Dépannage du téléphone MPP dans WxC pour l'approvisionnement et l'enregistrement

Table des matières

- Introduction
  - Exigences
  - Composants utilisés
- Ajout du périphérique dans le Control Hub
- Bref résumé du processus de provisionnement d'un périphérique dans WxC
- Dépanner le processus de provisionnement d'un périphérique dans WxC
  - Générer les journaux PRT à partir d'un périphérique MPP
  - Générer le PRT à partir du périphérique
  - Journaux PRT
  - Dépannage de DNS (provisionnement des URL)
- Dépannage de l'enregistrement d'un périphérique MPP dans WxC
  - Dépannage de DNS (Register URLs)
  - Capture de paquets (processus d'enregistrement)
  - Assistance TAC par téléphone Cisco Webex
  - Informations relatives au support

Introduction

Ce document décrit comment dépanner des téléphones MPP dans WxC pour des problèmes de provisionnement et d'enregistrement lorsque le périphérique est ajouté par adresse MAC.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du réseau
- Téléphones MPP

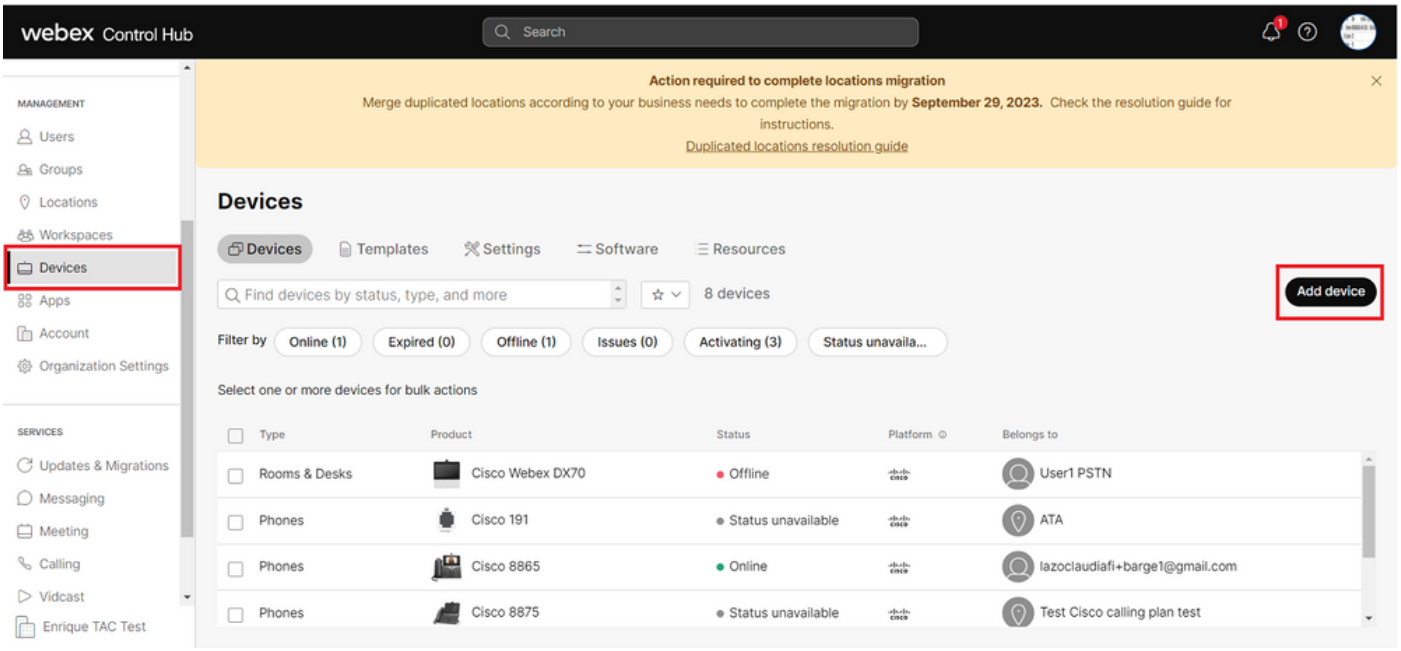
Composants utilisés

Les informations contenues dans ce document sont basées uniquement sur les téléphones MPP tels que 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

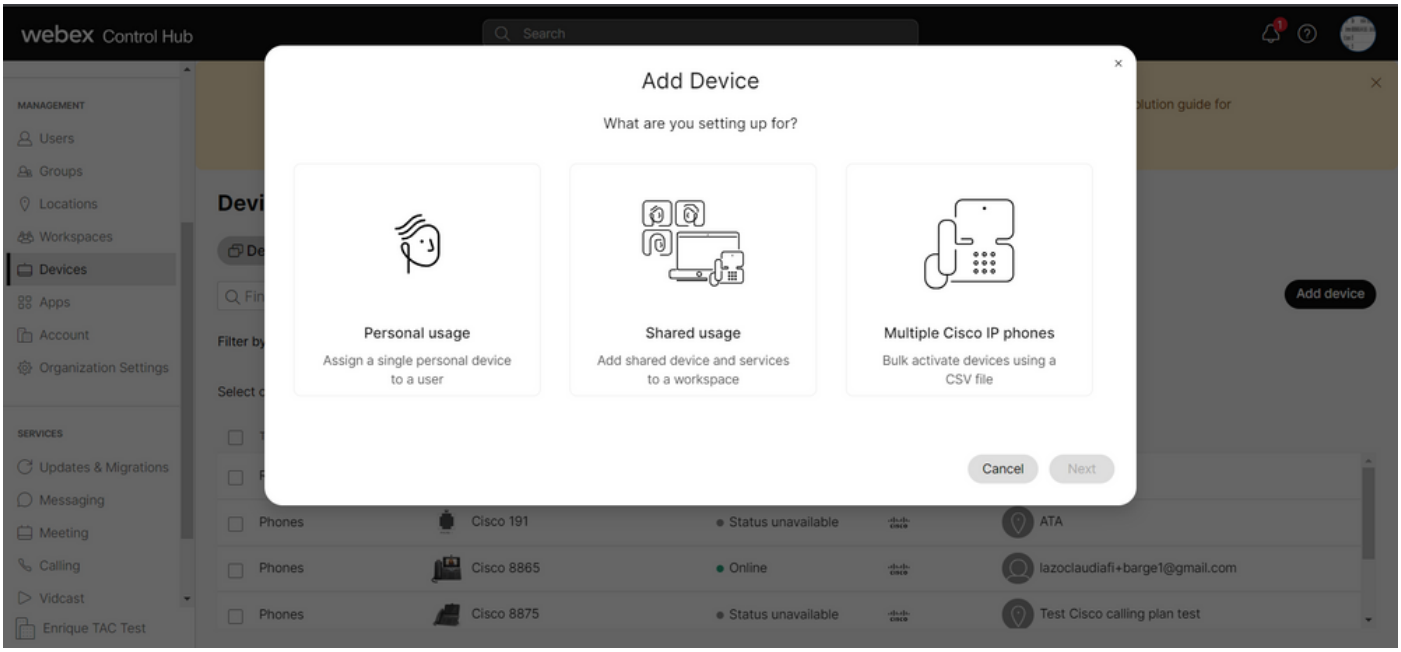
Ajout du périphérique dans le Control Hub

