

WxCでのプロビジョニングと登録のためのMPP電話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でデバイスをプロビジョニングする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 \(URLのプロビジョニング\)](#)

[WxCでのMPPデバイスの登録に関する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 TACサポートへの電話](#)

[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る場合に、プロビジョニングと登録の問題のためにWxCでMPP電話をトラブルシューティングする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。

- 基本的なネットワーク知識
- MPP電話

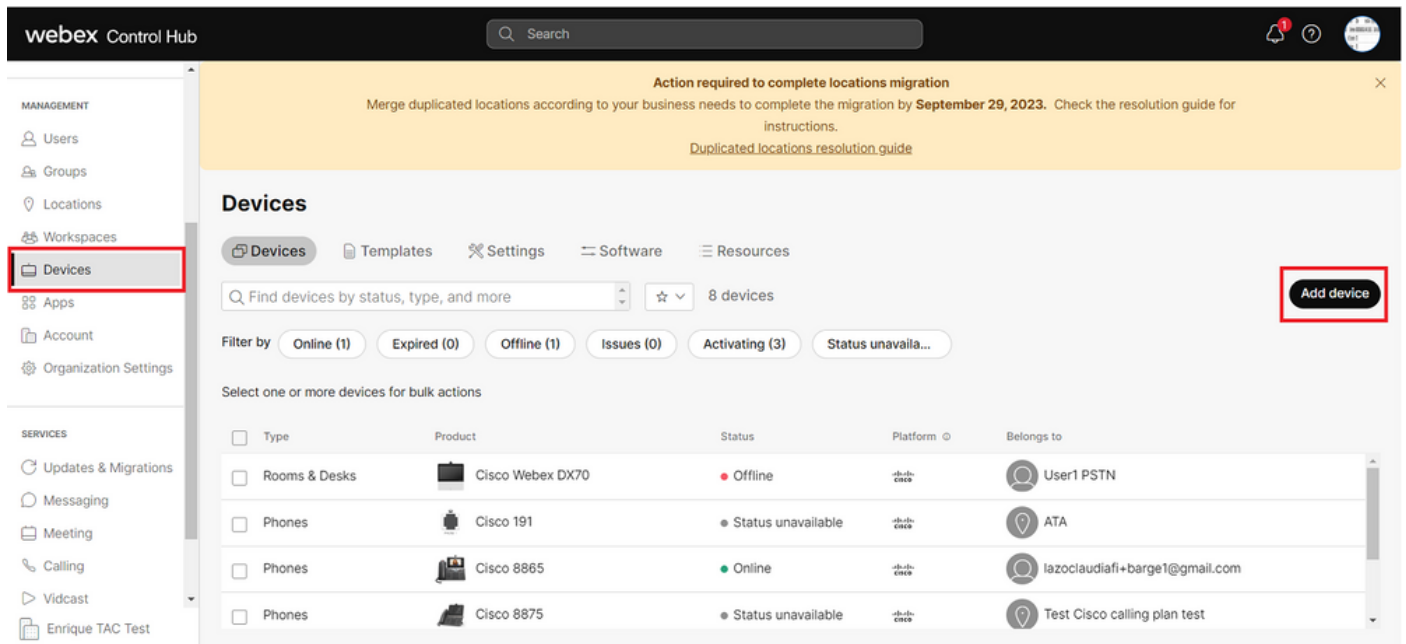
使用するコンポーネント

このドキュメントの情報は、78XX、88XXなどのMPP電話機にのみ基づいています。

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。

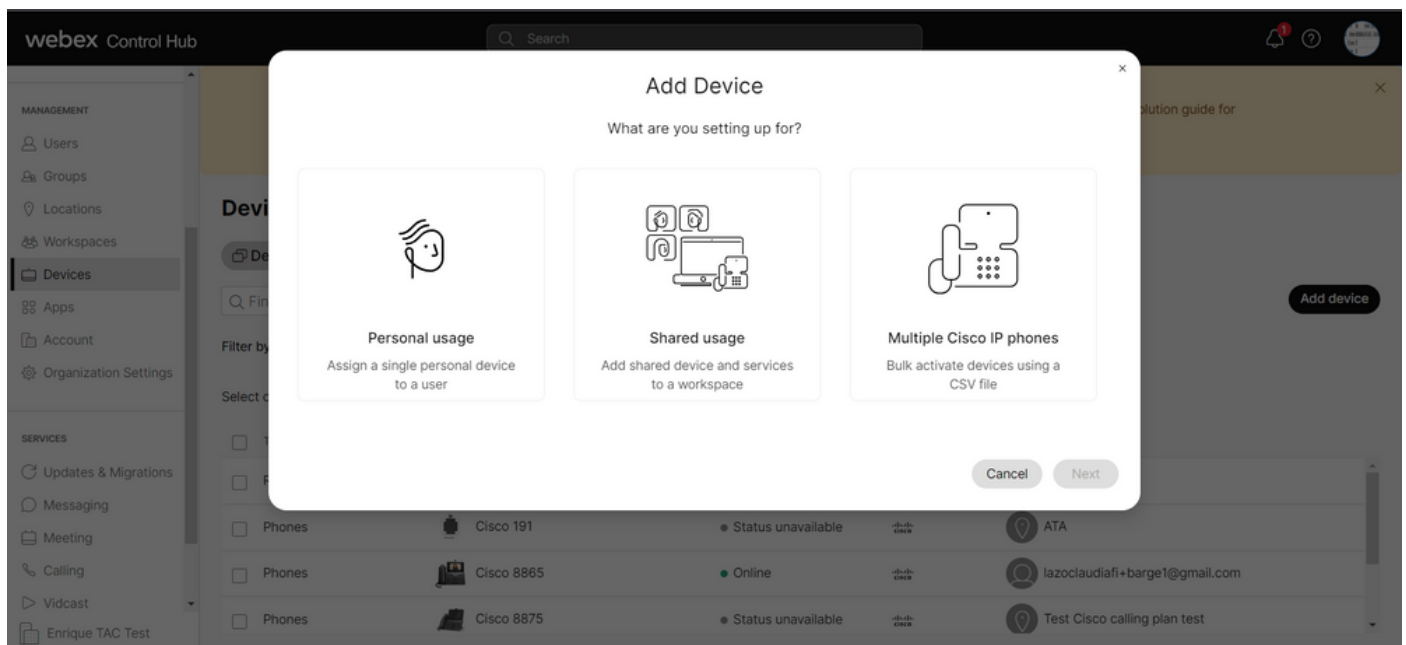
Control Hubでのデバイスの追加

ステップ 1 : admin.webex.comに移動し、管理者クレデンシャルを使用します。組織内で、Devices > Add deviceに移動します。



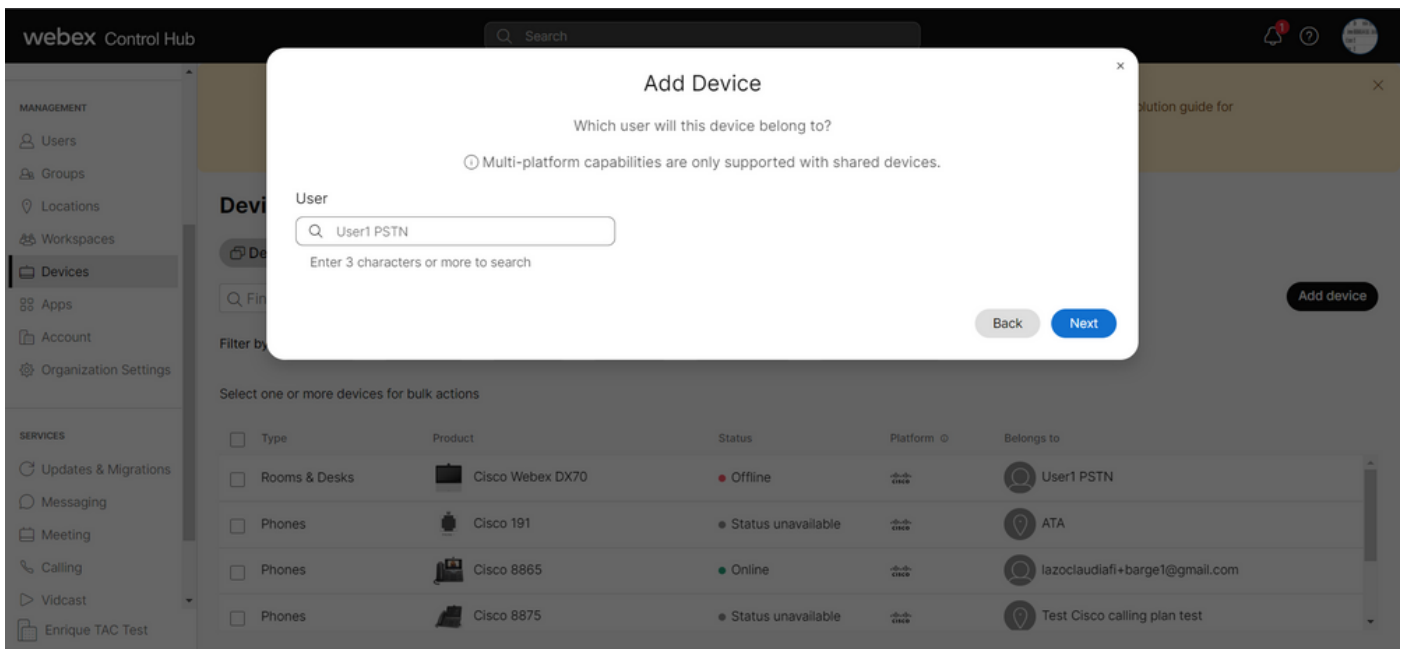
Devicesタブ

