WxC での MPP 電話のプロビジョニングと登録のトラブルシューティング

内容

はじめに
- 要件
- 使用するコンポーネント

Control Hub でのデバイスの追加

WxC でのデバイスのプロビジョニングプロセスの概要

WxC でのデバイスのプロビジョニングプロセスのトラブルシューティング
- MPP デバイスからの PRT ログの生成
- デバイスからの PRT の生成
- PRT ログ
- DNS のトラブルシューティング（URL プロビジョニング）

WxC での MPP デバイス登録のトラブルシューティング
- DNS のトラブルシューティング（URL の登録）
- パケットキャプチャ（登録プロセス）
- Cisco Webex Calling の TAC サポート
- サポート関連情報

はじめに

このドキュメントでは、デバイスが MAC アドレスによって追加されたときのプロビジョニングと登録の問題のために、WxC で MPP 電話のトラブルシューティングを行う方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

- ネットワークの基本知識
- MPP フォン

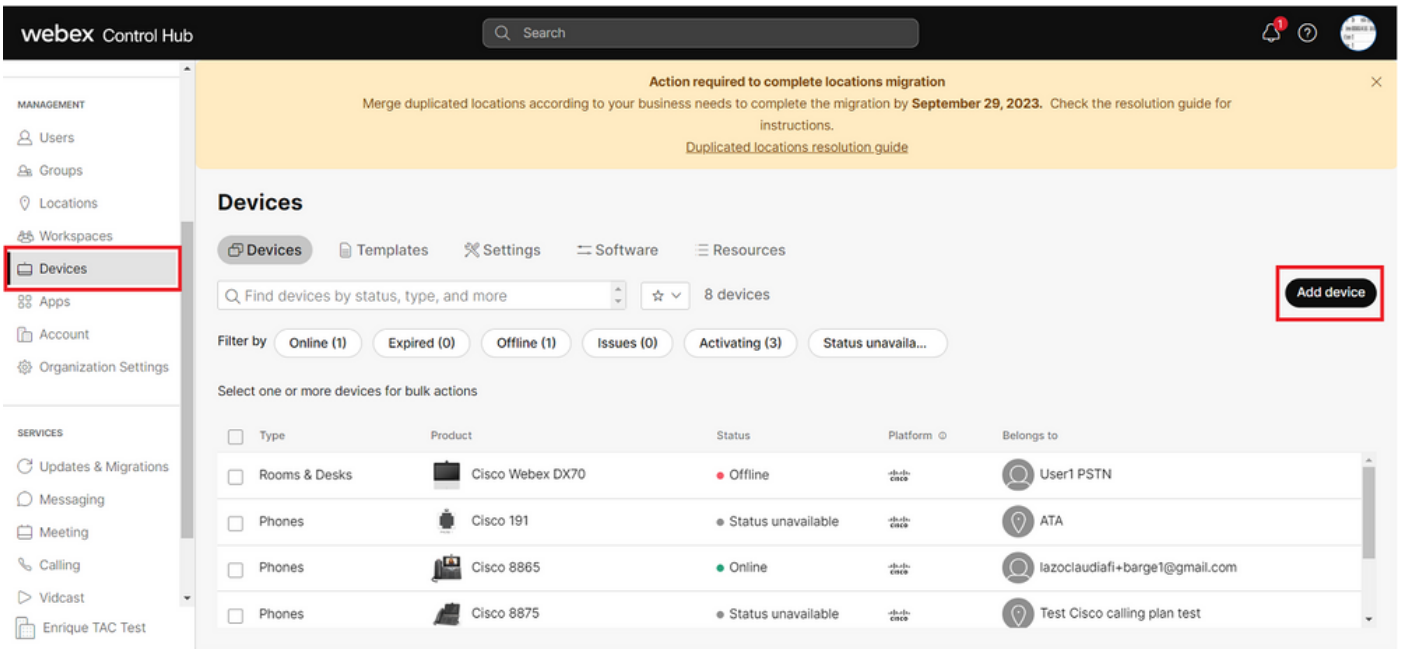
使用するコンポーネント

このドキュメントの情報は、78XX、88XX などの MPP 電話のみに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