Étape 1. Accédez à admin.webex.com et utilisez les informations d'identification de l'administrateur. Dans l'organisation, accédez à Périphériques > Ajouter un périphérique :



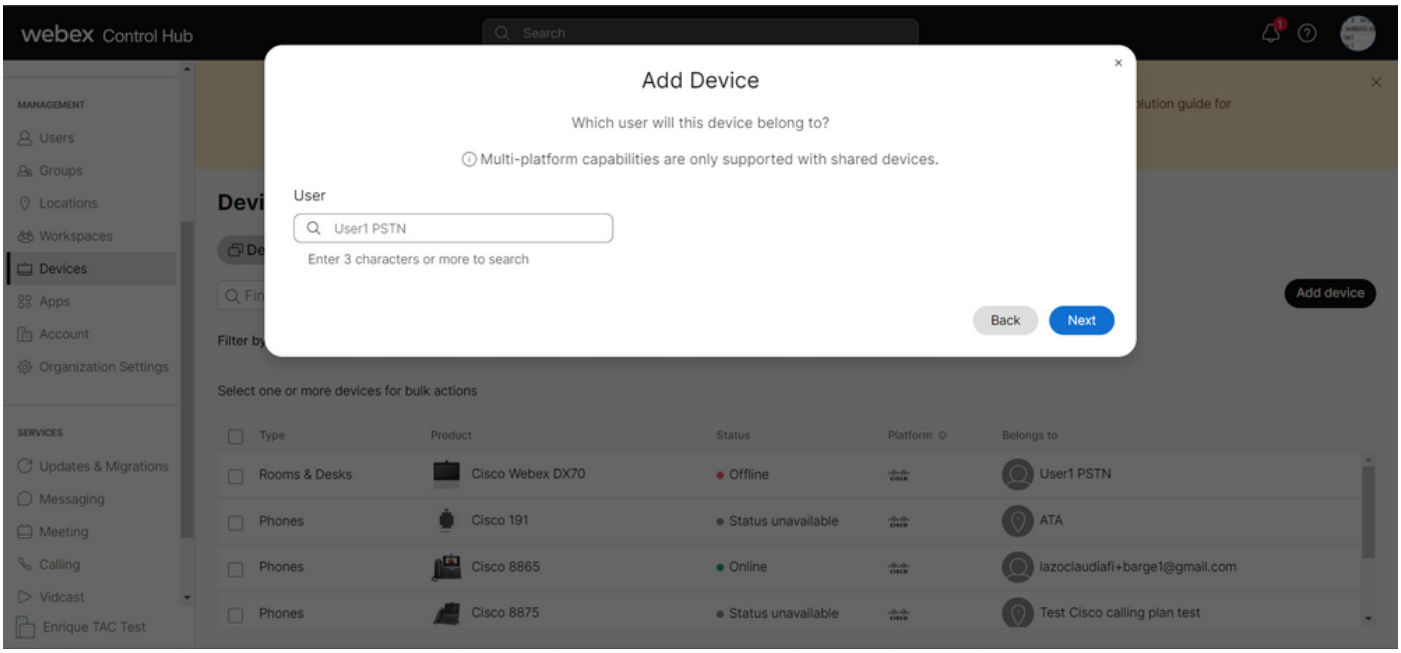
Onglet Périphériques

Étape 2. Sélectionnez Utilisation personnelle à affecter à un utilisateur ou Utilisation partagée à affecter à un espace de travail. (Dans ce scénario, un utilisateur est utilisé.)



