Fehlerbehebung beim MPP-Telefon in WxC für Bereitstellung und Registrierung

Inhalt

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei MPP-Telefonen in WxC für Bereitstellungs- und Registrierungsprobleme, wenn das Gerät über die MAC-Adresse hinzugefügt wird.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Netzwerkwissen
- MPP-Telefon

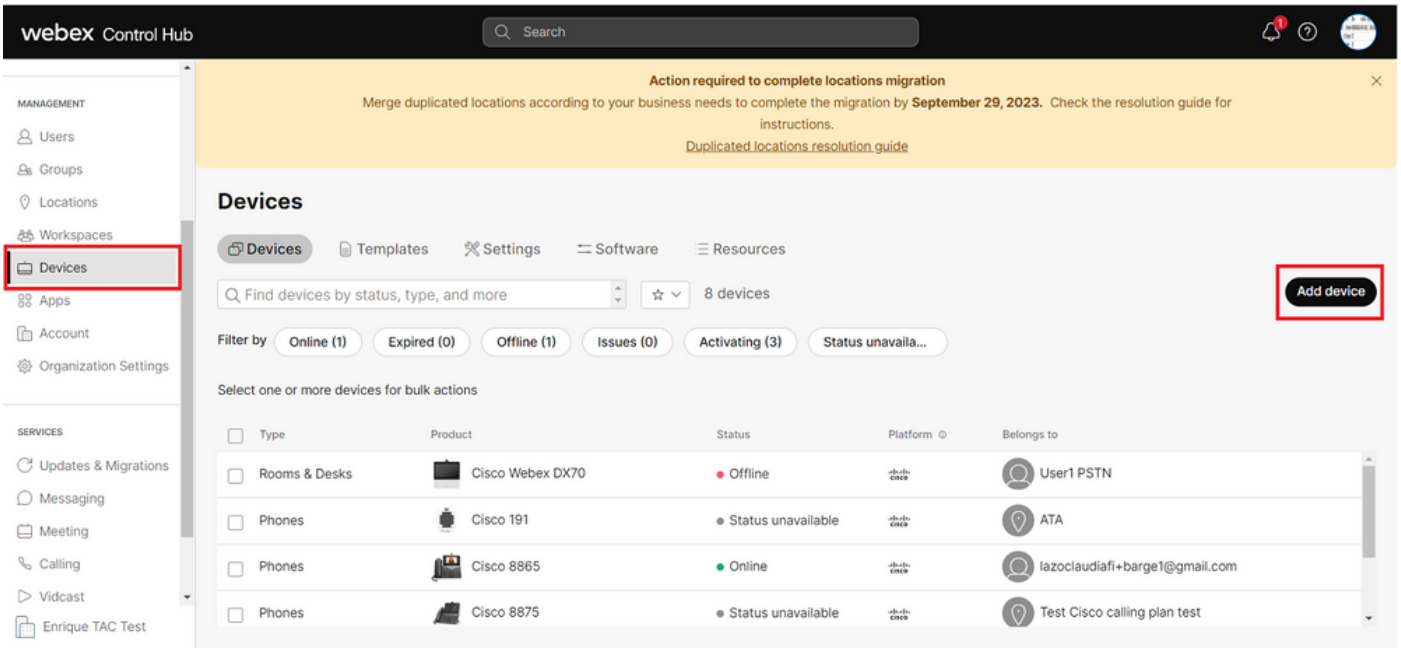
Verwendete Komponenten

Die Informationen in diesem Dokument basieren nur auf MPP-Telefonen wie 78XX, 88XX.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

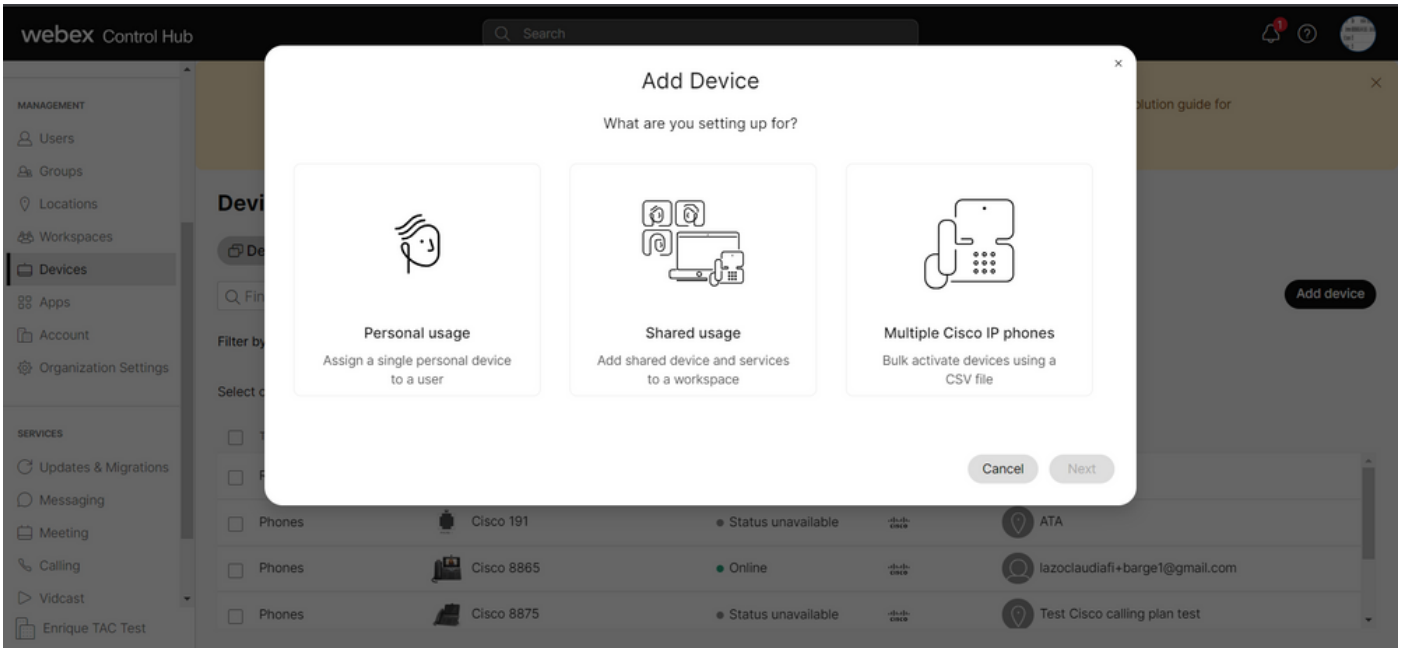
Gerät im Control Hub hinzufügen

Schritt 1: Navigieren Sie zu admin.webex.com, und verwenden Sie die Administrator-Anmeldeinformationen. Navigieren Sie in der Organisation zu Geräte > Gerät hinzufügen:



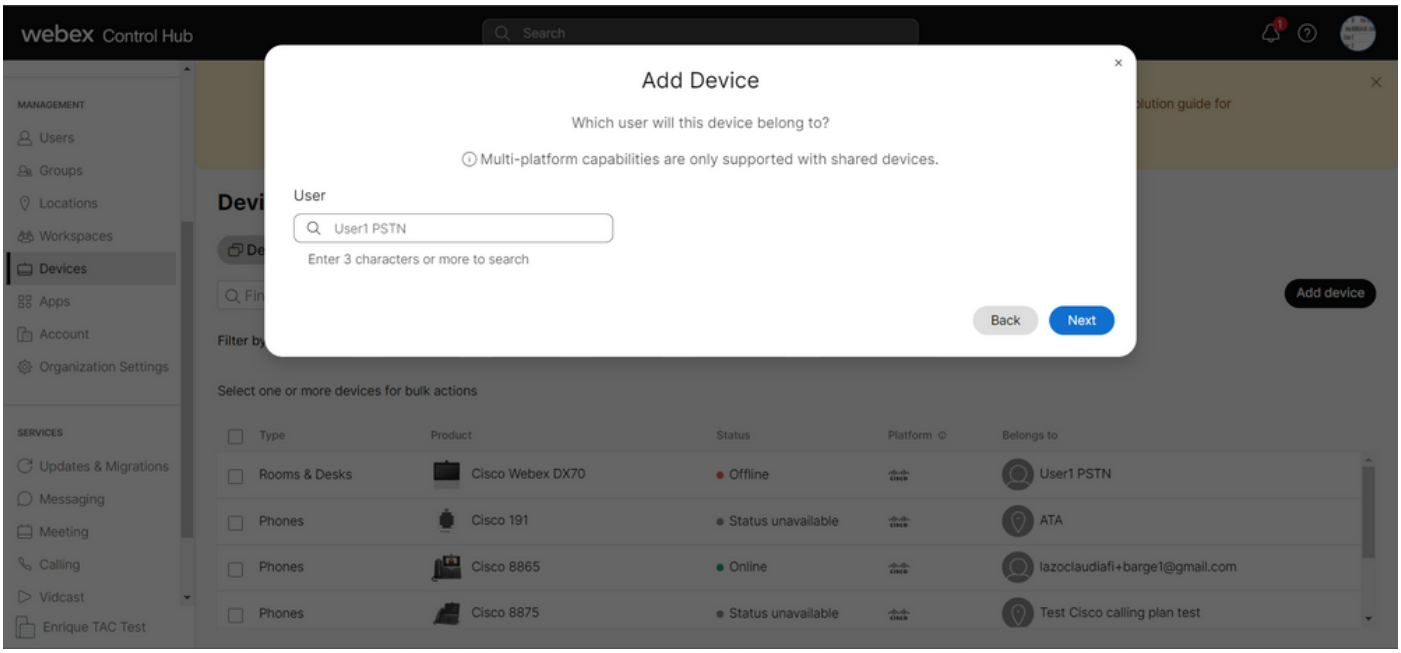
Registerkarte Geräte

Schritt 2: Wählen Sie Persönliche Nutzung, die einem Benutzer zugewiesen werden soll, oder Freigegebene Nutzung, die einem Arbeitsbereich zugewiesen werden soll. (In diesem Szenario wird ein Benutzer verwendet.)



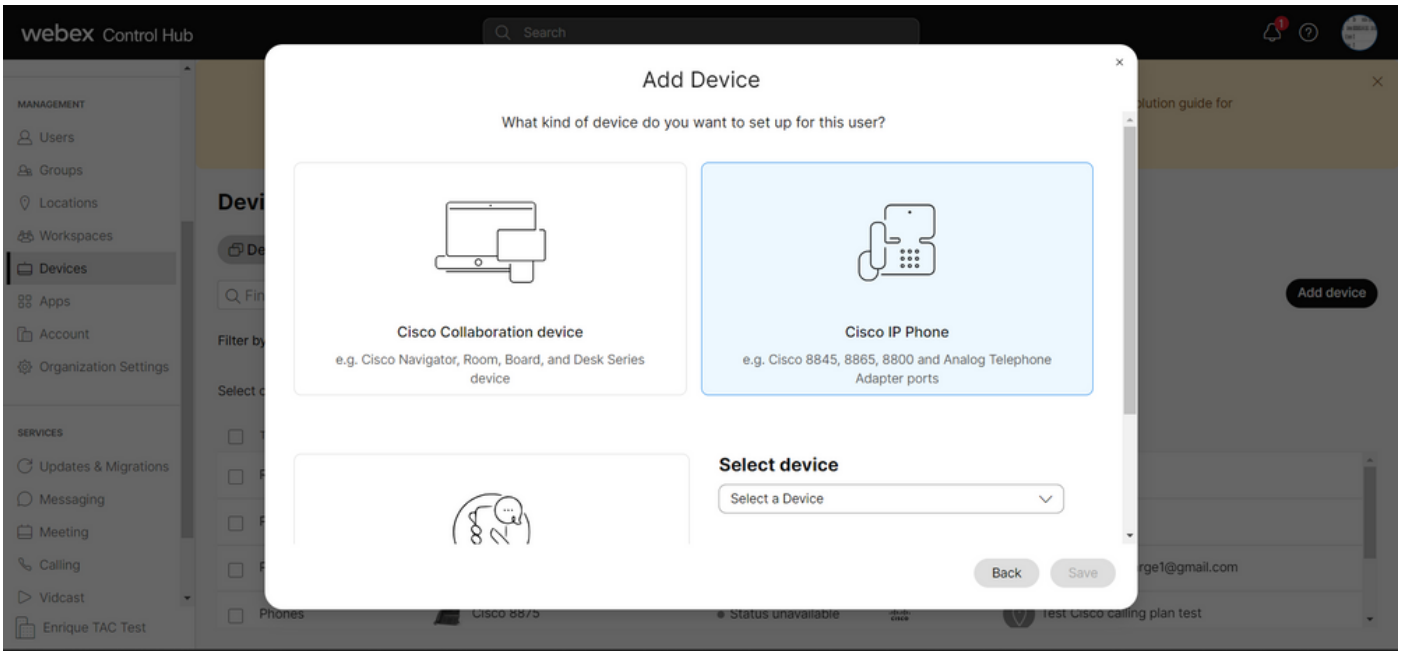
Gerät hinzufügen

Schritt 3: Suchen Sie den Benutzer, den Sie diesem Gerät zuweisen möchten, und klicken Sie auf Weiter:



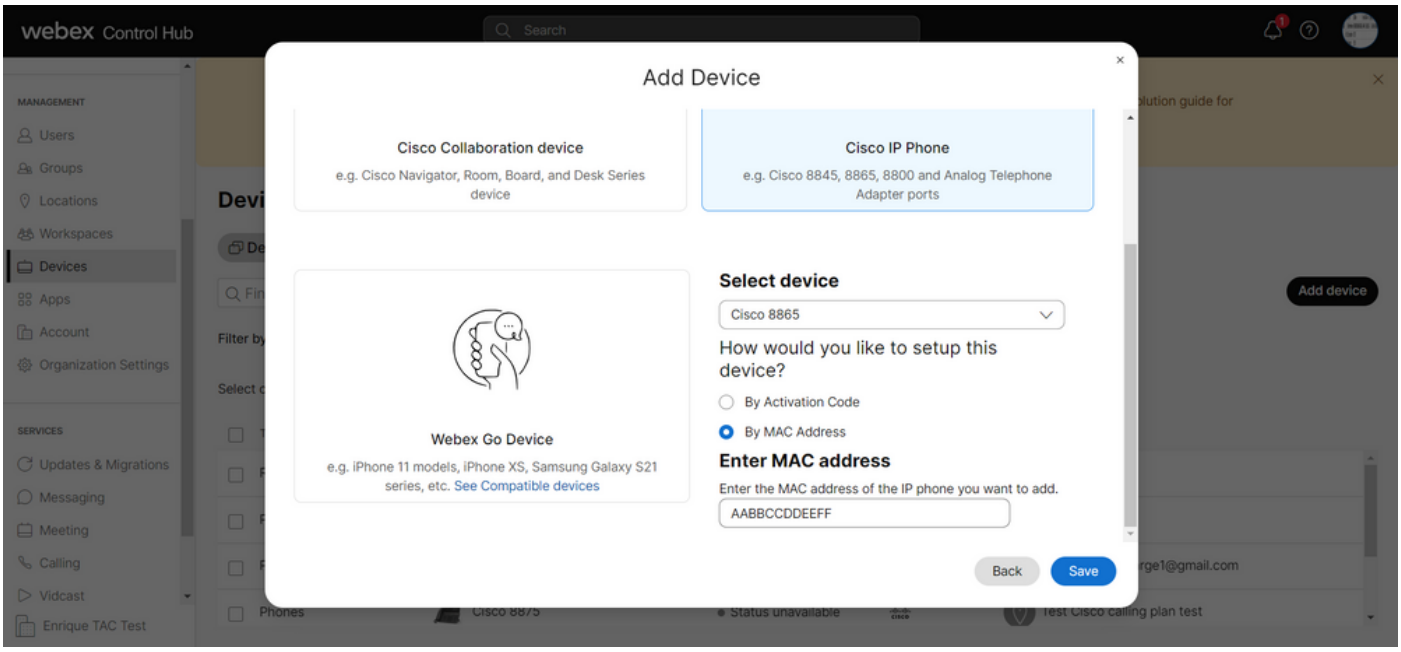
Nach einem Benutzer suchen

Schritt 4: Wählen Sie Cisco IP-Telefon aus, und suchen Sie nach dem gewünschten Gerätemodell:



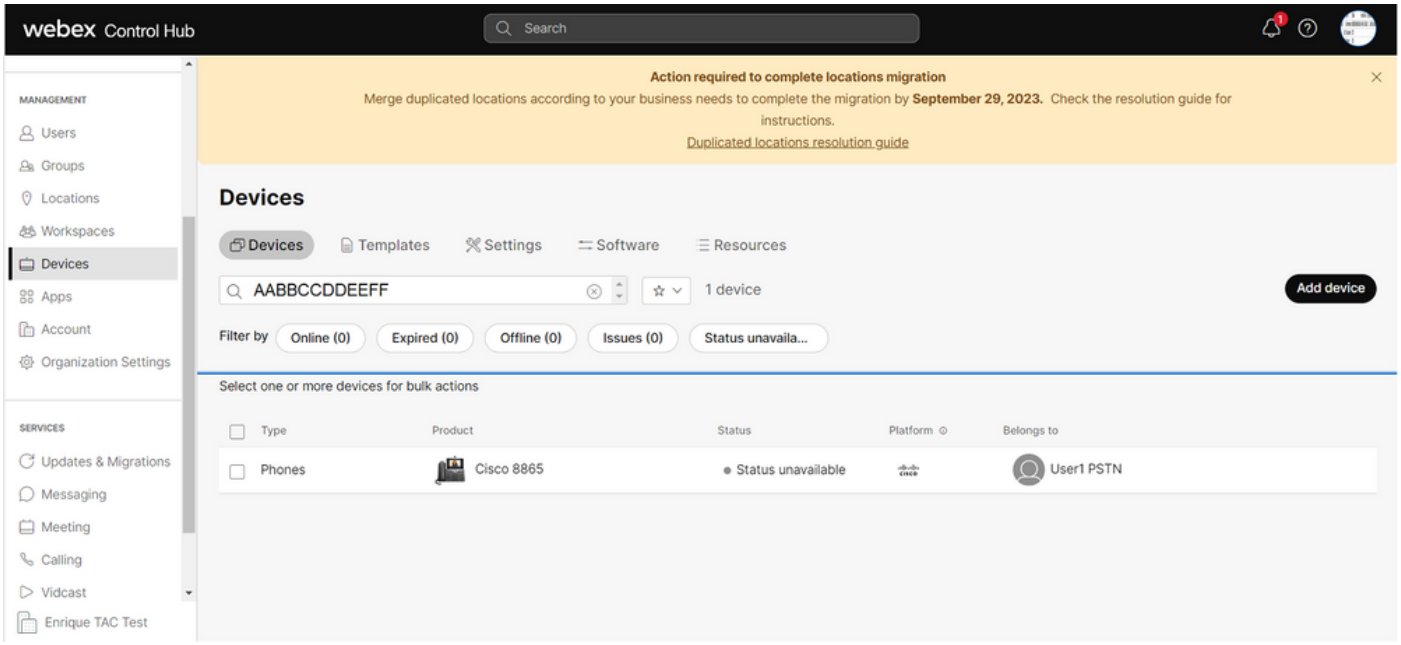
Gerätemodell auswählen

Schritt 5: Wählen Sie nach Auswahl des Geräts die Option Nach MAC-Adresse aus, geben Sie die MAC-Adresse des Geräts ein, und klicken Sie auf Speichern:



MAC-Adresse hinzufügen

Schritt 6: Sobald sich das Gerät im Control Hub befindet, können Sie überprüfen, ob es korrekt hinzugefügt wurde, wenn Sie die MAC-Adresse in der Suchleiste durchsuchen:

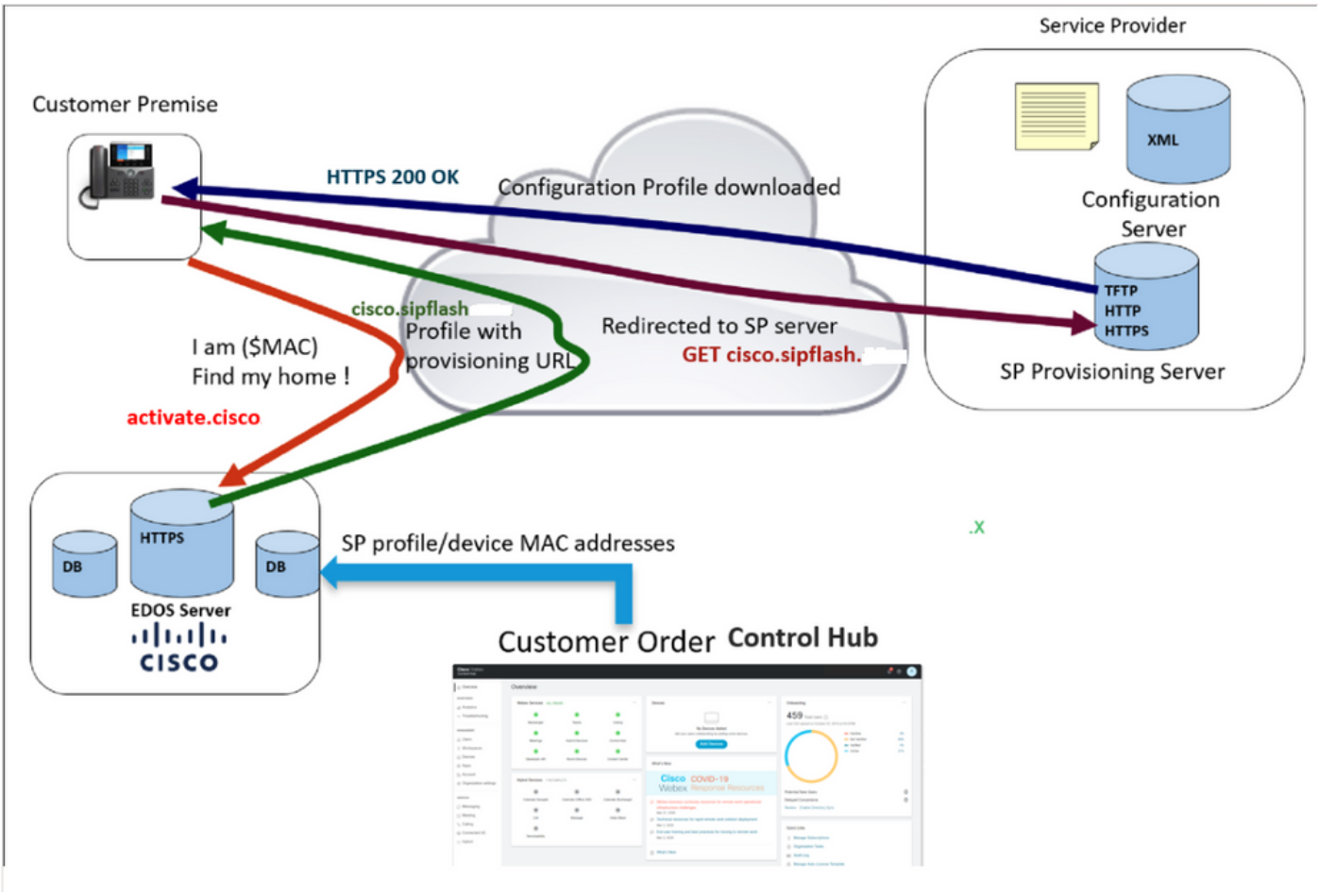


Überprüfung des Geräts

Der Status wird als "Nicht verfügbar" angezeigt, da das Gerät noch immer nicht bereitgestellt ist. Sobald sich das Gerät im Control Hub befindet, wird es im nächsten Schritt auf die Werkseinstellungen zurückgesetzt. Nach dem Zurücksetzen auf die Werkseinstellungen muss das Gerät eine Anforderung an die WxC-Server senden, um Konfigurationsdateien abzurufen. (Das ist der Bereitstellungsprozess.) Das Gerät wird erfolgreich bereitgestellt, wenn die Telefonnummer und/oder die Durchwahl auf dem Bildschirm angezeigt wird.

Wenn Sie feststellen, dass auf dem Gerät nicht die richtige Konfiguration angezeigt wird, ist der Bereitstellungsprozess für das Gerät fehlgeschlagen.

Kurze Zusammenfassung des Prozesses zur Bereitstellung eines Geräts in WxC



Bereitstellungsdiagramm

Fehlerbehebung beim Bereitstellen eines Geräts in WxC

Das MPP-Gerät kann WxC nicht bereitstellen, wenn es wie folgt konfiguriert ist:

- Ein im DHCP-Server konfigurierter TFTP-Server
- Wenn Option (OPT66, OPT160, OPT159 oder OPT150) vom DHCP-Server konfiguriert und bereitgestellt wird