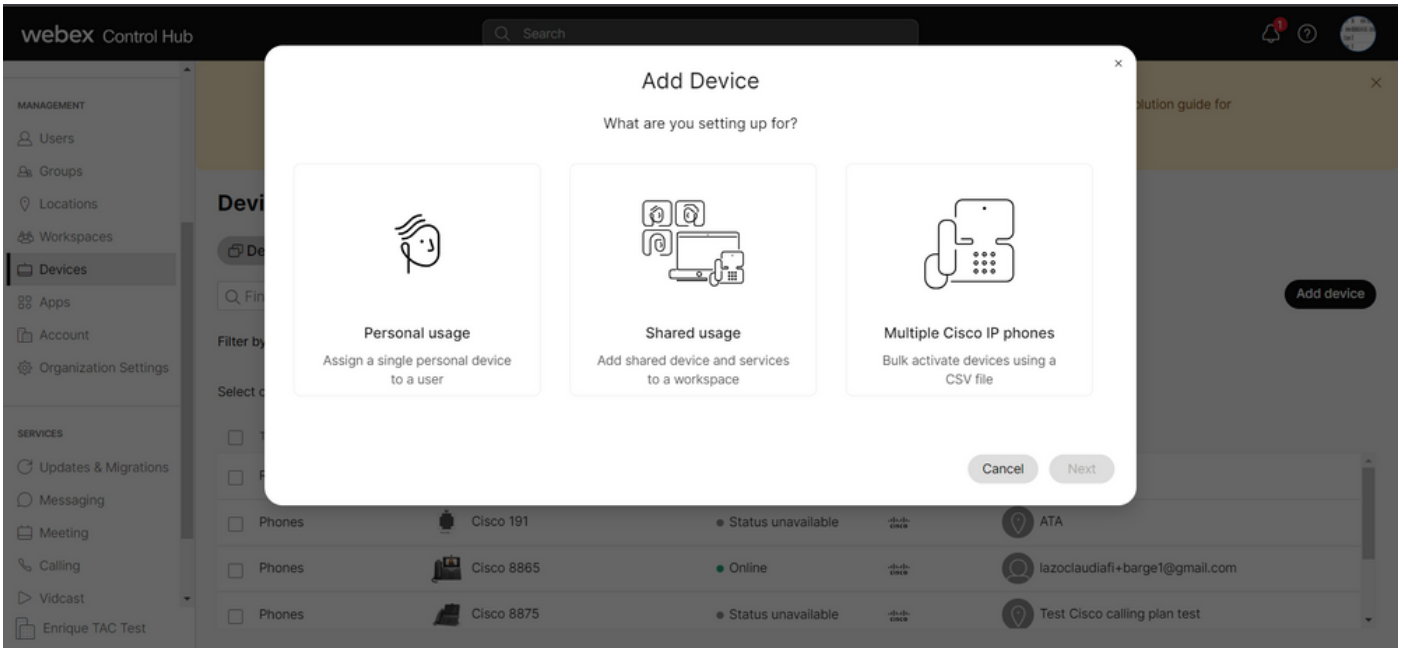
Control Hub でのデバイスの追加

ステップ 1：admin.webex.com に移動し、管理者ログイン情報を使用します。組織で、[デバイス（Devices）] > [デバイスの追加（Add device）] に移動します。



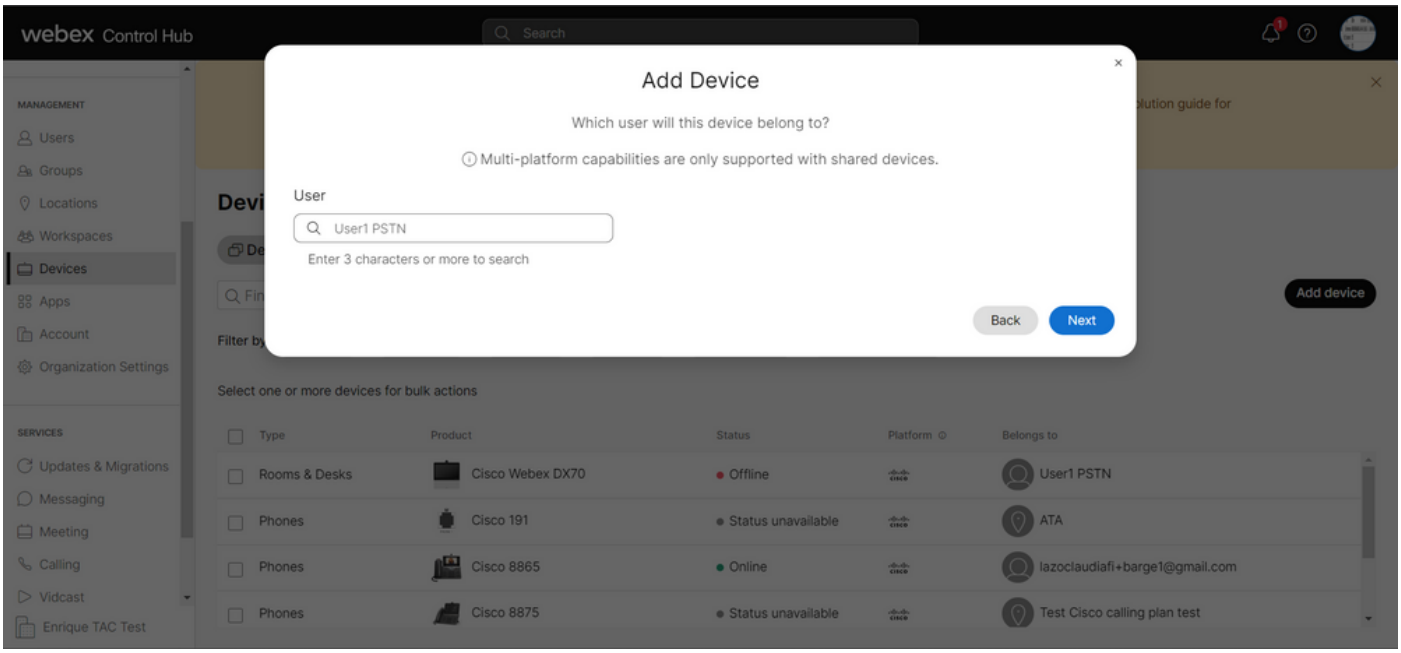
[デバイス（Devices）] タブ

ステップ 2：ユーザーに割り当てるときは [個人使用（Personal usage）] を選択し、ワークスペースに割り当てるときは [共有使用（Shared Usage）] を選択します。（このシナリオではユーザーが使用されます）