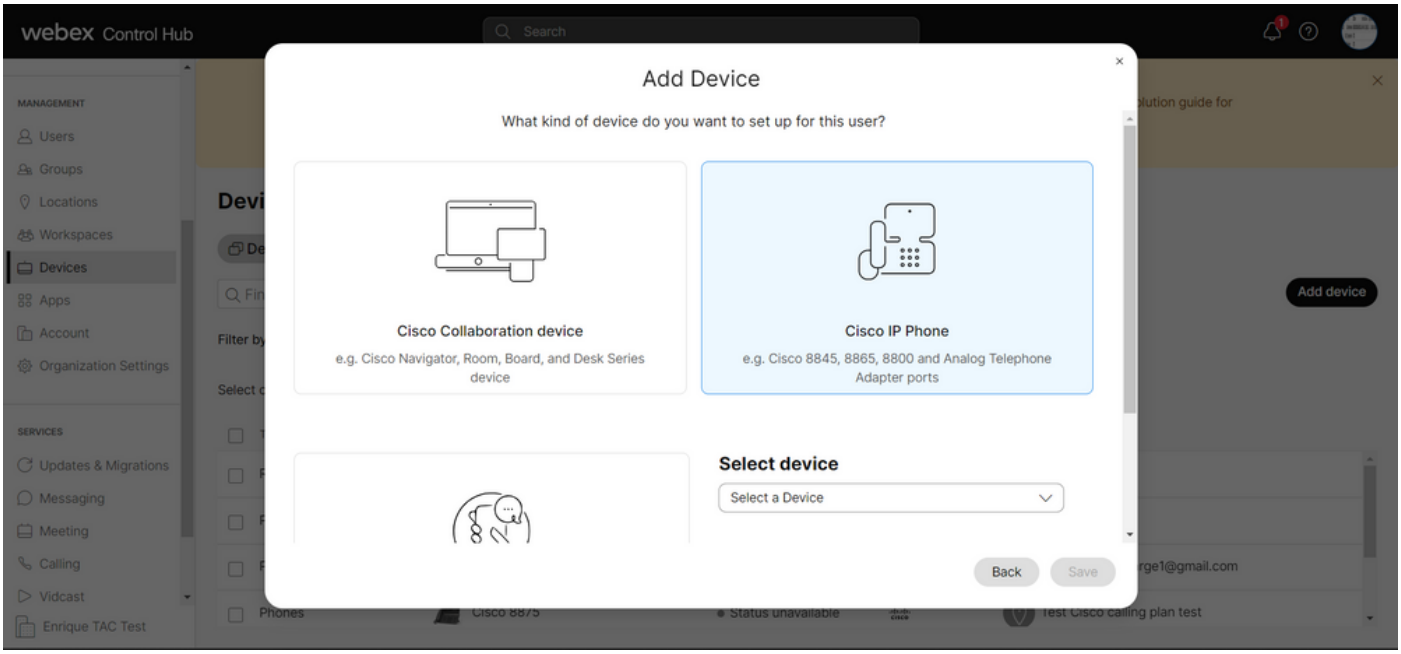
Ajouter un périphérique

Étape 3. Recherchez et sélectionnez l'utilisateur que vous souhaitez affecter à ce périphérique et cliquez sur Next :



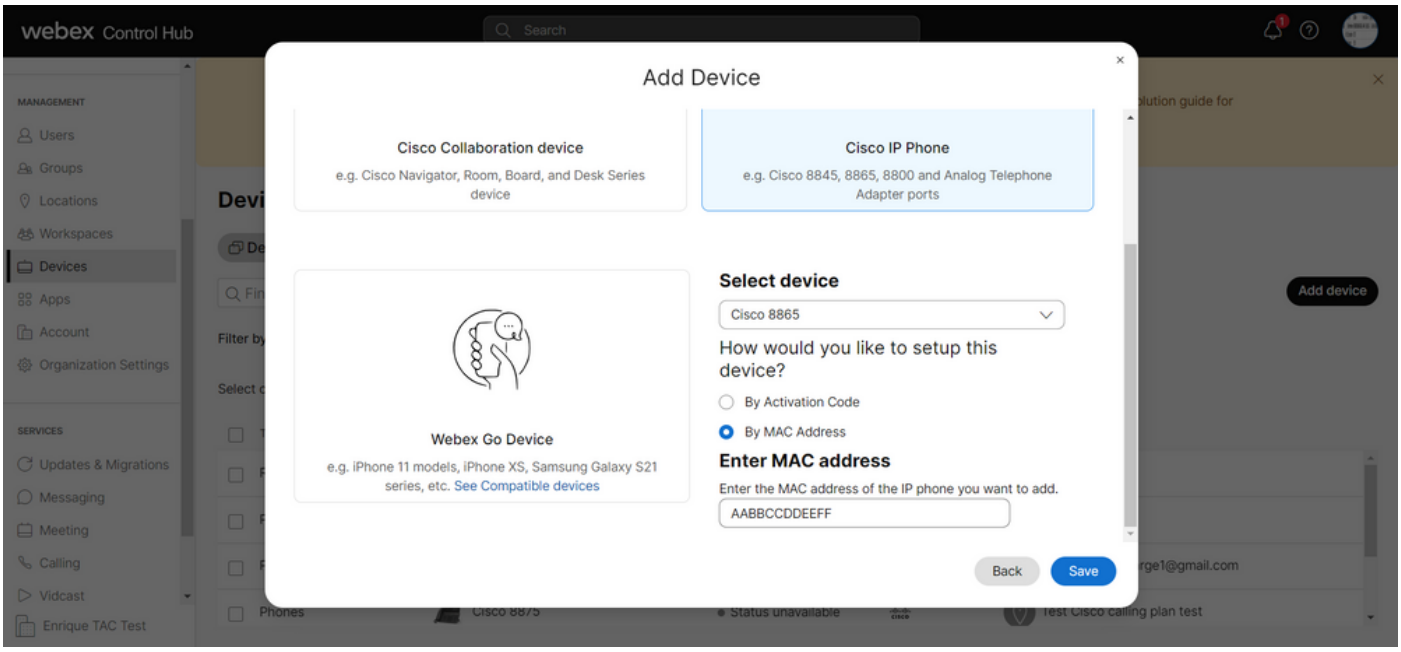
Rechercher un utilisateur

Étape 4. Sélectionnez le téléphone IP Cisco et recherchez le modèle de votre périphérique :