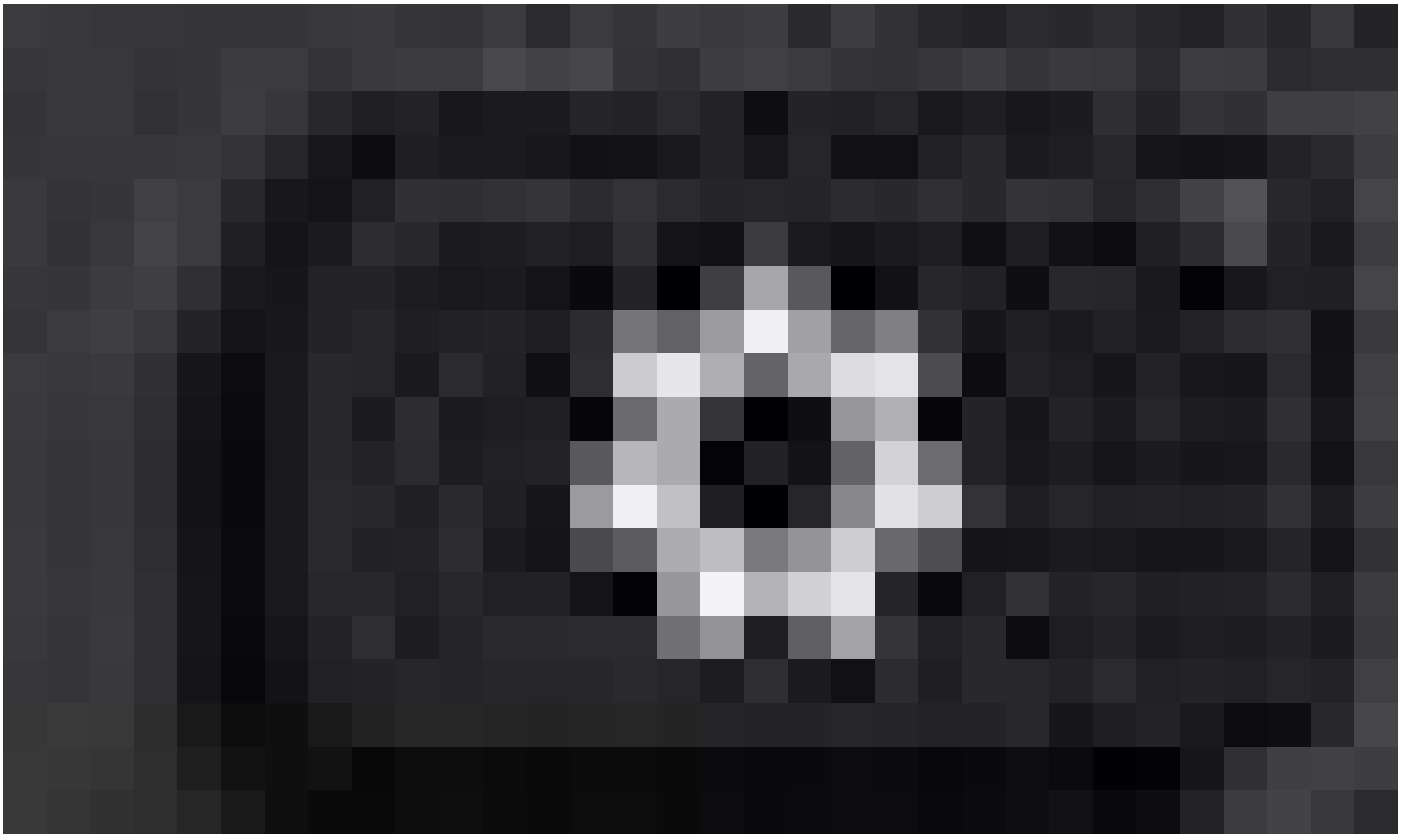
Um festzustellen, ob das Telefon eine TFTP-Konfiguration von einem DHCP-Server übernommen hat, sind die PRT-Protokolle erforderlich.

PRT-Protokolle von einem MPP-Gerät generieren

Senden Sie die PRT-Protokolle vom Telefon. Die nächsten Schritte zeigen, wie die PRT-Protokolle generiert werden.

PRT vom Gerät generieren

Schritt 1.Drücken Sie auf dem Gerät die Anwendungstaste



Einstellungen

.

Schritt 2:Gehe zu Status > Problem melden.

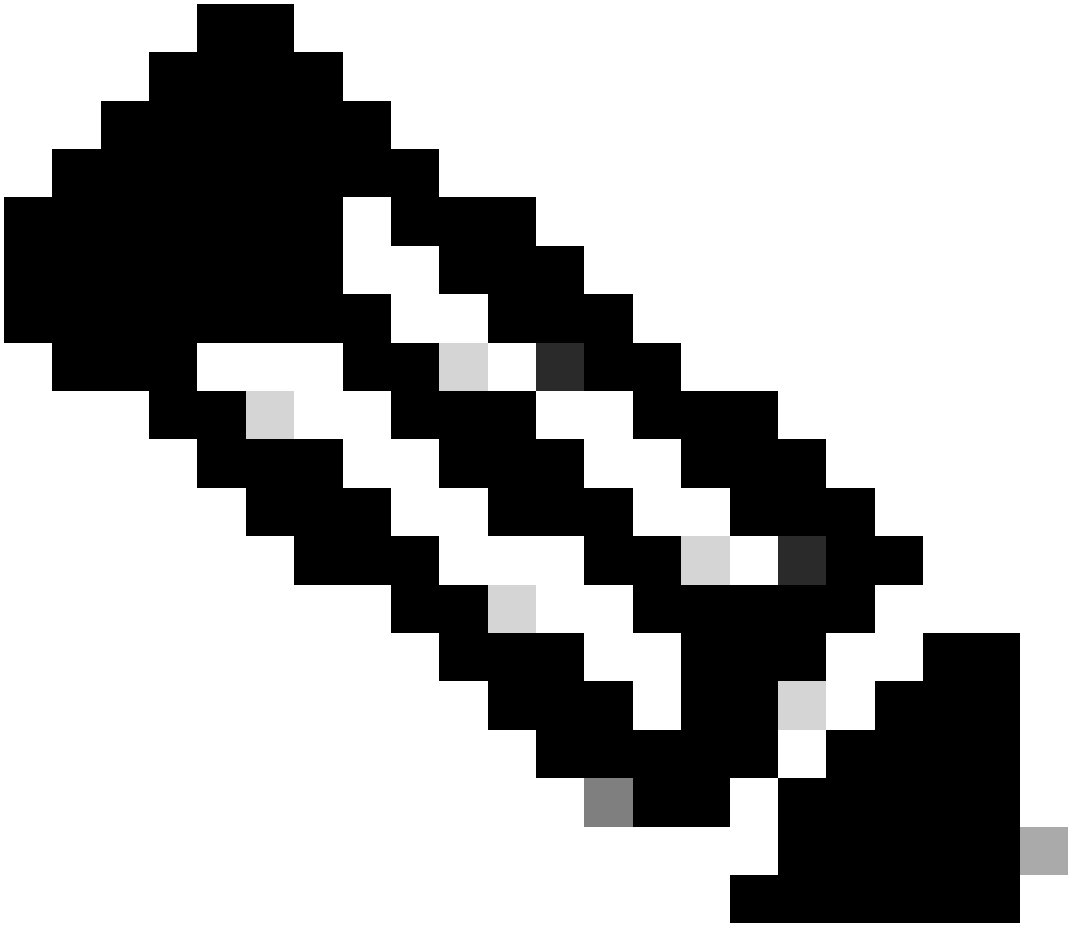
Schritt 3: Geben Sie Datum und Uhrzeit des Problems ein.