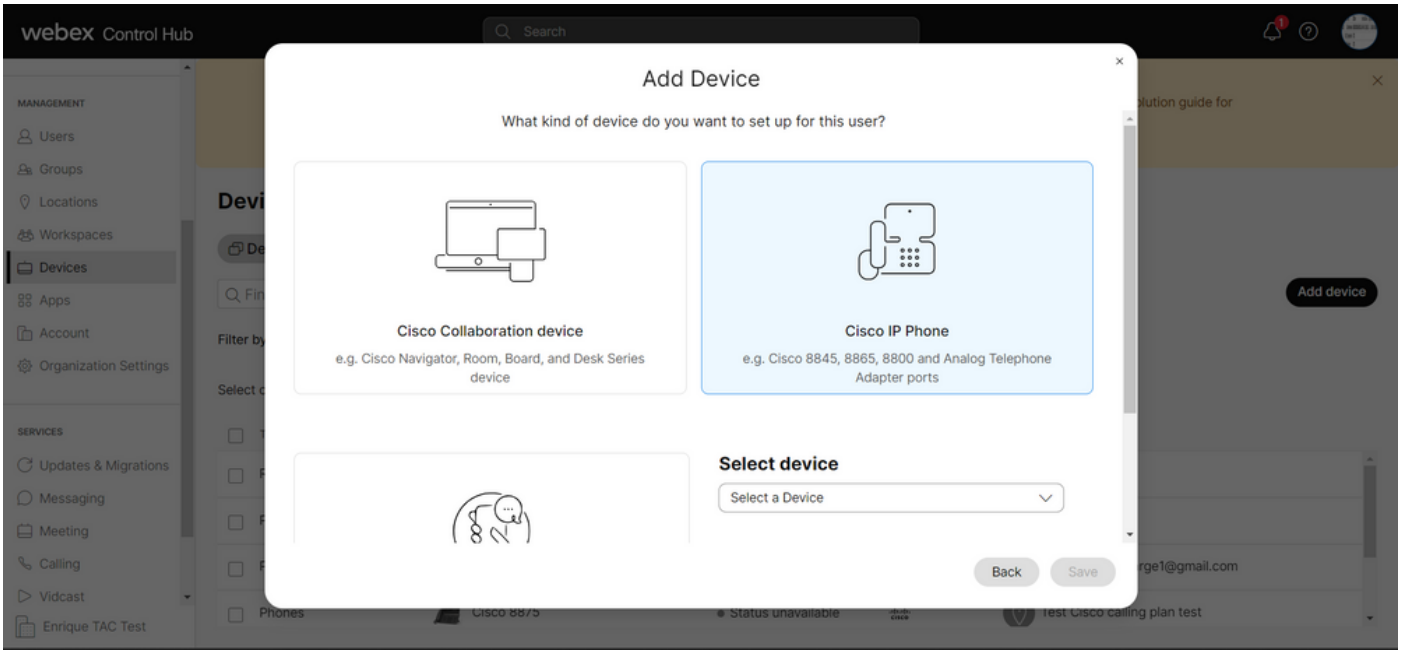
デバイスの追加

ステップ 3：このデバイスに割り当てるユーザーを検索して選択し、[次へ（Next）] をクリックします。



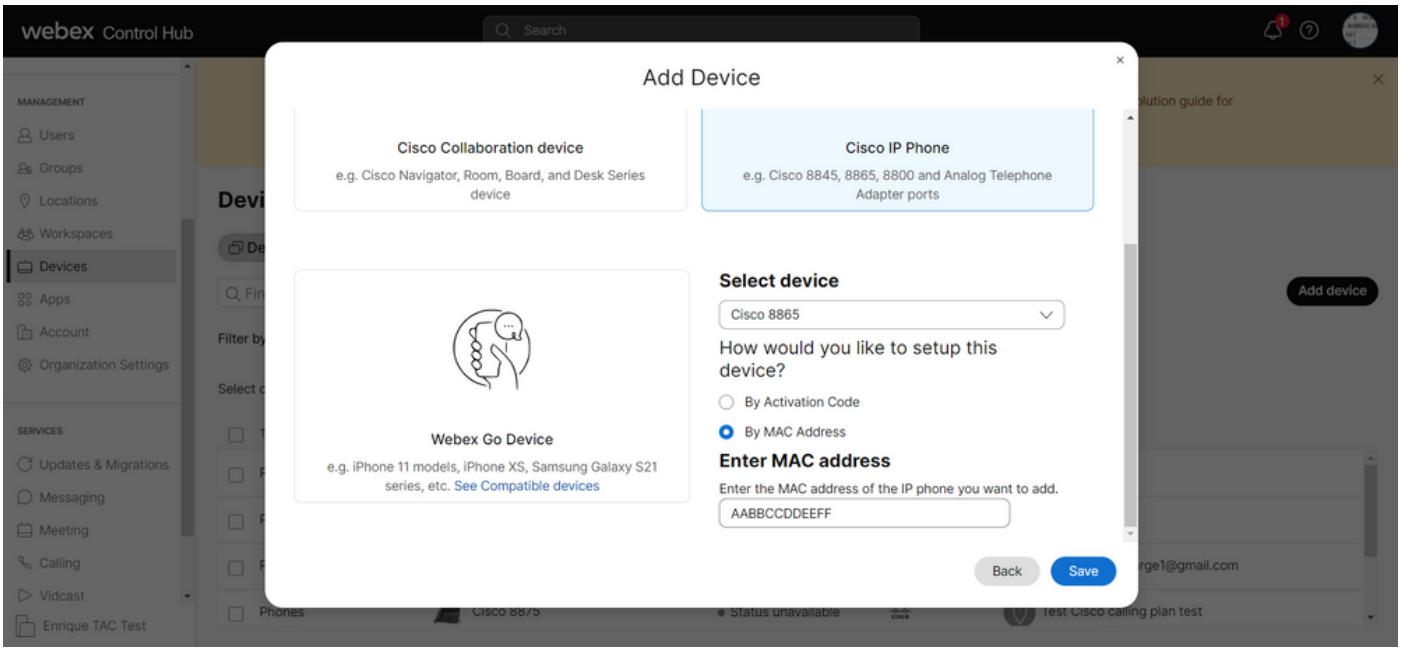
ユーザーの検索

ステップ 4：[Cisco IP電話（Cisco IP