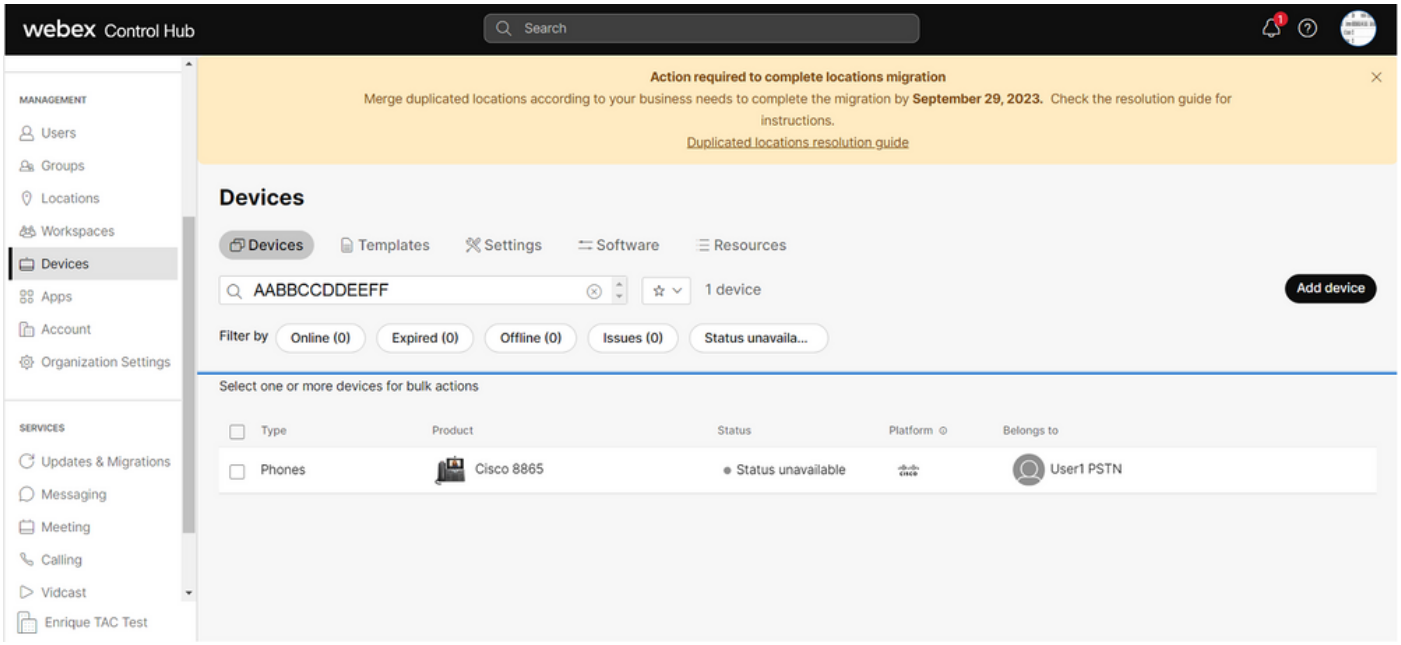
Sélectionner le modèle de périphérique

Étape 5. Une fois le périphérique sélectionné, sélectionnez l'option By MAC Address et entrez l'adresse MAC du périphérique et cliquez sur Save:



Ajouter une adresse MAC

Étape 6. Une fois que le périphérique est dans le Control Hub, vous pouvez vérifier qu'il a été ajouté correctement lorsque vous recherchez l'adresse MAC dans la barre de recherche :



Vérification du dispositif

L'état indique « Non disponible », car le périphérique n'est toujours pas provisionné. Une fois que le périphérique est dans le Control Hub, l'étape suivante consiste à le réinitialiser en usine. Après la réinitialisation en usine, le périphérique doit demander aux serveurs WxC d'obtenir les fichiers de configuration. (Il s'agit du processus de provisionnement.) Le périphérique est correctement configuré lorsque le périphérique affiche le numéro de téléphone et/ou le poste à l'écran.

Si vous constatez que le périphérique n'affiche pas la configuration appropriée, le processus de mise en service du périphérique a échoué.

Bref résumé du processus de provisionnement d'un périphérique dans WxC

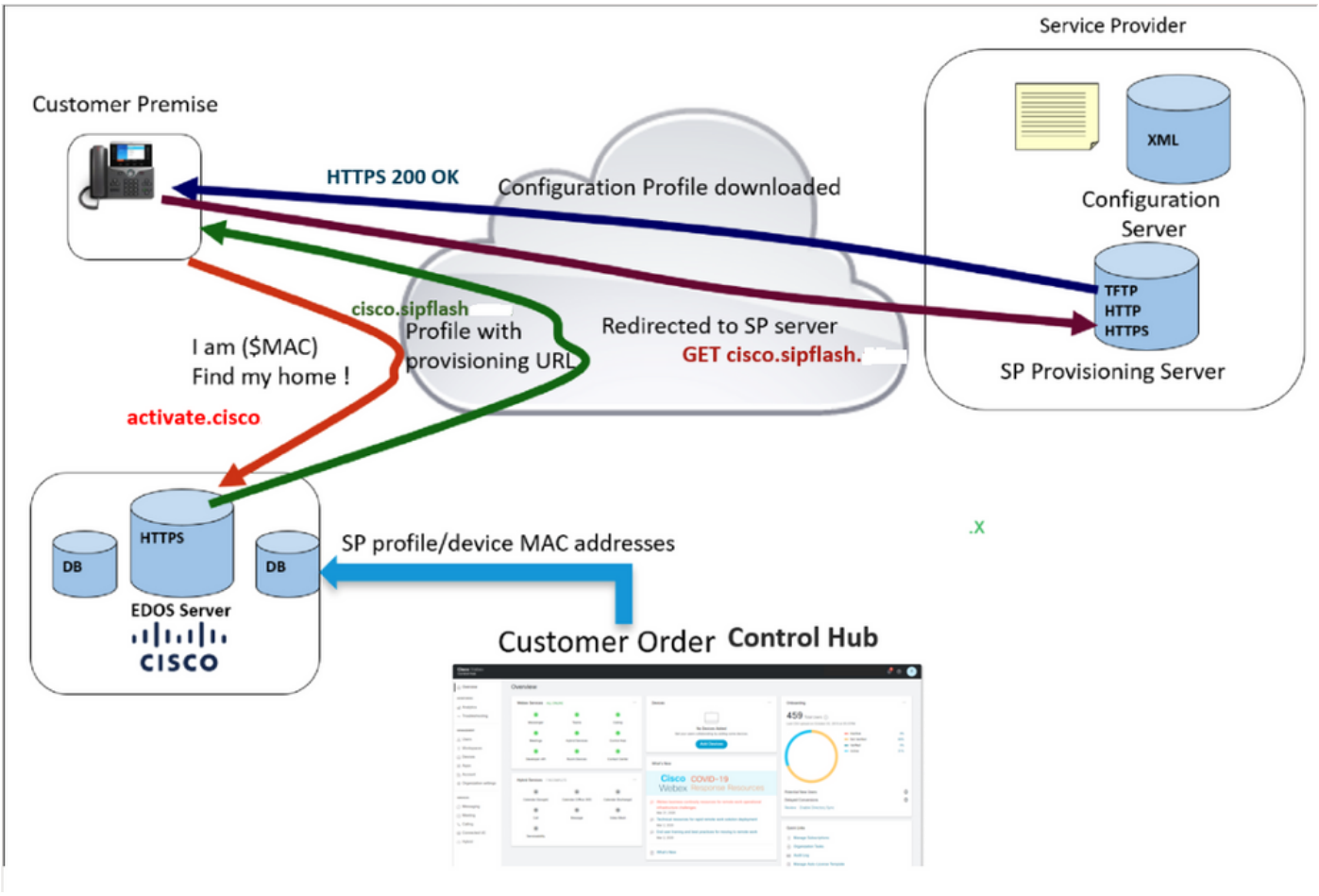


Diagramme de provisionnement

Dépanner le processus de provisionnement d'un périphérique dans WxC

Le périphérique MPP ne peut pas être configuré avec WxC s'il est configuré avec :