ステップ 2 : ユーザに割り当てる個人使用を選択するか、ワークスペースに割り当てる共有使用を選択します。(このシナリオでは、ユーザが使用されます)。



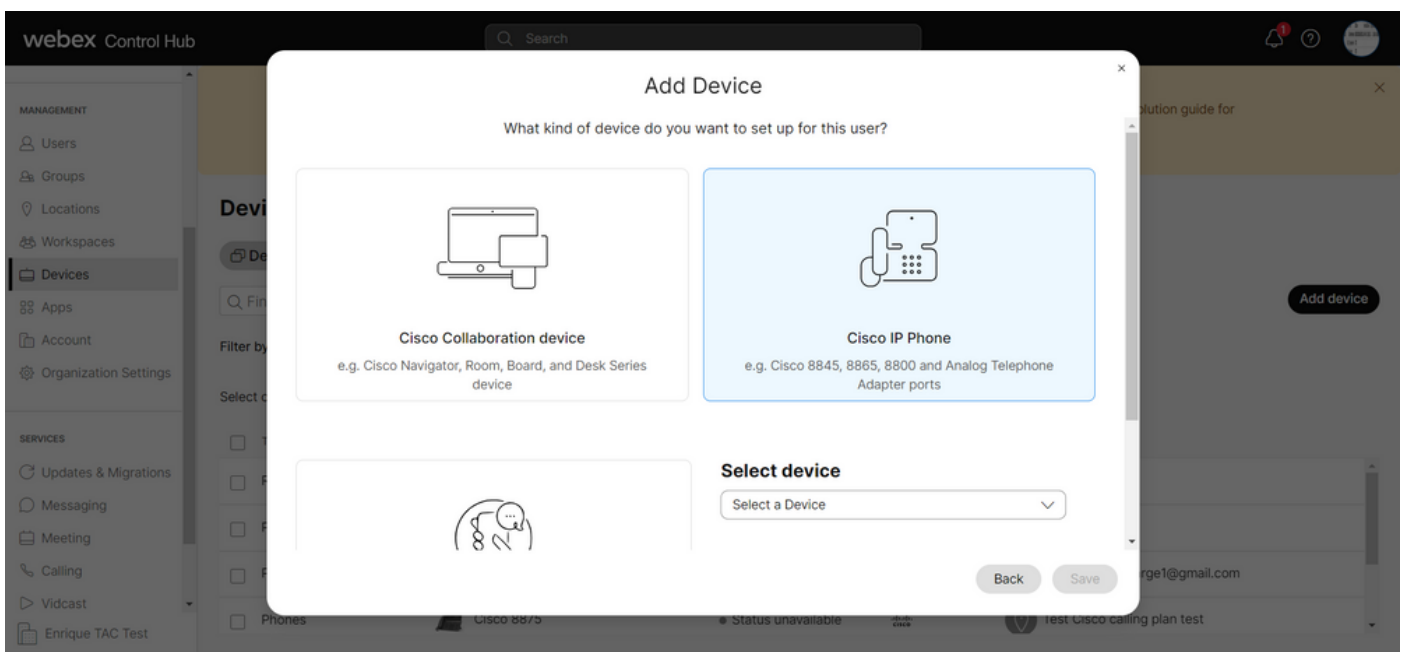
デバイスの追加

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



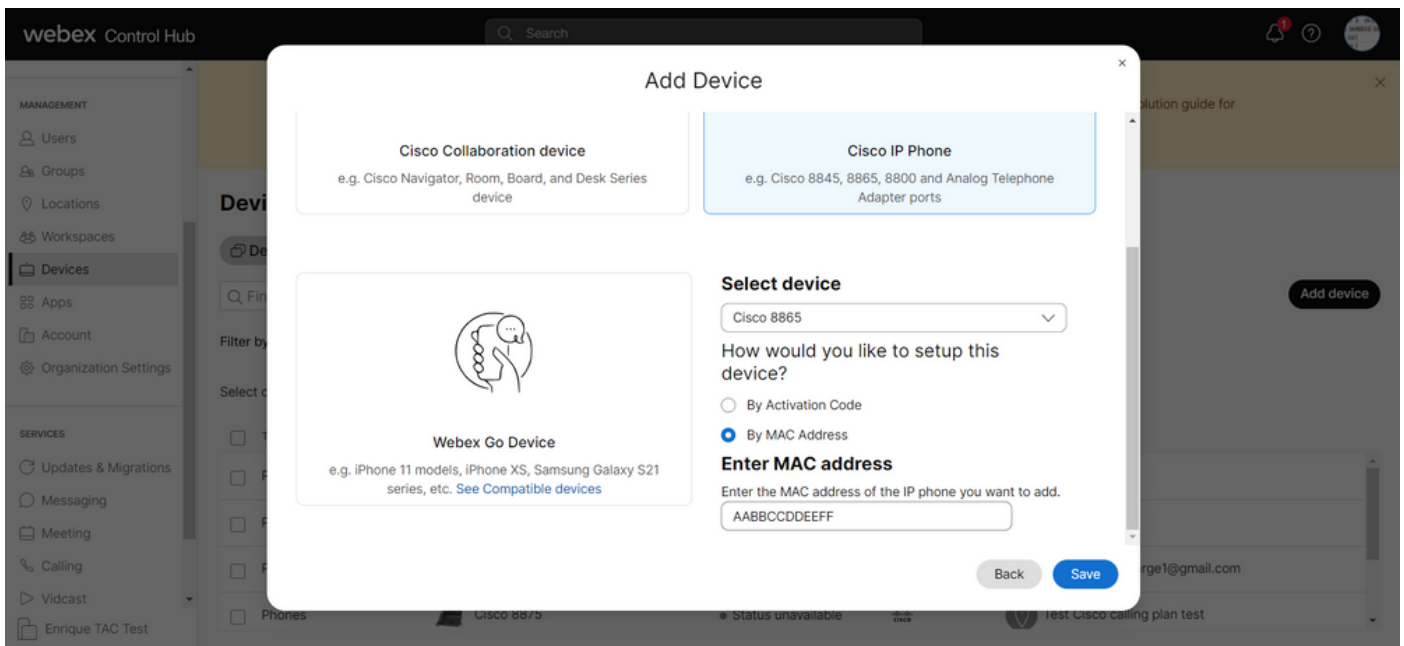
ユーザーの検索

ステップ 4 : Cisco IP Phoneを選択し、使用しているデバイスモデルを検索します。



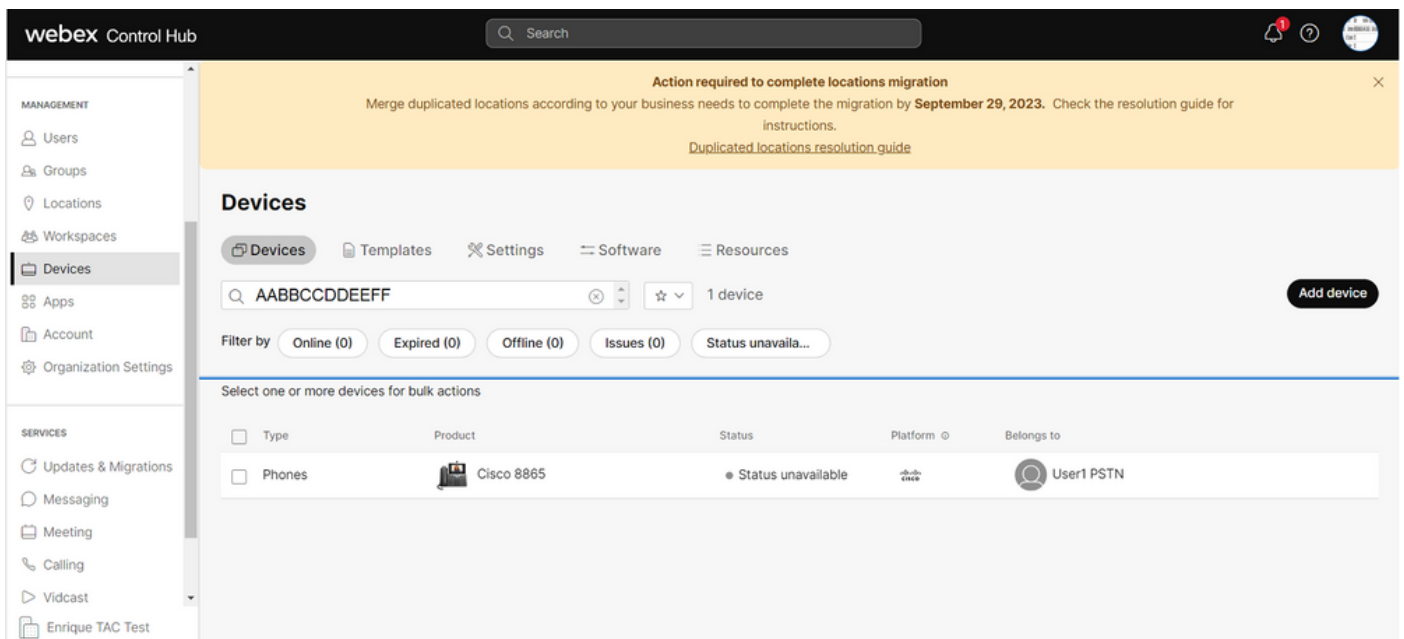
デバイスのモデルの選択

ステップ 5 : デバイスを選択したら、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、Saveをクリックします。