Phone）] を選択し、デバイスモデルを検索します。



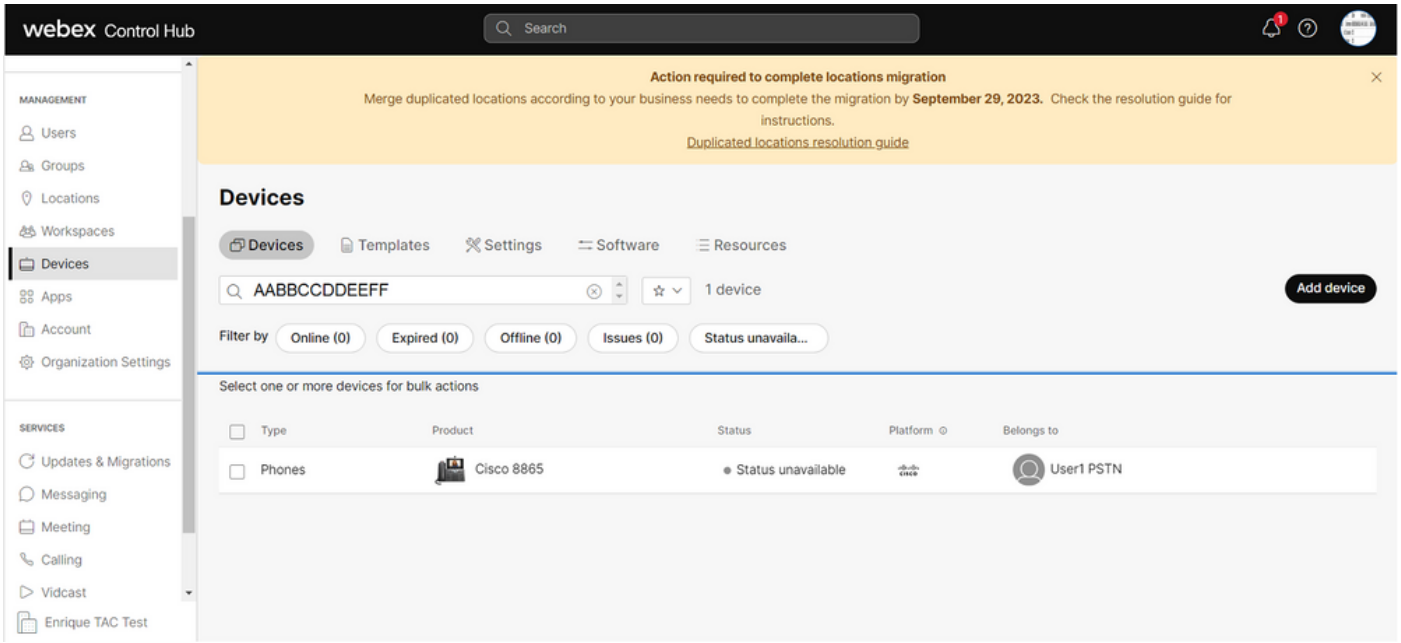
デバイスモデルの選択

ステップ 5：デバイスを選択したら [MACアドレスを使用（By MAC Address）] オプションを選択し、デバイスの MAC アドレスを入力して [保存（Save）] をクリックします。