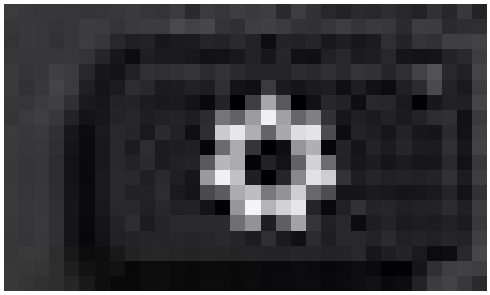
- Un serveur TFTP configuré dans le serveur DHCP
- Si Option (OPT66, OPT160, OPT159 ou OPT150) est configuré et fourni par le serveur DHCP

Pour voir si le téléphone a pris une configuration TFTP à partir d'un serveur DHCP, les journaux PRT sont nécessaires.

Générer les journaux PRT à partir d'un périphérique MPP

Envoyer à partir des journaux PRT à partir du téléphone. La procédure suivante indique comment générer les journaux PRT.

Générer le PRT à partir du périphérique

Étape 1.Sur le périphérique, appuyez sur le bouton Applications 

Bouton Paramètres

.

Étape 2.Accédez à Status > Report Problem.

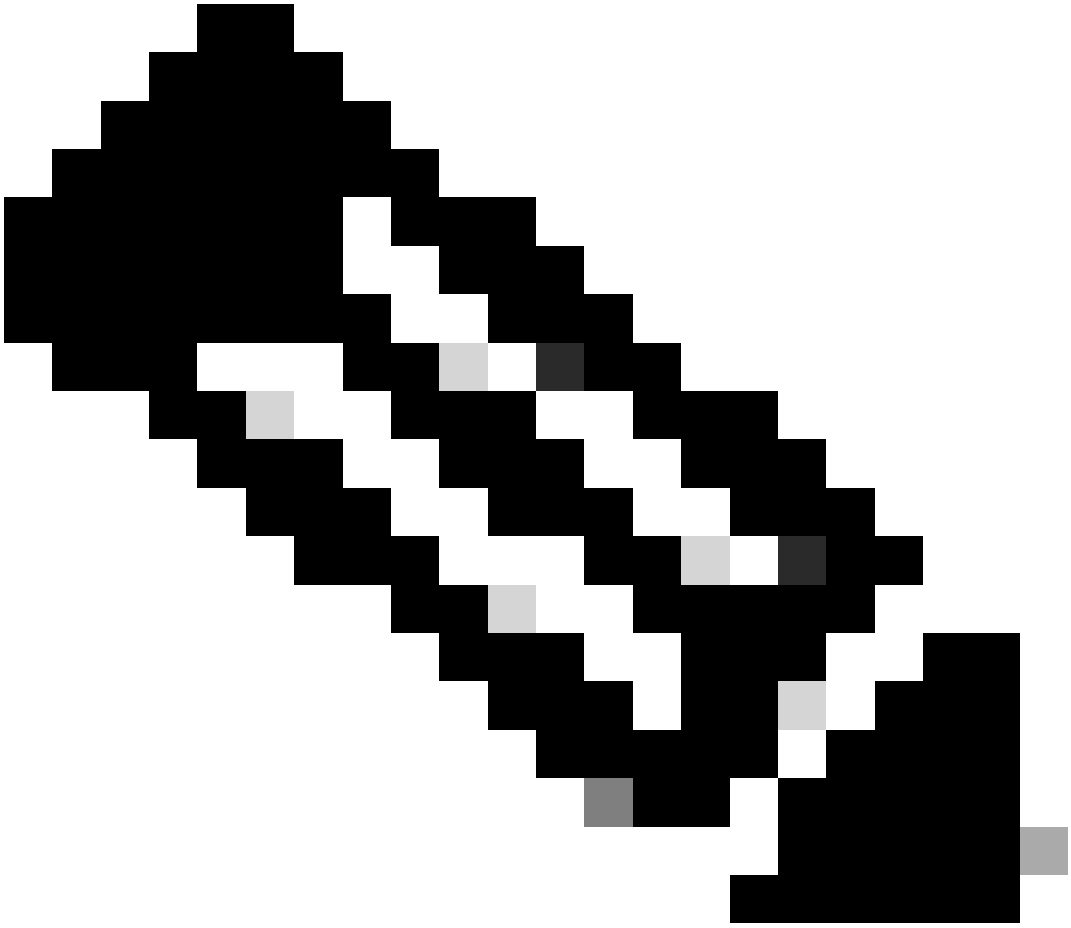
Étape 3.Entrez la date et l’heure du problème.

Étape 4. Sélectionnez une description dans la liste.

Étape 5.Appuyez sur Envoyer.

Une fois les journaux envoyés, reportez-vous aux étapes suivantes pour télécharger les journaux PRT :

Étape 1 : connexion à https://IP_ADDRESS_PHONE/



Remarque : Remarque : Si l'adresse IP est inconnue, elle peut être obtenue à partir de Paramètres > État > État du réseau > État IPv4