MACアドレスの追加

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

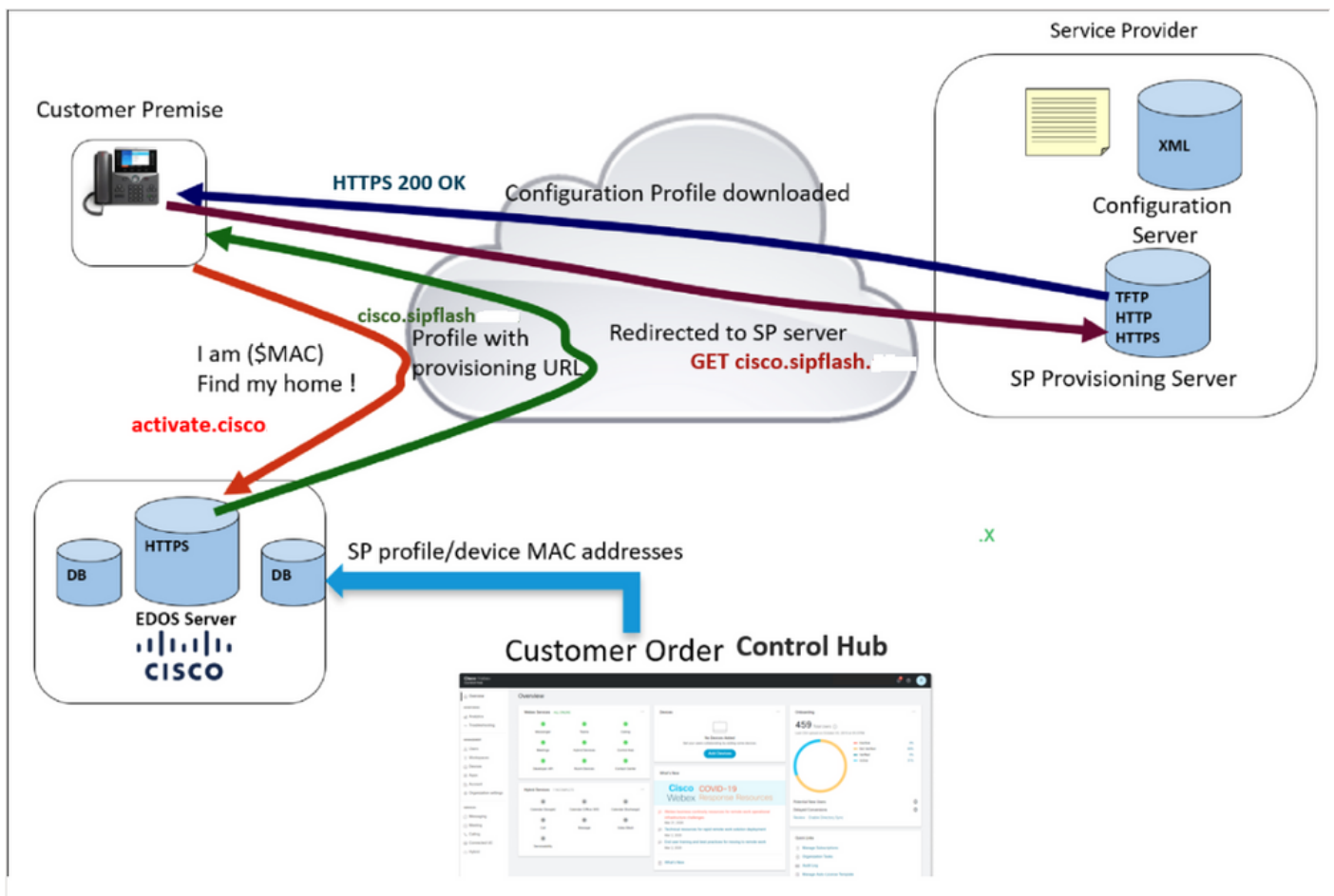


デバイスの検証

デバイスはまだプロビジョニングされていないため、ステータスは「Unavailable」と表示されます。デバイスがControl Hubに入ったら、次のステップはデバイスを工場出荷時の状態にリセットすることです。工場出荷時状態にリセットした後、デバイスはWxCサーバに設定ファイルの取得を行う必要があります。(これが提供プロセスです)。デバイスの画面に電話番号や内線番号が表示されると、デバイスは正常にプロビジョニングされます。