MAC アドレスを追加

手順 6：デバイスが Control Hub に追加されたら、検索バーで MAC アドレスを検索すると、デバイスが正しく追加されたことを確認できます。

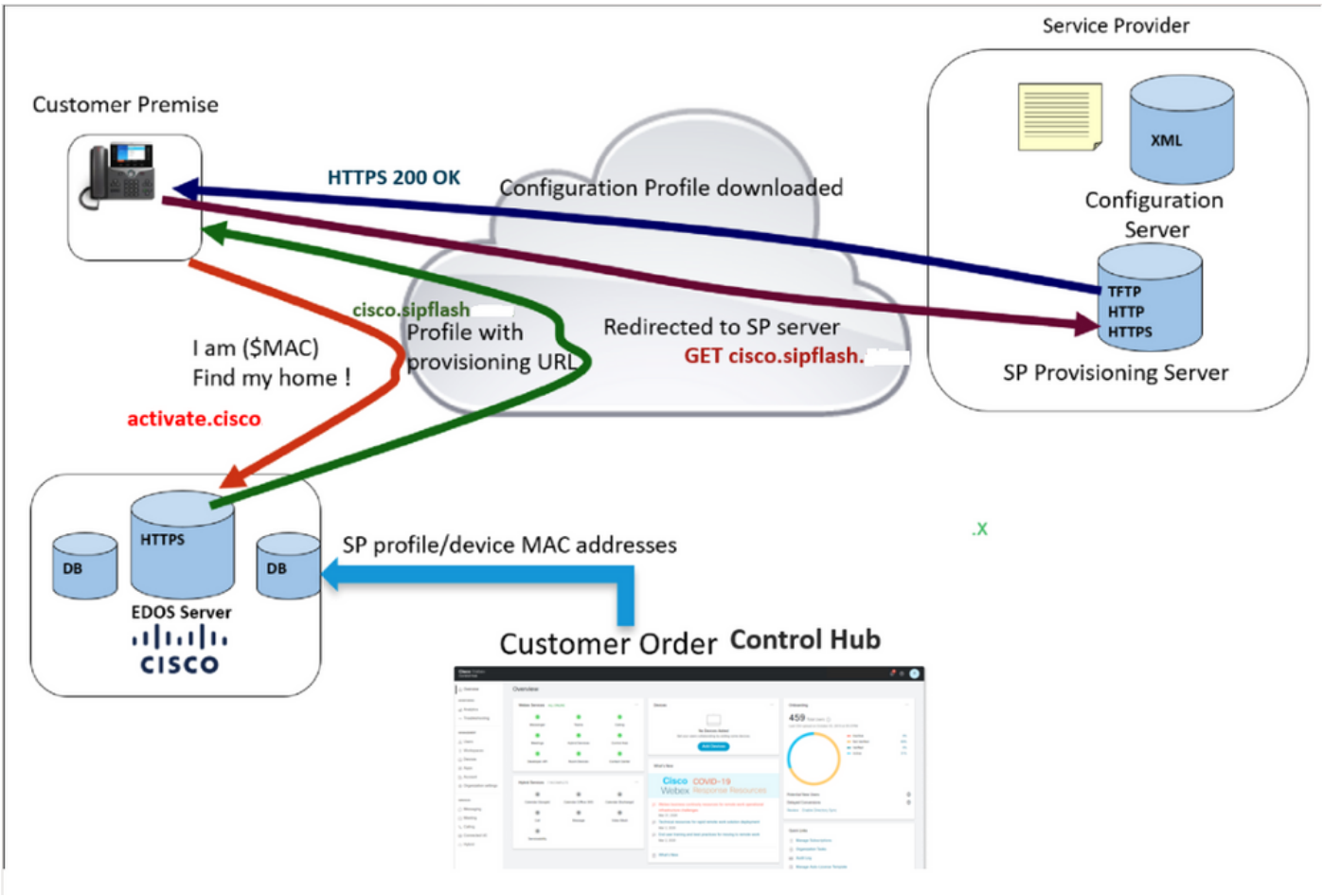


デバイスの検証

デバイスがまだプロビジョニングされていないため、ステータスは利用不可（Unavailable）と表示されています。デバイスが Control Hub に追加されたら、次のステップはデバイスを初期設定にリセットすることです。初期設定にリセットした後、デバイスは WxC サーバーにリクエストして設定ファイルを取得する必要があります。（これがプロビジョニングプロセスです）デバイスの画面に電話番号および/または内線番号が表示されたら、デバイスは正常にプロビジョニングされています。

デバイスに適切な設定が表示されない場合は、デバイスのプロビジョニングプロセスは失敗しています。

WxC でのデバイスのプロビジョニングプロセスの概要



プロビジョニングの図

WxC でのデバイスのプロビジョニングプロセスのトラブルシューティング

MPP デバイスは、次のような場合、WxC ではプロビジョニングできません。

- DHCP サーバーで設定された TFTP サーバーが設定されている
- オプション (OPT66、OPT160、OPT159、または OPT150) が DHCP サーバーによって設定および提供されている場合

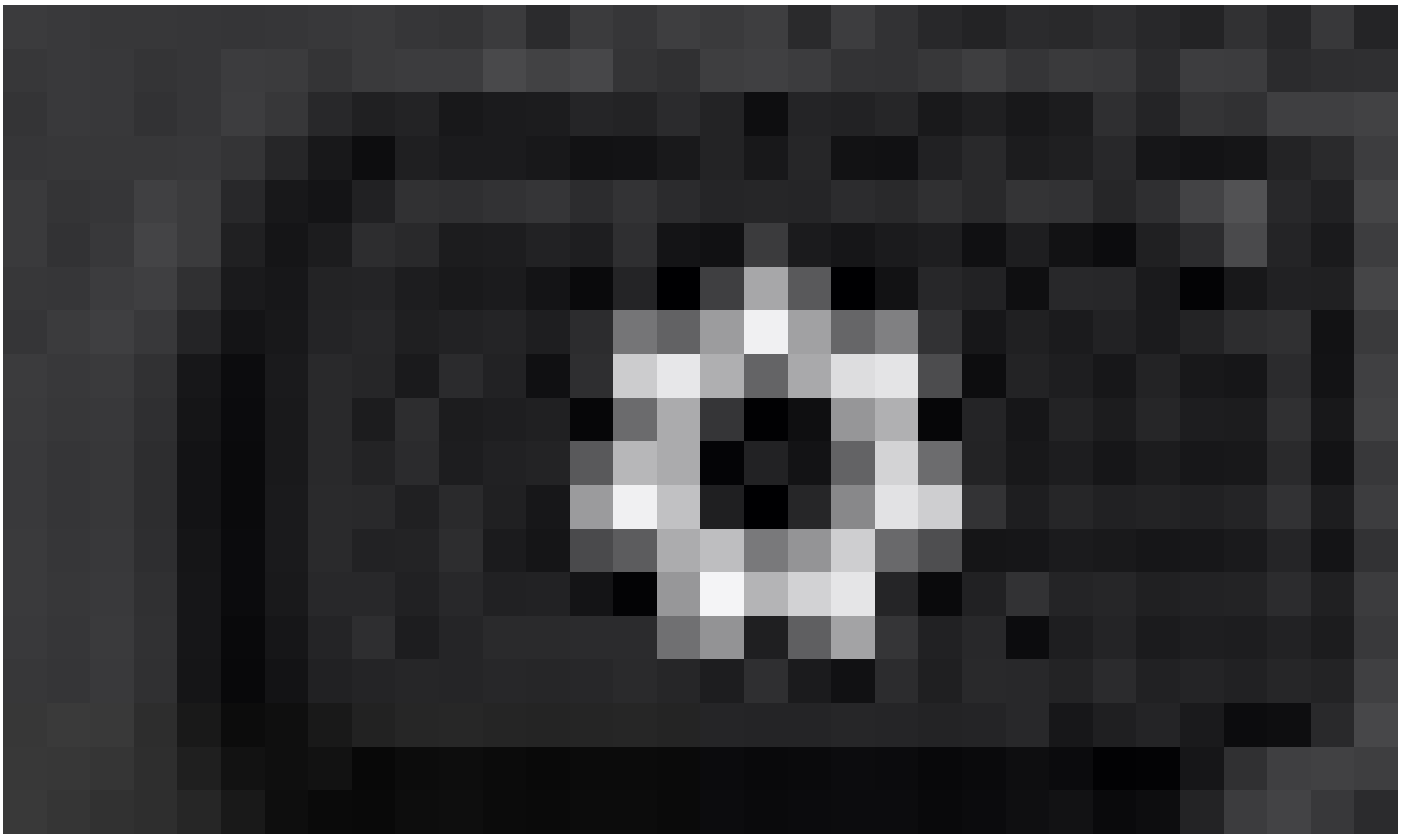
電話機が DHCP サーバーから TFTP 設定を取得したかどうかを確認するには、PRT ログが必要です。