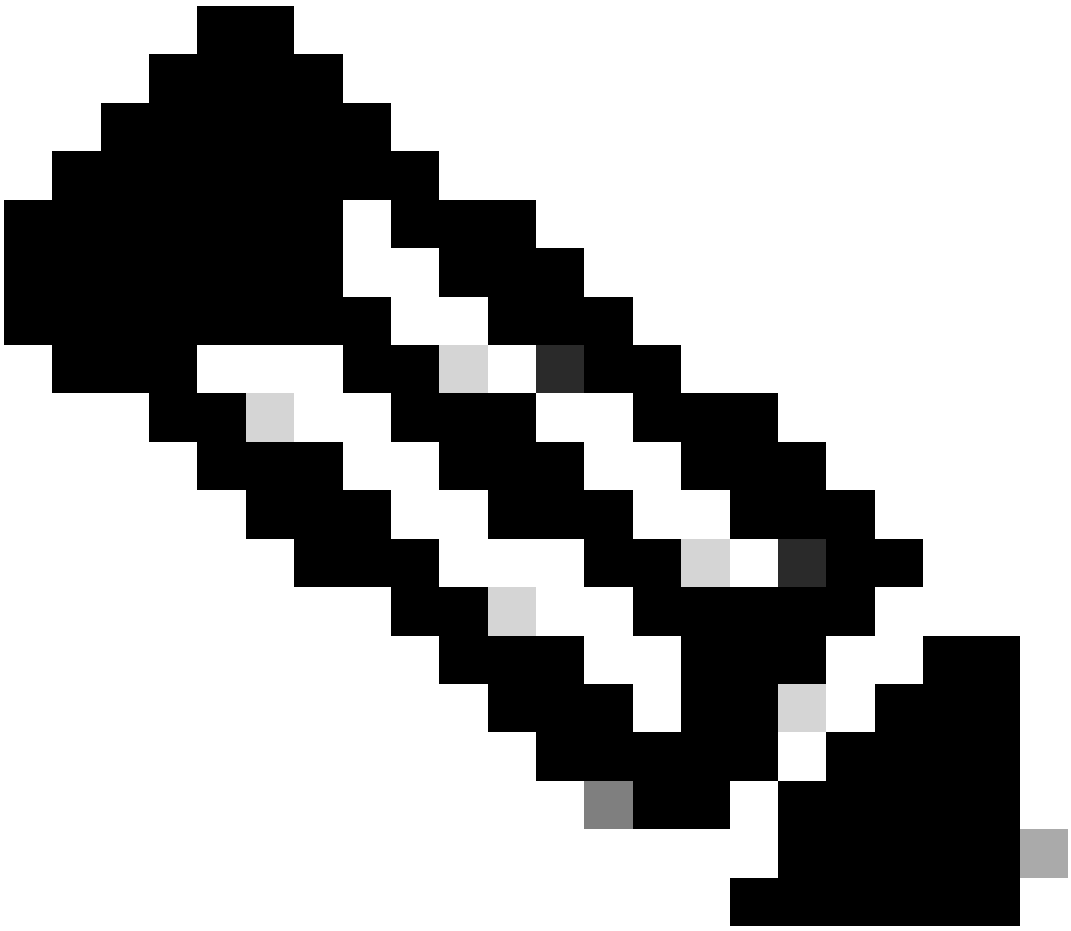
Étape 2. Accédez à Info > Debug Info > Download the PRT log (Cliquez avec le bouton droit sur le lien et sélectionnez Save As...)



GUI Web

Journaux PRT

Lorsque vous ouvrez les journaux, vous pouvez voir une vue comme celle-ci :



Remarque : Vous pouvez ouvrir les journaux avec un programme comme WinRAR puisque les journaux sont compressés.

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...	

Afin d'analyser le processus de provisionnement du périphérique, le journal appelé logcat doit être ouvert. Il peut être ouvert avec un éditeur de texte comme Notepad ou Notepad++.
La fonction "Rechercher" de l'éditeur de texte peut être utilisée afin de déterminer si le téléphone a un serveur TFTP configuré. Utilisez DHCP-tftpsvr1 ou DHCP-tftpsvr2 pour rechercher la ligne spécifique pour ce journal. Si vous regardez les autres lignes des journaux, vous trouverez plus d'informations sur la configuration DHCP :

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:

Comme vous pouvez le voir dans le journal, une adresse IP TFTP est configurée dans le serveur DHCP. Le téléphone a donc tenté de mettre en service ce serveur TFTP au lieu des serveurs Webex Calling.

```
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
```

Après avoir supprimé une configuration TFTP et une configuration OPT du serveur DHCP, vous devez réinitialiser le périphérique en usine afin de lancer le processus de réapprovisionnement du périphérique avec WxC.
La première tentative que le téléphone fait avec le processus de provisioning du périphérique est d'effectuer une requête à l'URL activate.cisco.com. Le téléphone envoie une requête au serveur DNS afin de résoudre le domaine. Si la résolution DNS échoue, elle peut ressembler à ceci :

<#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
```

Si le téléphone peut résoudre le domaine, il peut se présenter comme suit :

```
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
```

Après avoir reçu le 200 OK de la requête GET à activate.cisco.com, le téléphone envoie une requête à cisco.siplash.com. Il s'agit du même processus, le téléphone tente de résoudre le domaine et s'il échoue, il peut se présenter comme suit :

```
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"
```

Si le téléphone peut résoudre le domaine, il peut se présenter comme suit :