デバイスが適切な設定を表示していない場合は、デバイスをプロビジョニングするプロセスが失敗しました。

WxCでのデバイスのプロビジョニングプロセスの概要



プロビジョニング図

WxCでデバイスをプロビジョニングするプロセスのトラブルシューティング

次のように設定されている場合、MPPデバイスはWxCでプロビジョニングできません。

- DHCPサーバで設定されたTFTPサーバ
- オプション (OPT66、OPT160、OPT159、またはOPT150) が設定されていて、DHCPサーバから提供されている場合

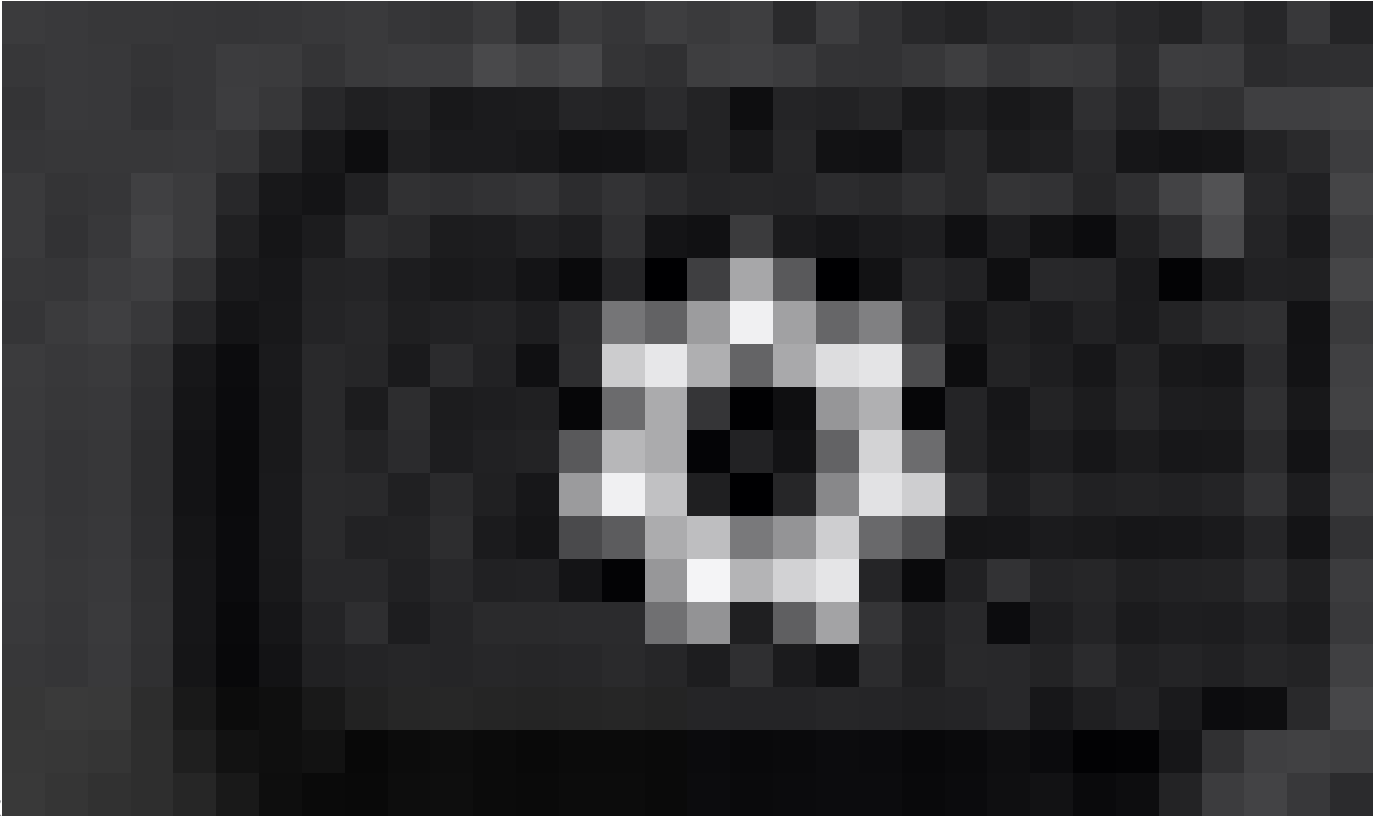
電話機がDHCPサーバからTFTP設定を取得したかどうかを確認するには、PRTログが必要です。