MPP デバイスからの PRT ログの生成

電話機の PRT ログから送信します。以下に PRT ログを生成する方法を示します。

デバイスからの PRT の生成

ステップ 1：デバイスで [アプリケーション (Applications)] ボタンを押します。



設定ボタン

.

ステップ 2：[ステータス（Status）] > [問題の報告（Report Problem）] に移動します。

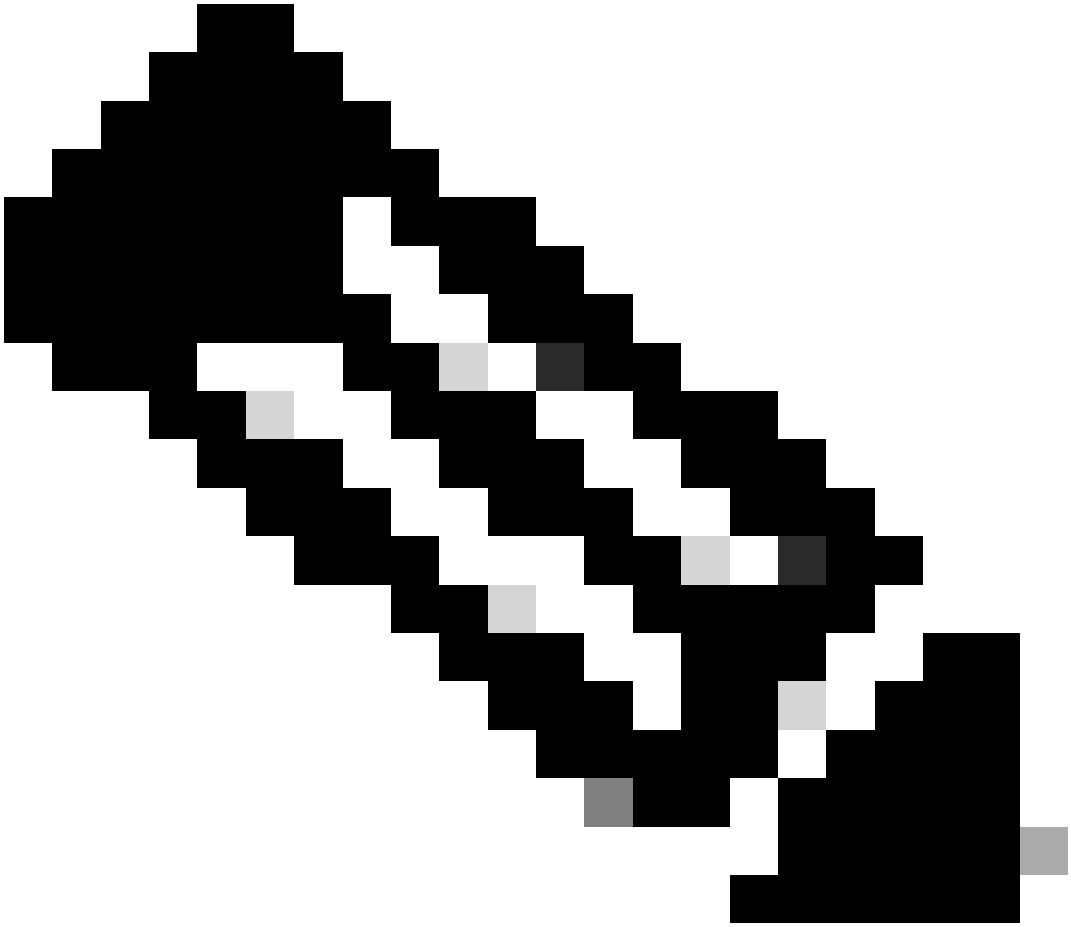
ステップ 3：問題の日付と時刻を入力します。

ステップ 4：リストから説明を選択します。

ステップ 5：[送信（Submit）] を押します。

ログが送信されたら、次の手順を参照して PRT ログをダウンロードします。

ステップ 1： https://IP_ADDRESS_PHONE/ にログインします。



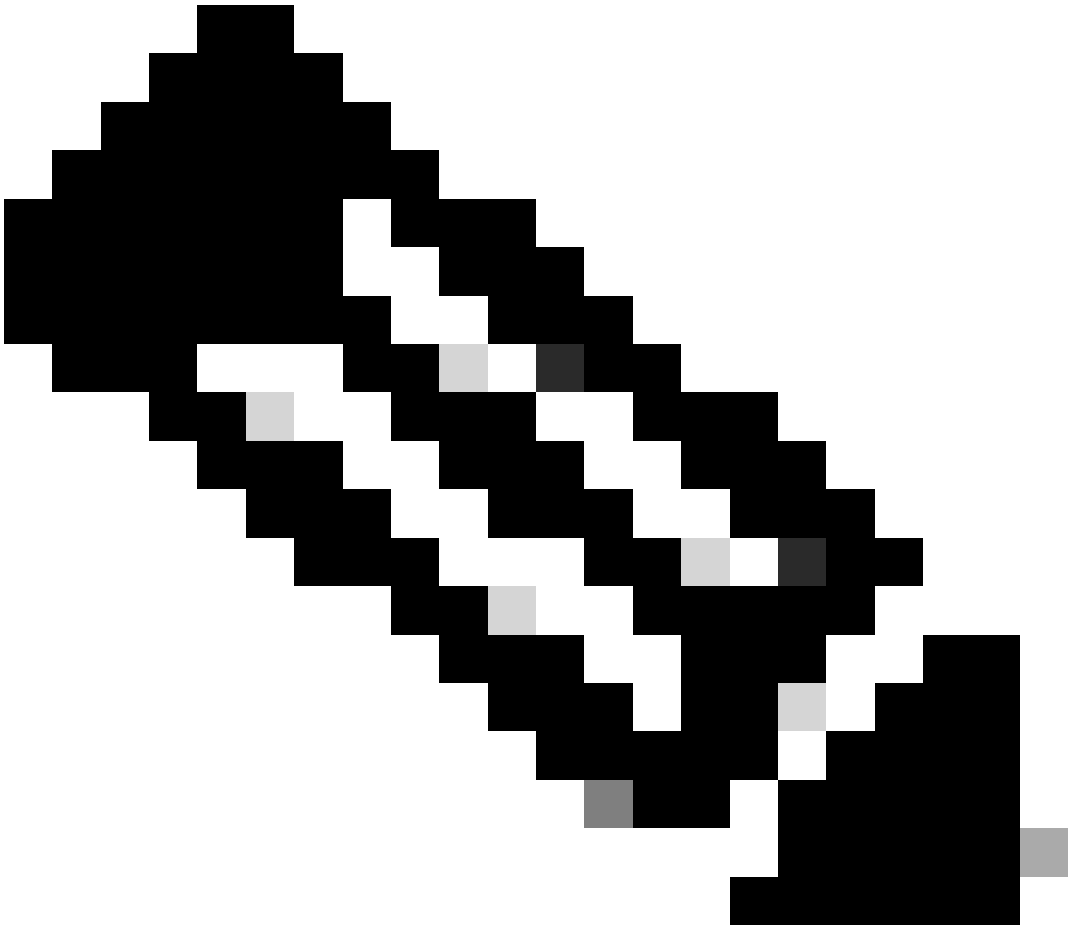
注：注：IP アドレスが不明の場合は、[設定（Settings）] > [ステータス（Status）] > [ネットワークのステータス（Network Status）] > [IPv4のステータス（IPv4 Status）] から取得できます。

ステップ 2： [情報（Info）] >[デバッグ情報（Debug Info）] > [PRTログをダウンロード（Download the PRT log）] に移動します（リンクを右クリックし、[名前を付けて保存（Save As...）] を選択します）。 ）

Web GUI

PRT ログ

ログを開くと以下のようなビューが表示されます。



注：ログは圧縮されているため、WinRAR などのプログラムでログを開くことができます。

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ログ（PRT Log）] ビュー

デバイスのプロビジョニングプロセスを分析するには、 logcat というログを開く必要があります。 Notepad や Notepad++ などのテキストエディタで開くことができます。
テキストエディタの「検索」機能を使用すると、電話機に TFTP サーバーが設定されているかどうかを確認できます。 DHCP-tftpsvr1 または DHCP-tftpsvr2 を使用して、そのログの特定の行を見つけます。ログの他の行を確認すると、DHCP 設定に関する詳細情報が見つかります。

```
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:
```

ログから分かるように、TFTP IP アドレスは DHCP サーバーで設定されています。そのため、電話機は Webex Calling サーバーではなく、この TFTP サーバーへのプロビジョニングを試みました。

```
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
```