```
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
```

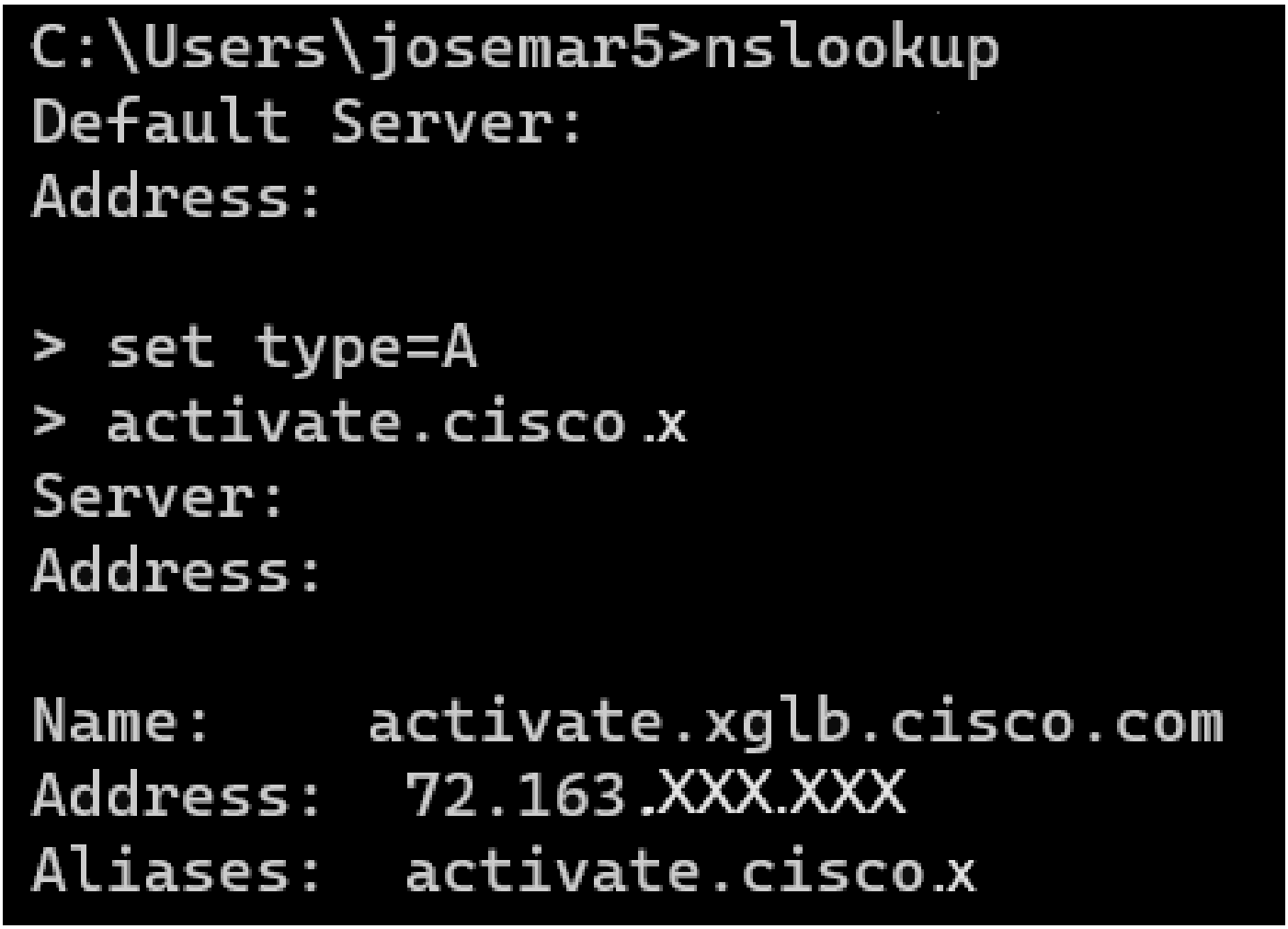
```
Accept-Charset: iso-8859-1^M
^M
1996 NOT Sep 04 22:49:29.506969 <
1997 NOT Sep 04 22:49:29.507037 HTTP/1.1 200 OK^M
```

Dépannage de DNS (provisionnement des URL)

Si vous êtes sur le même réseau où les périphériques ont des problèmes avec la résolution DNS, une commande nslookup peut être utilisée pour vérifier si le serveur DNS est capable de résoudre le domaine. Ouvrez l'interface de ligne de commande et procédez comme suit :

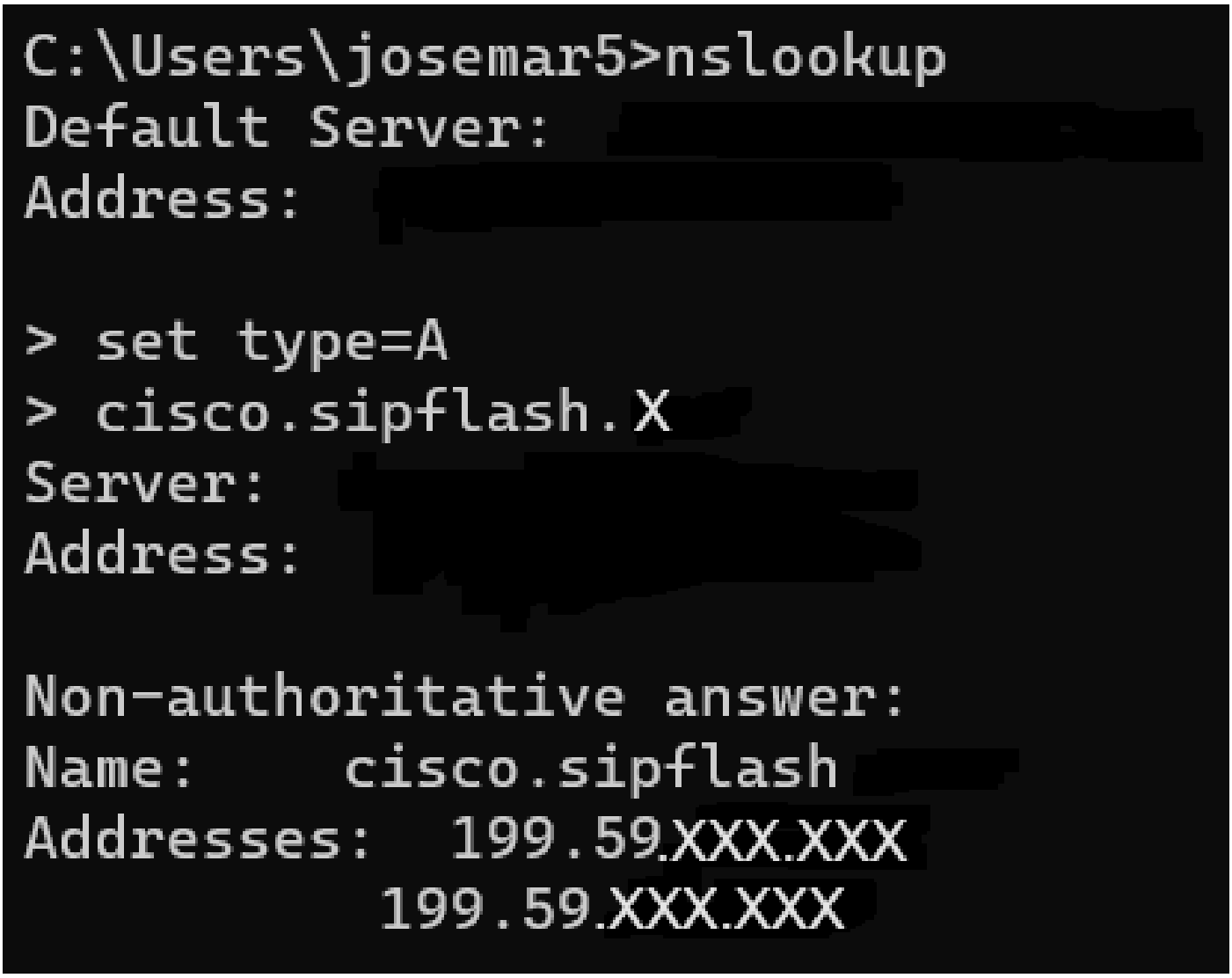
- nslookup -> Entrée
- set type=A -> Entrée
- activate.cisco.com

Si le PC peut résoudre le domaine, il peut se présenter comme suit :



nslookup activate.cisco

Le même processus peut être effectué pour que cisco.sipflash.x résolve le domaine :



nslookup cisco sipflash

Si le PC ne parvient pas à résoudre les domaines, consultez votre serveur DNS.

Dépannage de l'enregistrement d'un périphérique MPP dans WxC

Dans cet exemple, le proxy sortant est da02.hosted-us10.bcld.webex.com. Le téléphone tente de résoudre le domaine SRV :