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。次の手順では、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、アプリケーションボタンの



設定ボタンを

押します。

ステップ2: Status > Report Problemの順に選択します。

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: Press Submit。

ログを送信したら、次の手順で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:IPアドレスが不明な場合は、Settings > Status > Network Status > IPv4 Statusから取得できます。

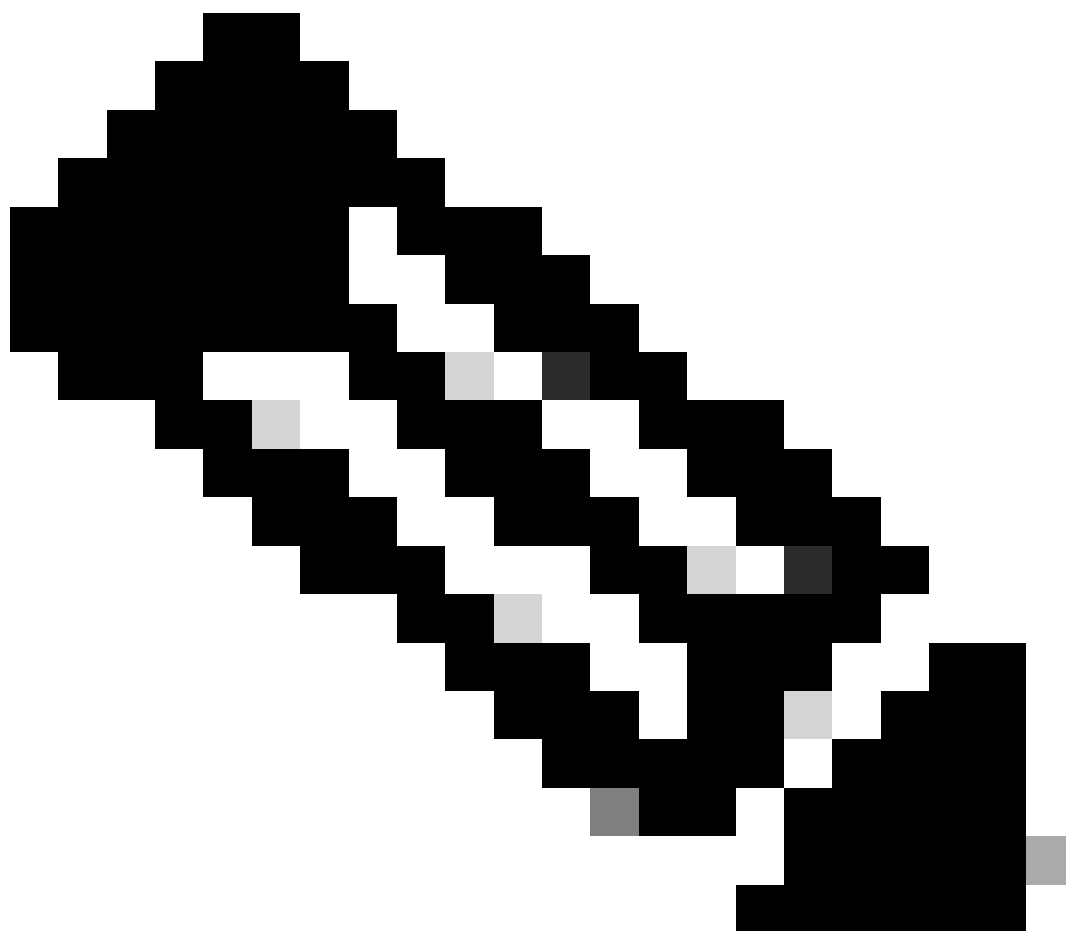
ステップ 2 : Info > Debug Info > Download the PRT logに移動します(リンクを右クリックして、Save As...を選択します)。



Web GUI

PRTログ

ログを開くと、次のようなビューが表示されます。



注：ログは圧縮されるため、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 Logビュー

デバイスをプロビジョニングする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関数「Find」を使用して、電話機にTFTPサーバ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探します。ログの他の行を参照すると、DHCP設定の詳細を確認できます。

```
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:
```