DHCP サーバーから TFTP 設定と OPT 設定を削除した後、デバイスを工場出荷時の状態にリセットして、WxC を使用してデバイスを再度プロビジョニングするプロセスを開始する必要があります。
電話機がデバイスのプロビジョニングプロセスで最初に試みるのは、URL activate.cisco.com へのリクエストです。電話機は、ドメインを解決するために DNS サーバーへのクエリを実行します。DNS 解決が失敗した場合は、以下のようになります。

<#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
```

電話機がドメインを解決できる場合は、以下のようになります。

```
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
```

activate.cisco.com への GET リクエストから 200 OK を受信した後、電話機は cisco.siplash.com へのリクエストを行います。これは同じプロセスです。電話機はドメインの解決を試み、失敗した場合は以下のようになります。

```
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"
```

電話機がドメインを解決できる場合は、以下のようになります。

```
1980 NOT Sep 04 22:49:28.832733 (968-1290) voice-reqByCurlInternal sending http request out..., url: htt
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
```

DNS のトラブルシューティング（URL プロビジョニング）

デバイスに DNS 解決の問題があるネットワークと同じネットワーク内では、nslookup を使用して DNS サーバーがドメインを解決できるかどうかを確認できます。コマンドライン インターフェイスを開き、次の手順を実行します。

- nslookup -> Enter キーを押す
- set type=A -> Enter キーを押す
- activate.cisco.com

PC がドメインを解決できる場合は、以下のようになります。

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

> set type=A
> activate.cisco.x
Server:
Address:

Name:    activate.xglb.cisco.com
Address:  72.163.XXX.XXX
Aliases:  activate.cisco.x
```

nslookup activate.cisco

ドメインを解決するために、cisco.sipflash.x に対して同じプロセスを実行できます。

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

> set type=A
> cisco.sipflash.X
Server:
Address:

Non-authoritative answer:
Name:    cisco.sipflash
Addresses:  199.59.XXX.XXX
          199.59.XXX.XXX
```

nslookup cisco sipflash

PC がドメインを解決できない場合は、DNS サーバーを調べます。

WxC での MPP デバイス登録のトラブルシューティング

この例では、アウトバウンドプロキシは da02.hosted-us10.bcld.webex.com です。電話機は SRV ドメインの解決を試みます。

```
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
```

電話機は SRV ドメインを解決できる場合、次のホスト名を取得します。

```
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
```

電話機は、これらのいずれかからホスト名を取得して、デバイスを WxC SBC に登録します。

```
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:


        ;tag=fcd8304d2abdd95co0^M


 To:


        ^M


 Call-ID: 98126dba-9df06bd9@192.168.100.6^M
```

```
 CSeq: 6367 REGISTER^M
 Max-Forwards: 70^M
 Contact:



        ;expires=3600^M


 User-Agent: Cisco-CP-8865-3PCC/12.0.2_



        _47cff26a-4713-41a1-8d75-28d7b638ffe8_2c01b5e7-53d5-41a1-8d75-28d7b638ffe8^M


 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
```

デバイスは、WxC 側から 401 Unauthorized メッセージを取得する必要があります。

```
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:



        ;tag=fcd8304d2abdd95co0^M


To:



         ;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:



          ;expires=120^M
```

```
Content-Length:0^M

^M
```

デバイスは、Authorization ヘッダーとともに REGISTER を送信します。

```
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:

        ;tag=fcd8304d2abdd95co0^M

To:

         ^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",uri="sip:XXXXX.example.co

Contact:

          ;expires=3600^M

User-Agent: Cisco-CP-8865-3PCC/12.0.2_

           _47cff26a-4713-41a1-8d75-28d7b638ffe8_2c01b5e7-53d5-41a1-8d75-28d7b638ffe8^M

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
```

次に、デバイスは SIP 200 OK を取得します。

```
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:

        ;tag=fcd8304d2abdd95co0^M

To:

         ;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:
```

```
            ;q=0.5;expires=120^M

Content-Length:0^M

^M
```

このプロセスの後、デバイスは起動して WxC サービスに登録される必要があります。

DNS のトラブルシューティング（URL の登録）

デバイスに DNS 解決の問題があるネットワークと同じネットワーク内では、nslookup を使用して DNS サーバーがドメインを解決できるかどうかを確認できます。コマンドライン インターフェイスを開き、次の手順を実行します。

- nslookup -> Enter キーを押す
- set type=SRV -> Enter キーを押す
- _sips._tcp.da02.hosted-us10.bcld.webex.com

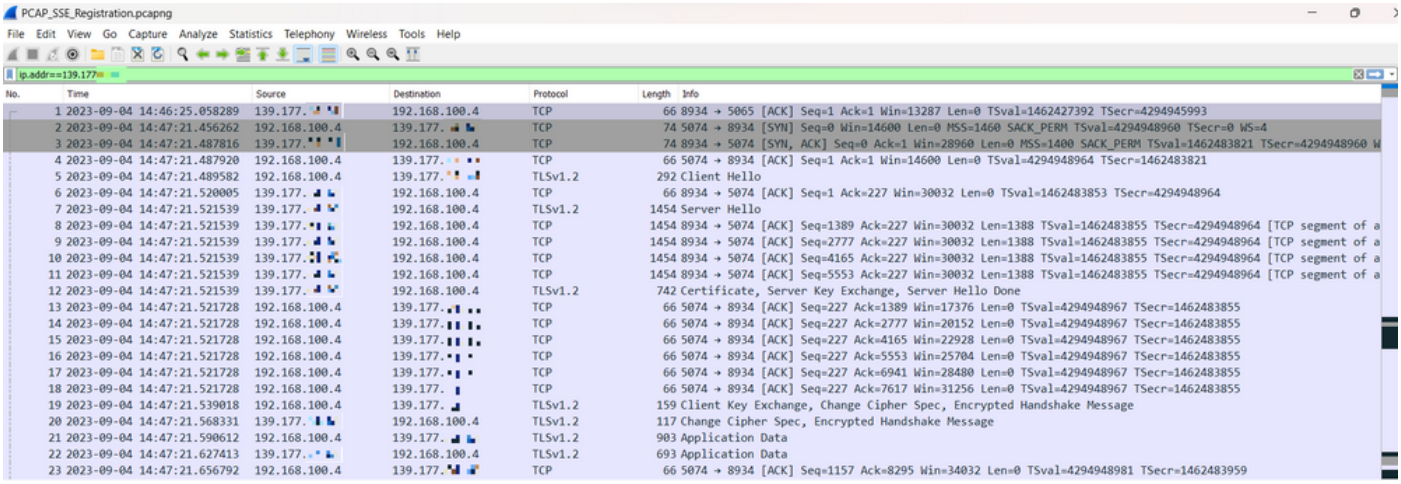
PC がドメインを解決できる場合は、以下のようになります。

```
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

パケットキャプチャ（登録プロセス）

電話機の登録用の IP アドレスを取得できます。パケットキャプチャでフィルタ処理を使用して TLS ハンドシェイクを確認できます。



PCAP SSE

パケットキャプチャは、TLS ハンドシェイクが失敗したかどうかを確認するのに役立ちます。

Cisco Webex Calling の TAC サポート

ログを分析して問題の根本原因を見つけるためにサポートが必要な場合は、Cisco Webex Calling TAC チームにお問い合わせください。

サポート関連情報

[Webex Calling のポート参照情報]

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。