10.bcld.webex.com to 1
1729 INF Sep 04 22:50:32.082459 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1730 INF Sep 04 22:50:32.082512 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
1731 INF Sep 04 22:50:32.082661 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bcld.webex.com
1732 INF Sep 04 22:50:32.082689 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1733 INF Sep 04 22:50:32.082714 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
1734 INF Sep 04 22:50:32.082738 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bcld.webex.com
```

```
1735 INF Sep 04 22:50:32.082762 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1736 INF Sep 04 22:50:32.082786 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
1737 INF Sep 04 22:50:32.082810 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bcld.webex.com
1738 INF Sep 04 22:50:32.082838 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1739 INF Sep 04 22:50:32.082864 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
1740 INF Sep 04 22:50:32.082888 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bcld.webex.com
1741 INF Sep 04 22:50:32.082911 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1742 INF Sep 04 22:50:32.082936 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
1743 INF Sep 04 22:50:32.082958 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bcld.webex.com
1744 INF Sep 04 22:50:32.082981 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex
1745 INF Sep 04 22:50:32.083006 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hoste
```

If the phone is able to resolve the SRV domain it gets the hostnames:

```
1746 NOT Sep 04 22:50:32.082468 (2059-2271) voice-RSE_DEBUG: getting SRV:_sips._tcp.da02.hosted-us10.bc
1747 NOT Sep 04 22:50:32.082525 (2059-2271) voice-RSE_DEBUG: new priority:a by host: hosted02aj-us10.bc
1748 NOT Sep 04 22:50:32.082548 (2059-2271) voice-RSE_DEBUG: old priority:a by host: hosted02as-us10.bc
1749 NOT Sep 04 22:50:32.082565 (2059-2271) voice-RSE_DEBUG: new priority:5 by host: hosted01as-us10.bc
1750 NOT Sep 04 22:50:32.082581 (2059-2271) voice-RSE_DEBUG: old priority:5 by host: hosted01aj-us10.bc
1751 NOT Sep 04 22:50:32.082598 (2059-2271) voice-RSE_DEBUG: old priority:5 by host: hosted01ai-us10.bc
1752 NOT Sep 04 22:50:32.082613 (2059-2271) voice-RSE_DEBUG: old priority:a by host: hosted02ai-us10.bc
```

From one of those hostnames the phone takes one of them to register de device to the WxC SBC:

```
1774 NOT Sep 04 22:50:32.083015 (2059-2271) voice-RSE_DEBUG: Refreshing host[3]:hosted01aj-us10.bcld.we
1775 INF Sep 04 22:50:32.083539 dnsmasq[560]: query[A] hosted01aj-us10.bcld.webex.com from 127.0.0.1
1776 INF Sep 04 22:50:32.083567 dnsmasq[560]: found A record=hosted01aj-us10.bcld.webex.com with TTL=81
1777 INF Sep 04 22:50:32.083590 dnsmasq[560]: cached hosted01aj-us10.bcld.webex.com is 139.177.XXX.XXX
1778 INF Sep 04 22:50:32.083668 dnsmasq[560]: query[AAAA] hosted01aj-us10.bcld.webex.com from 127.0.0.1
1779 INF Sep 04 22:50:32.083698 dnsmasq[560]: found A record=hosted01aj-us10.bcld.webex.com with TTL=26
1780 INF Sep 04 22:50:32.083723 dnsmasq[560]: cached hosted01aj-us10.bcld.webex.com is 2607:fcf0:9000:X
1781 NOT Sep 04 22:50:32.084094 (2059-2271) voice-RSE_DEBUG: Refresh host:hosted01aj-us10.bcld.webex.co
1782 NOT Sep 04 22:50:32.084133 (2059-2271) voice-RSE_DEBUG: rse_save_addr_list res = 0x43227cc8 af = 2
1783 NOT Sep 04 22:50:32.084152 (2059-2271) voice-RSE_DEBUG: skip AF_INET6 addr
1784 NOT Sep 04 22:50:32.084185 (2059-2271) voice-RSE_DEBUG: Found one old entry<4320b538> [139.177.XXX
3673 NOT Sep 04 22:51:08.127871 (2656-2764) voice- =====> Send (TLS) [139.177.XXX.XXX]:8934 SIP MSG::
 Via: SIP/2.0/TLS 192.168.100.6:5072;branch=z9hG4bK-c77bd320^M
 From: <sip:w3nca1a025@XXXXX.example.com>;tag=fcd8304d2abdd95co0^M
 To: <sip:w3nca1a025@XXXXX.example.com>^M
 Call-ID: 98126dba-9df06bd9@192.168.100.6^M
 CSeq: 6367 REGISTER^M
 Max-Forwards: 70^M
 Contact: <sip:w3nca1a025@192.168.100.6:5072;transport=tls>;expires=3600^M
 User-Agent: Cisco-CP-8865-3PCC/12.0.2_<MAC_ADDRESS>_47cff26a-4713-41a1-8d75-28d7b638ffe8_2c01b5e7-53d5
 Peripheral-Data: none^M
 Session-ID: 300e21a200105000a0002c01b5e753d5;remote=00000000000000000000000000000000^M
 Content-Length: 0^M
 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE^M
 Allow-Events: hold,talk,conference^M
 Supported: replaces, sec-agree, record-aware^M
 Accept-Language: en^M
```

The device must get a 401 Unauthorized message from the WxC side:

```
3857 NOT Sep 04 22:51:08.176087 (2656-2764) voice- <===== Recv (TCP) [139.177.XXX.XXX]:8934 SIP MSG:: S
Via:SIP/2.0/TLS 192.168.100.6:5072;received=187.190.XXX.XXX;branch=z9hG4bK-c77bd320^M
From:<sip:w3nca1a025@XXXXX.example.com>;tag=fcd8304d2abdd95co0^M
To:<sip:w3nca1a025@XXXXX.example.com>;tag=799618563-1693867868150^M
Call-ID:98126dba-9df06bd9@192.168.100.6^M
CSeq:6367 REGISTER^M
Session-ID:d1b7e5b700804ca4a817949623258793;remote=300e21a200105000a0002c01b5e753d5^M
WWW-Authenticate:DIGEST realm="BroadWorks",qop="auth",nonce="BroadWorksXlm5h6zucT8ymkkBW",algorithm=MD5
Contact:<sip:w3nca1a025@192.168.100.6:5072;transport=tls>;expires=120^M
Content-Length:0^M
^M
```

The device sends the REGISTER with the Authorization header:

```
3863 NOT Sep 04 22:51:08.186602 (2656-2764) voice- =====> Send (TLS) [139.177.XXX.XXX]:8934 SIP MSG:: R
Via: SIP/2.0/TLS 192.168.100.6:5072;branch=z9hG4bK-be588fb^M
From: <sip:w3nca1a025@XXXXX.example.com>;tag=fcd8304d2abdd95co0^M
To: <sip:w3nca1a025@XXXXX.example.com>^M
Call-ID: 98126dba-9df06bd9@192.168.100.6^M
CSeq: 6368 REGISTER^M
Max-Forwards: 70^M
Authorization: Digest username="+1XXXXXXXXXX",realm="BroadWorks",nonce="BroadWorksXlm5h6zucT8ymkkBW",ur
Contact: <sip:w3nca1a025@192.168.100.6:5072;transport=tls>;expires=3600^M
User-Agent: Cisco-CP-8865-3PCC/12.0.2_<MAC_ADDRESS>_47cff26a-4713-41a1-8d75-28d7b638ffe8_2c01b5e7-53d5-
Peripheral-Data: none^M
Session-ID: 300e21a200105000a0002c01b5e753d5;remote=d1b7e5b700804ca4a817949623258793^M
Content-Length: 0^M
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE^M
Allow-Events: hold,talk,conference^M
```

And then, the device gets a SIP 200 OK:

```
4056 NOT Sep 04 22:51:08.236092 (2656-2764) voice- <===== Recv (TCP) [139.177.XXX.XXX]:8934 SIP MSG:: S
Via:SIP/2.0/TLS 192.168.100.6:5072;received=187.190.XXX.XXX;branch=z9hG4bK-be588fb^M
From:<sip:w3nca1a025@XXXXX.example.com>;tag=fcd8304d2abdd95co0^M
To:<sip:w3nca1a025@XXXXX.example.com>;tag=258864438-1693867868205^M
Call-ID:98126dba-9df06bd9@192.168.100.6^M
CSeq:6368 REGISTER^M
Session-ID:d1b7e5b700804ca4a817949623258793;remote=300e21a200105000a0002c01b5e753d5^M
Allow-Events:call-info,line-seize,dialog,message-summary,as-feature-event,x-broadworks-hoteling,x-broad
Contact:<sip:w3nca1a025@192.168.100.6:5072;transport=tls>;q=0.5;expires=120^M
Content-Length:0^M
^M
```

After this process, the device must be up and registered to the WxC services.

Troubleshoot DNS (Register URLs)

If you are in the same network where the devices have problems with the DNS resolution, nslookup can be used to check if the DNS server is able to resolve the domain. Open the command line interface and do the next steps:

- nslookup -> Enter
- set type=SRV -> Enter

- _sips._tcp.da02.hosted-us10.bcld.webex.com

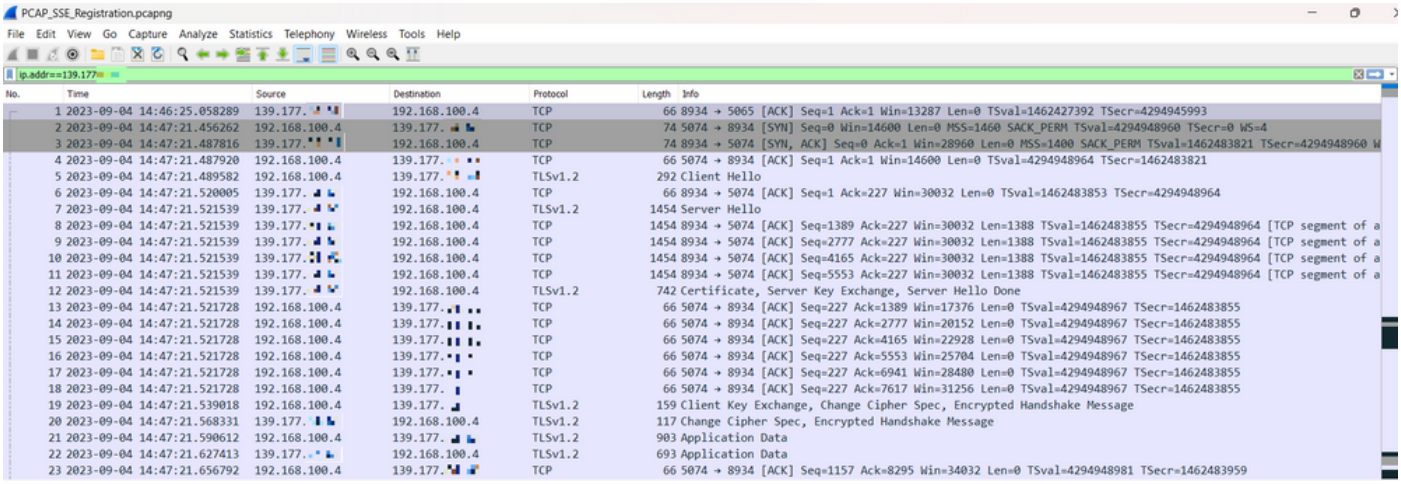
If the PC is able to resolve the domain it can look like this:

```
C:\Users\josemar5>nslookup
Default Server:
Address:

> set type=SRV
> _sips._tcp.da02.hosted-us10.bcld.webex.com
Server:
Address:

Non-authoritative answer:
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 5
          weight         = 50
          port           = 8934
          svr hostname   = hosted01ai-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 10
          weight         = 50
          port           = 8934
          svr hostname   = hosted02as-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 5
          weight         = 50
          port           = 8934
          svr hostname   = hosted01as-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 10
          weight         = 50
          port           = 8934
          svr hostname   = hosted02ai-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 10
          weight         = 50
          port           = 8934
          svr hostname   = hosted02aj-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 5
          weight         = 50
          port           = 8934
          svr hostname   = hosted01aj-us10.bcld.webex.com

hosted01ai-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted01aj-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted01as-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted02ai-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted02aj-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted02as-us10.bcld.webex.com  internet address = 139.177.XXX.XXX
hosted01ai-us10.bcld.webex.com  AAAA IPv6 address = 2607:fcf0:9000:
```

nslookup SRV OBP

Packet Capture (Registration Process)

You can take the IP Address that the phone has for register, a filter can be used in the packet capture to look at the TLS handshake:



PCAP SSE

The packet capture can help in order to see if the TLS handshake failed.

Cisco Webex Calling TAC Support

If you need support in order to analyze the logs and find the root cause of the issue, please contact the Cisco Webex Calling TAC team.

Support Related Information

Port Reference Information for Webex Calling