ログからわかるように、TFTP IPアドレスはDHCPサーバで設定されています。この原因は、電話機がWebexコーリングサーバの代わりにこのTFTPサーバにプロビジョニングしようとしたことにあります。

```
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サーバからTFTP設定とOPT設定を削除した後、デバイスをWxCで再プロビジョニングするプロセスを開始するには、デバイスを工場出荷時の状態にリセットする必要があります。電話機がデバイスをプロビジョニングするプロセスを最初に実行するのは、URL activate.cisco.comに要求を行うことです。電話機は、ドメインを解決するためにDNSサーバにクエリーを実行します。DNS解決が失敗した場合は、次のようになります。

<#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、次のように表示されます。

```
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要求から200 OKを受信すると、電話機はcisco.siplash.comに要求を行います。これは同じプロセスであり、電話はドメインの解決を試み、失敗した場合は次のように表示されます。

```
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、次のように表示されます。

```
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
```

DNSのトラブルシューティング (URLのプロビジョニング)

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にいる場合は、nslookupを使用して、DNSサーバ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(CLI)を開き、次の手順を実行します。

- nslookup ->入力
- set type=A -> Enterキー
- activate.cisco.com

PCがドメインを解決できる場合は、次のようになります。

```
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アクティブ化.cisco

同じプロセスをcisco.sipflash.xに対しても実行して、ドメインを解決できます。

```
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サーバを確認します。

WxCでのMPPデバイスの登録に関する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.webex.com
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.hosted-us10.bcld.webex.com
1725 NOT Sep 04 22:50:32.068975 (2059-2271) voice-RSE_DEBUG: rse_refresh_addr_list target:_sips._tcp.da02.hosted-us10.bcld.webex.com
1726 NOT Sep 04 22:50:32.069001 (2059-2271) voice-RSE_DEBUG: RR[0], name:_sips._tcp.da02.hosted-us10.bcld.webex.com
1727 INF Sep 04 22:50:32.069517 dnsmasq[560]: query[SRV] _sips._tcp.da02.hosted-us10.bcld.webex.com from 192.168.1.100
1728 INF Sep 04 22:50:32.069549 dnsmasq[560]: forwarded _sips._tcp.da02.hosted-us10.bcld.webex.com to 192.168.1.100
1729 INF Sep 04 22:50:32.082459 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bcld.webex.com
1730 INF Sep 04 22:50:32.082512 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hosted by 192.168.1.100
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.com
1733 INF Sep 04 22:50:32.082714 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bcld.webex.com is hosted by 192.168.1.100
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.bc1d.webex
1736 INF Sep 04 22:50:32.082786 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bc1d.webex.com is hosted
1737 INF Sep 04 22:50:32.082810 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bc1d.webex.com
1738 INF Sep 04 22:50:32.082838 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bc1d.webex
1739 INF Sep 04 22:50:32.082864 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bc1d.webex.com is hosted
1740 INF Sep 04 22:50:32.082888 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bc1d.webex.com
1741 INF Sep 04 22:50:32.082911 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bc1d.webex
1742 INF Sep 04 22:50:32.082936 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bc1d.webex.com is hosted
1743 INF Sep 04 22:50:32.082958 dnsmasq[560]: [cache_insert] _sips._tcp.da02.hosted-us10.bc1d.webex.com
1744 INF Sep 04 22:50:32.082981 dnsmasq[560]: caching SRV record=_sips._tcp.da02.hosted-us10.bc1d.webex
1745 INF Sep 04 22:50:32.083006 dnsmasq[560]: reply _sips._tcp.da02.hosted-us10.bc1d.webex.com is hosted
```

電話機がSRVドメインを解決できる場合は、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
```

これらのホスト名の1つから、電話はデバイスをWxC SBCに登録するためにホスト名の1つを取得します。

```
1774 NOT Sep 04 22:50:32.083015 (2059-2271) voice-RSE_DEBUG: Refreshing host[3]:hosted01aj-us10.bc1d.web
1775 INF Sep 04 22:50:32.083539 dnsmasq[560]: query[A] hosted01aj-us10.bc1d.webex.com from 127.0.0.1
1776 INF Sep 04 22:50:32.083567 dnsmasq[560]: found A record=hosted01aj-us10.bc1d.webex.com with TTL=81
1777 INF Sep 04 22:50:32.083590 dnsmasq[560]: cached hosted01aj-us10.bc1d.webex.com is 139.177.XXX.XXX
1778 INF Sep 04 22:50:32.083668 dnsmasq[560]: query[AAAA] hosted01aj-us10.bc1d.webex.com from 127.0.0.1
1779 INF Sep 04 22:50:32.083698 dnsmasq[560]: found A record=hosted01aj-us10.bc1d.webex.com with TTL=26
1780 INF Sep 04 22:50:32.083723 dnsmasq[560]: cached hosted01aj-us10.bc1d.webex.com is 2607:fcf0:9000:X
1781 NOT Sep 04 22:50:32.084094 (2059-2271) voice-RSE_DEBUG: Refresh host:hosted01aj-us10.bc1d.webex.com
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-c77bd320AM
From: <sip:w3nca1a025@XXXXX.example.com>;tag=fcd8304d2abdd95co0AM
To: <sip:w3nca1a025@XXXXX.example.com>AM
Call-ID: 98126dba-9df06bd9@192.168.100.6AM
CSeq: 6367 REGISTERAM
Max-Forwards: 70AM
Contact: <sip:w3nca1a025@192.168.100.6:5072;transport=tls>;expires=3600AM
User-Agent: Cisco-CP-8865-3PCC/12.0.2_<MAC_ADDRESS>_47cff26a-4713-41a1-8d75-28d7b638ffe8_2c01b5e7-53d5
Peripheral-Data: noneAM
Session-ID: 300e21a200105000a0002c01b5e753d5;remote=00000000000000000000000000000000AM
Content-Length: 0AM
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATEAM
Allow-Events: hold,talk,conferenceAM
Supported: replaces, sec-agree, record-awareAM
Accept-Language: enAM
```

デバイスは、WxC側から401 Unauthorizedメッセージを受信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:<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="BroadWorksX1m5h6zucT8ymkkBW",algorithm=MD5
Contact:<sip:w3nca1a025@192.168.100.6:5072;transport=tls>;expires=120^M
Content-Length:0^M
^M
```