```
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
```

Si le téléphone peut résoudre le domaine SRV, il obtient les noms d'hôte :

```
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
```

À partir de l'un de ces noms d'hôte, le téléphone prend l'un d'eux pour enregistrer le périphérique sur le 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:

        ;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
```

Le périphérique doit recevoir un message 401 Unauthorized du côté WxC :

```
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
```

Le périphérique envoie l'en-tête REGISTER avec l'en-tête Authorization :

```
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
```

Ensuite, le périphérique reçoit un 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:

        ;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
```

Après ce processus, le périphérique doit être activé et enregistré auprès des services WxC.

Dépannage de DNS (Register URLs)

Si vous vous trouvez sur le même réseau où les périphériques rencontrent des problèmes avec la résolution DNS, la commande nslookup peut être utilisée pour vérifier si le serveur DNS est en mesure de résoudre le domaine. Ouvrez l'interface de ligne de commande et procédez comme suit :

- nslookup -> Entrée
- set type=SRV -> Entrée
- _sips._tcp.da02.hosted-us10.bcld.webex.com

Si le PC peut résoudre le domaine, il peut se présenter comme suit :

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

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

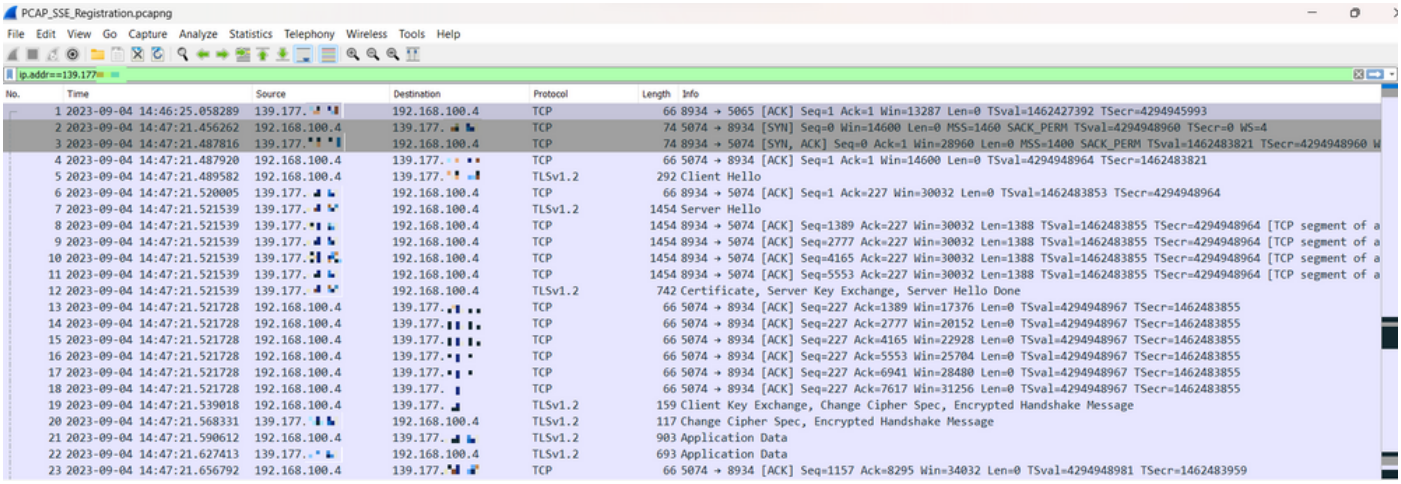
Non-authoritative answer:
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service location:
          priority       = 5
          weight         = 50
          port           = 8934
          svr hostname   = hosted01ai-us10.bcld.webex.com
_sips._tcp.da02.hosted-us10.bcld.webex.com      SRV service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

Capture de paquets (processus d’enregistrement)

Vous pouvez prendre l'adresse IP du téléphone pour l'enregistrer, un filtre peut être utilisé dans la capture de paquets pour examiner la connexion TLS :


PCAP_SSE_Registration.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==139.177

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-04 14:46:25.058289	139.177.	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.	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.	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 W
4	2023-09-04 14:47:21.487920	192.168.100.4	139.177.	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.	TLSv1.2	292	Client Hello
6	2023-09-04 14:47:21.520005	139.177.	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.	192.168.100.4	TLSv1.2	1454	Server Hello
8	2023-09-04 14:47:21.521539	139.177.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20	2023-09-04 14:47:21.568331	139.177.	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.	TLSv1.2	903	Application Data
22	2023-09-04 14:47:21.627413	139.177.	192.168.100.4	TLSv1.2	693	Application Data
23	2023-09-04 14:47:21.656792	192.168.100.4	139.177.	TCP	66	5074 → 8934 [ACK] Seq=1157 Ack=8295 Win=34032 Len=0 TSval=4294948981 TSecr=1462483959

PCAP SSE

La capture de paquets peut aider à voir si la connexion TLS a échoué.

Assistance TAC par téléphone Cisco Webex

Si vous avez besoin d'aide pour analyser les journaux et trouver la cause première du problème, contactez l'équipe Cisco Webex Calling TAC.

Informations relatives au support

Informations de référence de port pour les appels Webex

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.