Schritt 4.Wählen Sie eine Beschreibung aus der Liste aus.

Schritt 5.Drücken Sie Senden.

Wenn die Protokolle eingesendet wurden, sehen Sie sich die folgenden Schritte zum Herunterladen der PRT-Protokolle an:

Schritt 1: Melden Sie sich an unter https://IP_ADDRESS_PHONE/



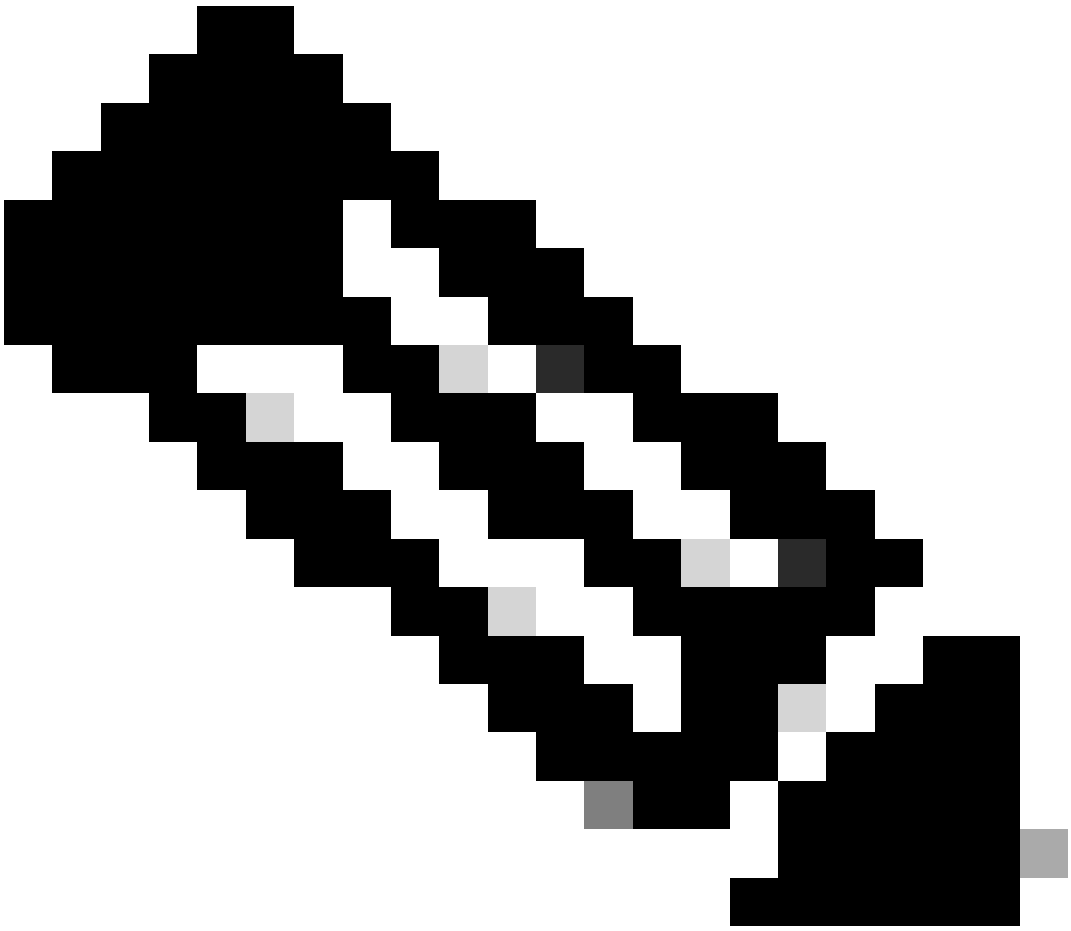
Hinweis: Hinweis: Wenn die IP-Adresse unbekannt ist, finden Sie sie unter Einstellungen > Status > Network Status > IPv4 Status.

Schritt 2: Navigieren Sie zu Info > Debug Info > Laden Sie das PRT-Protokoll herunter (klicken Sie mit der rechten Maustaste auf den Link, und wählen Sie Save As...)

Weboberfläche

PRT-Protokolle

Wenn Sie die Protokolle öffnen, sehen Sie eine Ansicht wie diese:



Hinweis: Sie können die Protokolle mit einem Programm wie WinRAR öffnen, da die Protokolle komprimiert sind.

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...	

Um den Bereitstellungsprozess für das Gerät zu analysieren, muss das Protokoll " logcat" geöffnet werden. Es kann mit einem Texteditor wie Notepad oder Notepad++ geöffnet werden.
Mit der Funktion "Suchen" im Texteditor kann ermittelt werden, ob auf dem Telefon ein TFTP-Server konfiguriert ist. Verwenden Sie DHCP-tftpsvr1 oder DHCP-tftpsvr2, um die spezifische Zeile für dieses Protokoll zu finden. Wenn Sie einen Blick und die anderen Zeilen der Protokolle werfen, finden Sie weitere Informationen zur DHCP-Konfiguration:

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:

Wie Sie im Protokoll sehen können, wird im DHCP-Server eine TFTP-IP-Adresse konfiguriert. Aus diesem Grund hat das Telefon versucht, eine Bereitstellung auf diesem TFTP-Server anstelle der WebEx Calling Server vorzunehmen.

```
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
```

Nachdem Sie eine TFTP- und eine OPT-Konfiguration vom DHCP-Server entfernt haben, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen, um den Bereitstellungsprozess für das Gerät mit WxC erneut zu starten.
Der erste Versuch, den das Telefon mit dem Bereitstellungsprozess für das Gerät unternimmt, besteht darin, eine Anforderung an die URL activate.cisco.com zu senden. Das Telefon fragt den DNS-Server ab, um die Domäne aufzulösen. Wenn die DNS-Auflösung fehlschlägt, kann sie wie folgt aussehen:

<#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
```

Wenn das Telefon die Domäne auflösen kann, kann es wie folgt aussehen:

```
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
```

Nachdem das Telefon die 200 OK von der GET-Anfrage an activate.cisco.com erhalten hat, sendet es eine Anfrage an cisco.siplash.com. Es ist der gleiche Prozess, das Telefon versucht, die Domain aufzulösen und wenn es scheitert, kann es so aussehen:

```
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"
```

Wenn das Telefon die Domäne auflösen kann, kann es wie folgt aussehen:

```
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
```

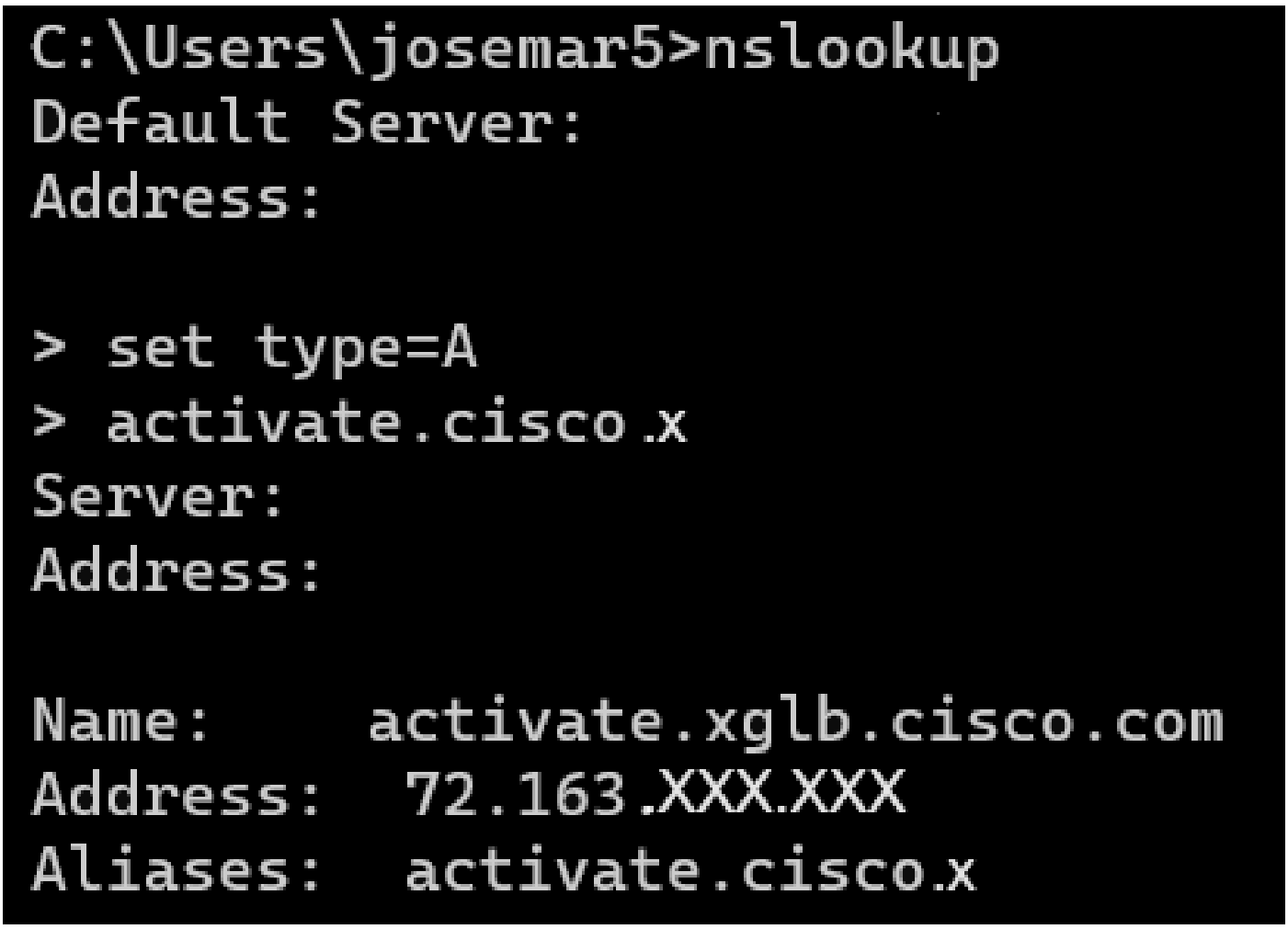
```
Accept-Language: en^M
Accept-Charset: iso-8859-1^M
^M
1996 NOT Sep 04 22:49:29.506969 <
1997 NOT Sep 04 22:49:29.507037 HTTP/1.1 200 OK^M
```

Fehlerbehebung-DNS (Bereitstellung von URLs)

Wenn Sie sich in demselben Netzwerk befinden, in dem die Geräte Probleme mit der DNS-Auflösung haben, kann ein nslookup verwendet werden, um zu überprüfen, ob der DNS-Server in der Lage ist, die Domäne aufzulösen. Öffnen Sie die Befehlszeilenschnittstelle, und führen Sie die folgenden Schritte aus:

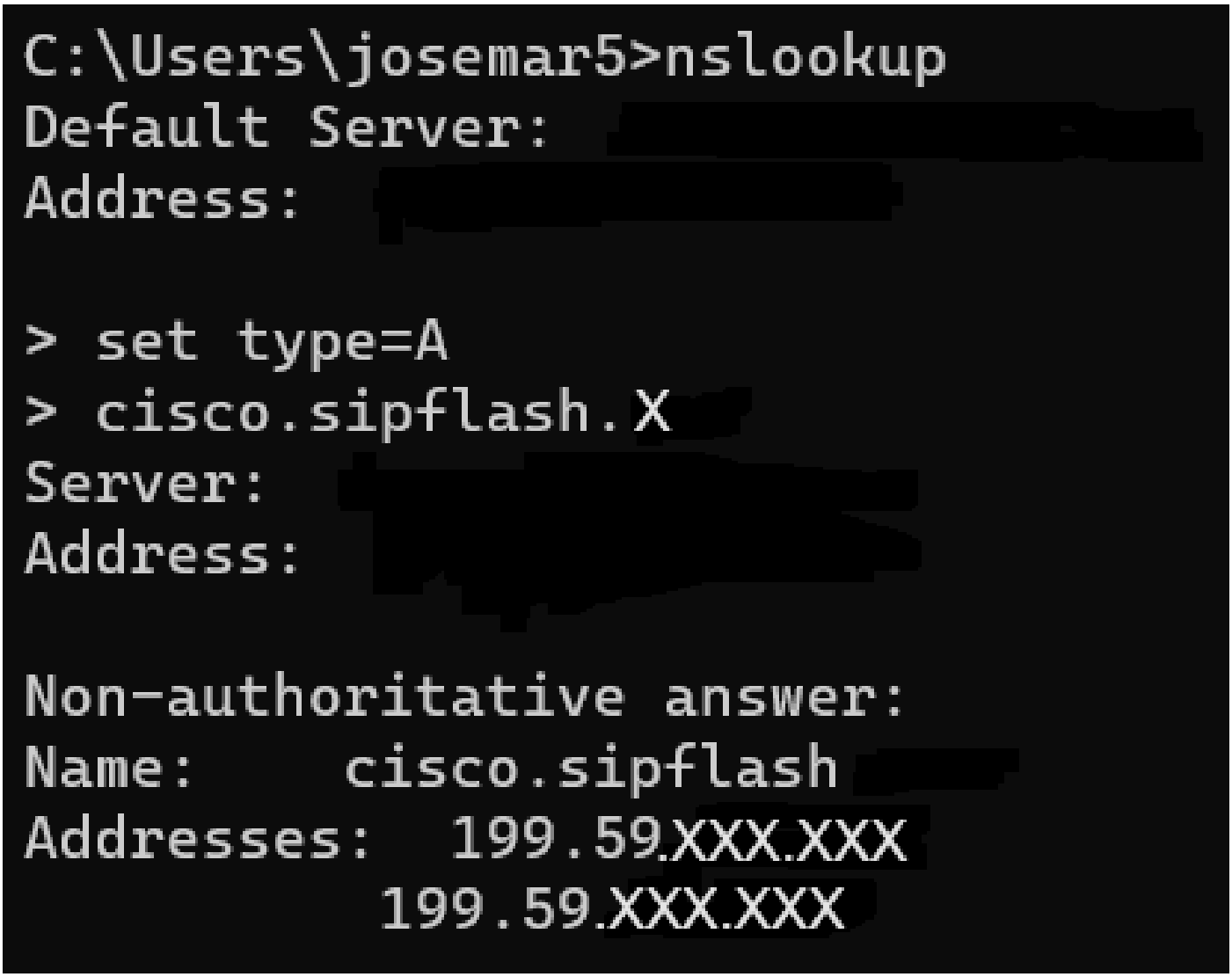
- nslookup -> Eingabe
- set type=A -> Eingabe
- activate.cisco.com

Wenn der PC die Domäne auflösen kann, sieht er wie folgt aus:



nslookup activate.cisco

Derselbe Prozess kann für cisco.sipflash.x durchgeführt werden, um die Domäne aufzulösen:



nslookup cisco sipflash

Wenn der PC die Domänen nicht auflösen kann, überprüfen Sie Ihren DNS-Server.

Fehlerbehebung bei der Registrierung für ein MPP-Gerät in WxC

In diesem Beispiel lautet der ausgehende Proxy da02.hosted-us10.bcld.webex.com. Das Telefon versucht, die SRV-Domäne aufzulösen:

```
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
```

Wenn das Telefon die SRV-Domäne auflösen kann, werden die Hostnamen abgerufen:

```
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
```

Von einem dieser Hostnamen führt das Telefon einen von ihnen, um sich für den WxC-SBC zu registrieren:

```
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
```

Das Gerät muss eine 401 Unauthorized-Meldung von der WxC-Seite erhalten:

```
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
```

Das Gerät sendet REGISTER mit dem Autorisierungs-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
```

Und dann bekommt das Gerät einen 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
```

Anschließend muss das Gerät bei den WxC-Services registriert und aktiviert werden.

Fehlerbehebung bei DNS (URLs registrieren)

Wenn Sie sich in demselben Netzwerk befinden, in dem die Geräte Probleme mit der DNS-

Auflösung haben, kann nslookup verwendet werden, um zu überprüfen, ob der DNS-Server in der Lage ist, die Domäne aufzulösen. Öffnen Sie die Befehlszeilenschnittstelle, und führen Sie die folgenden Schritte aus:

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

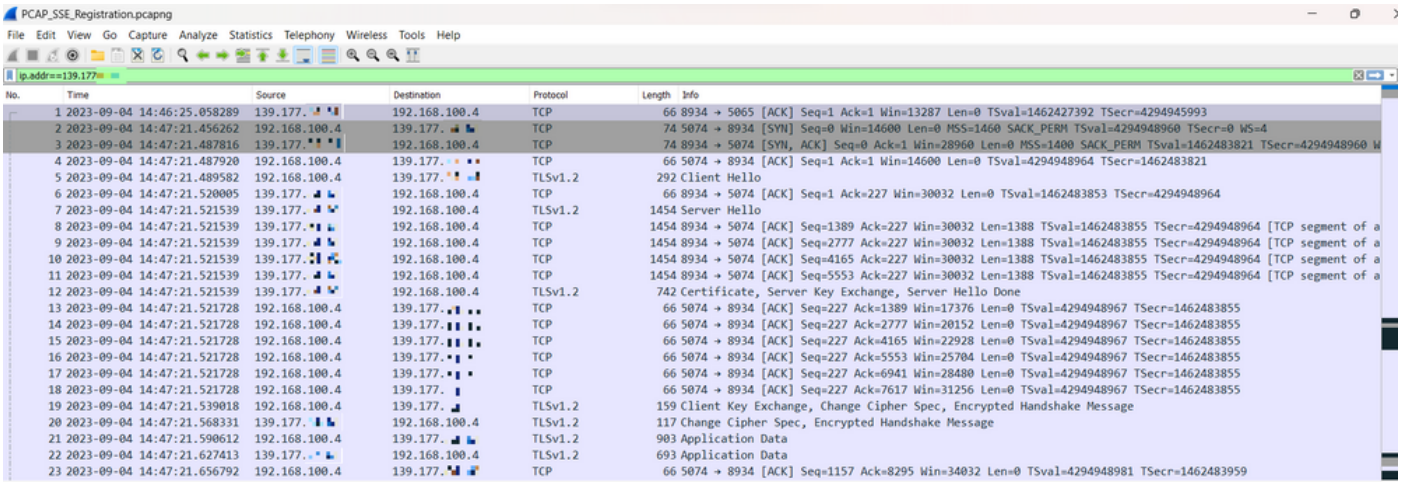
Wenn der PC in der Lage ist, die Domäne aufzulösen, kann dies folgendermaßen aussehen:

```
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

Paketerfassung (Registrierungsprozess)

Sie können die IP-Adresse des Telefons für die Registrierung verwenden. Ein Filter kann bei der Paketerfassung verwendet werden, um den TLS-Handshake zu untersuchen:



PCAP-SSE

Die Paketerfassung kann dabei helfen, festzustellen, ob der TLS-Handshake fehlgeschlagen ist.

Cisco WebEx TAC-Support

Wenn Sie Unterstützung benötigen, um die Protokolle zu analysieren und die Ursache des Problems zu finden, wenden Sie sich an das Cisco Webex Calling TAC-Team.

Support-bezogene Informationen

[Port-Referenzinformationen für WebEx Anrufe]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.