デバイスは認証ヘッダー付きで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: <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="BroadWorksX1m5h6zucT8ymkkBW",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
```

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:<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
```

このプロセスの後、デバイスが起動し、WxCサービスに登録されている必要があります。

DNSのトラブルシューティング (URLの登録)

デバイスにDNS解決の問題がある同じネットワークにいる場合は、nslookupを使用して、DNSサ

ーバ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(CLI)を開き、次の手順を実行します。

- nslookup ->入力
- set type=SRV ->入力
- _sips._tcp.da02.hosted-us10.bcl.d.webex.com

PCがドメインを解決できる場合は、次のようになります。

```

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

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

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

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

```


パケットキャプチャ (登録プロセス)

電話機に登録されている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を使用して、TLSハンドシェイクを確認できます。

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-04 14:46:25.058289	139.177.0.0	192.168.100.4	TCP	66	8934 → 5065 [ACK] Seq=1 Ack=1 Win=13287 Len=0 TSval=1462427392 TSecr=4294945993
2	2023-09-04 14:47:21.456262	192.168.100.4	139.177.0.0	TCP	74	5074 → 8934 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294948960 TSecr=0 WS=4
3	2023-09-04 14:47:21.487816	139.177.0.0	192.168.100.4	TCP	74	8934 → 5074 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM TSval=1462483821 TSecr=4294948960 WS=4
4	2023-09-04 14:47:21.487920	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294948964 TSecr=1462483821
5	2023-09-04 14:47:21.489582	192.168.100.4	139.177.0.0	TLSv1.2	292	Client Hello
6	2023-09-04 14:47:21.520005	139.177.0.0	192.168.100.4	TCP	66	8934 → 5074 [ACK] Seq=1 Ack=227 Win=30032 Len=0 TSval=1462483853 TSecr=4294948964
7	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TLSv1.2	1454	Server Hello
8	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TCP	1454	8934 → 5074 [ACK] Seq=1389 Ack=227 Win=30032 Len=1388 TSval=1462483855 TSecr=4294948964 [TCP segment of a
9	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TCP	1454	8934 → 5074 [ACK] Seq=2777 Ack=227 Win=30032 Len=1388 TSval=1462483855 TSecr=4294948964 [TCP segment of a
10	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TCP	1454	8934 → 5074 [ACK] Seq=4165 Ack=227 Win=30032 Len=1388 TSval=1462483855 TSecr=4294948964 [TCP segment of a
11	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TCP	1454	8934 → 5074 [ACK] Seq=5553 Ack=227 Win=30032 Len=1388 TSval=1462483855 TSecr=4294948964 [TCP segment of a
12	2023-09-04 14:47:21.521539	139.177.0.0	192.168.100.4	TLSv1.2	742	Certificate, Server Key Exchange, Server Hello Done
13	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=1389 Win=17376 Len=0 TSval=4294948967 TSecr=1462483855
14	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=2777 Win=20152 Len=0 TSval=4294948967 TSecr=1462483855
15	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=4165 Win=22928 Len=0 TSval=4294948967 TSecr=1462483855
16	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=5553 Win=25704 Len=0 TSval=4294948967 TSecr=1462483855
17	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=6941 Win=28480 Len=0 TSval=4294948967 TSecr=1462483855
18	2023-09-04 14:47:21.521728	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=227 Ack=7617 Win=31256 Len=0 TSval=4294948967 TSecr=1462483855
19	2023-09-04 14:47:21.539018	192.168.100.4	139.177.0.0	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20	2023-09-04 14:47:21.568331	139.177.0.0	192.168.100.4	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
21	2023-09-04 14:47:21.590612	192.168.100.4	139.177.0.0	TLSv1.2	903	Application Data
22	2023-09-04 14:47:21.627413	139.177.0.0	192.168.100.4	TLSv1.2	693	Application Data
23	2023-09-04 14:47:21.656792	192.168.100.4	139.177.0.0	TCP	66	5074 → 8934 [ACK] Seq=1157 Ack=8295 Win=34032 Len=0 TSval=4294948981 TSecr=1462483959

PCAPの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 TACサポートへの電話

ログを分析して問題の根本原因を突き止めるための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通話のポート参照情報](#)

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。