프로비저닝 및 등록을 위해 WxC에서 MPP Phone 문제 해결

목차

소개

이 문서에서는 MAC 주소로 디바이스를 추가할 때 프로비저닝 및 등록 문제에 대해 WxC에서 MPP 전화기의 문제를 해결하는 방법을 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 네트워크 지식
- MPP 전화

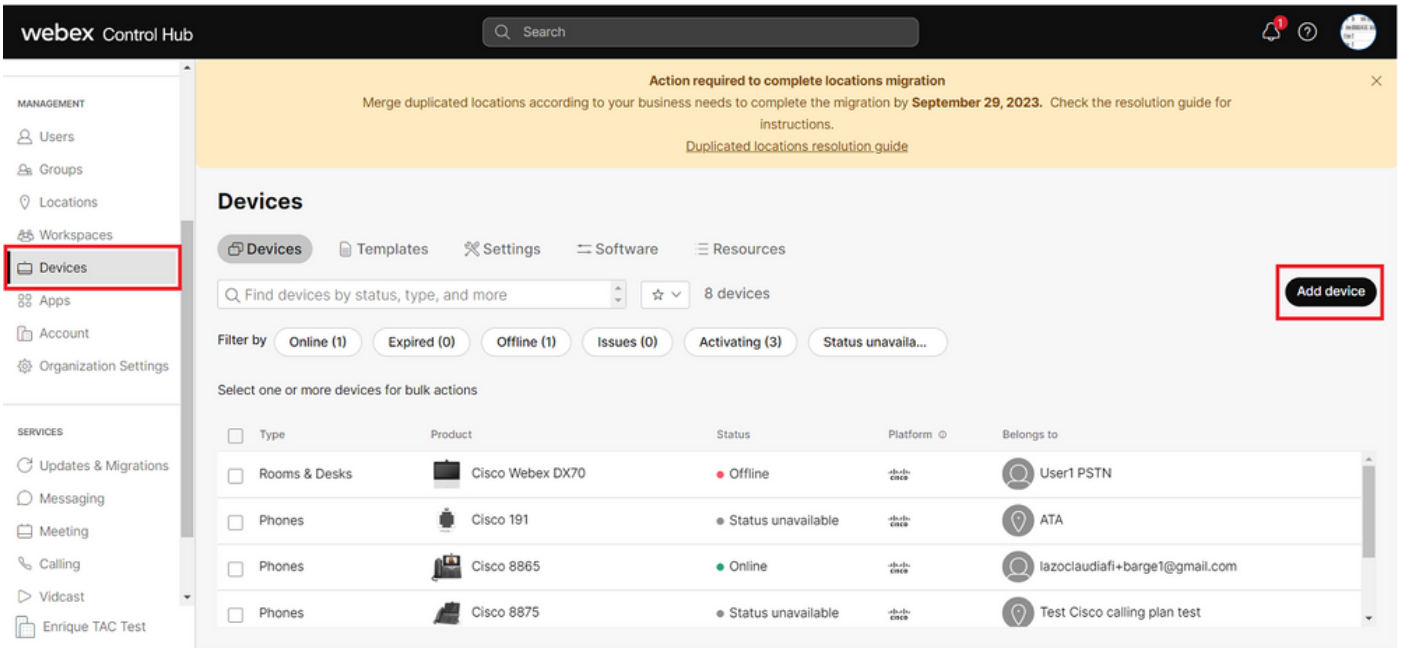
사용되는 구성 요소

이 문서의 정보는 78XX, 88XX와 같은 MPP 전화기만 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

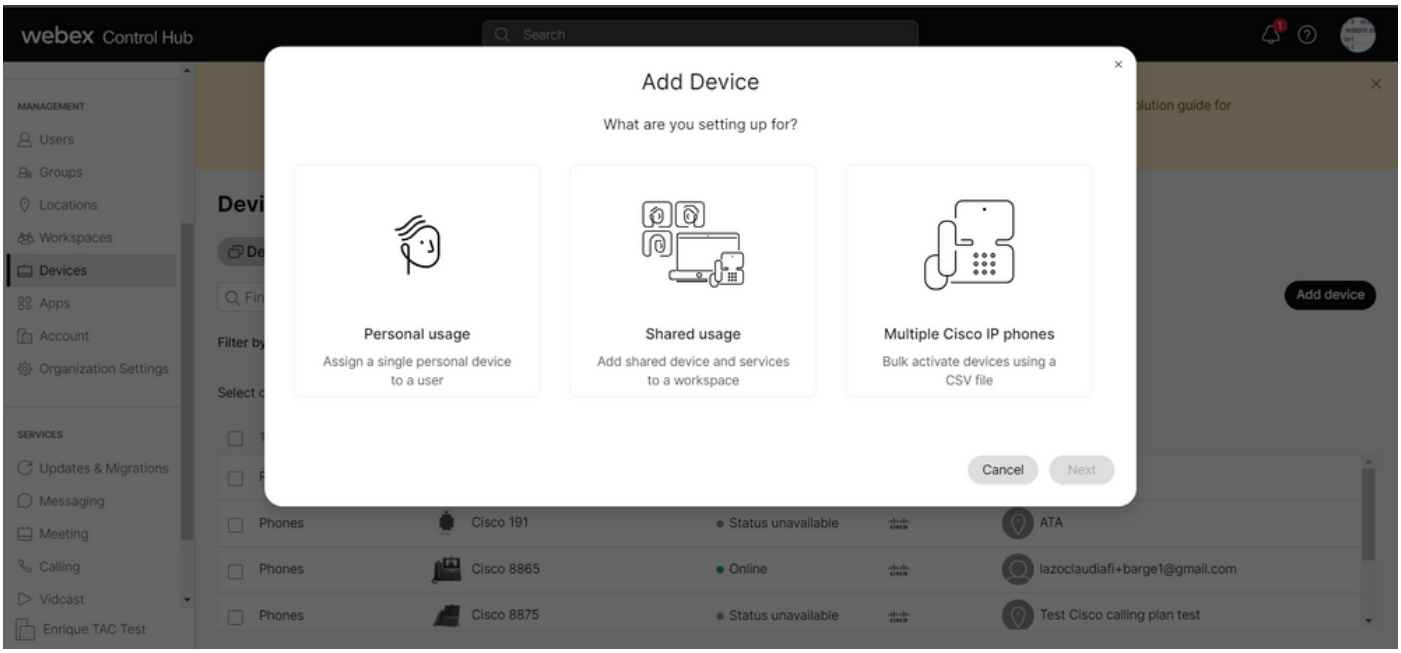
Control Hub에 디바이스 추가

1단계. admin.webex.com으로 이동하고 관리자 자격 증명을 사용합니다. 조직에서 Devices(디바이스) > Add device(디바이스 추가)로 이동합니다.



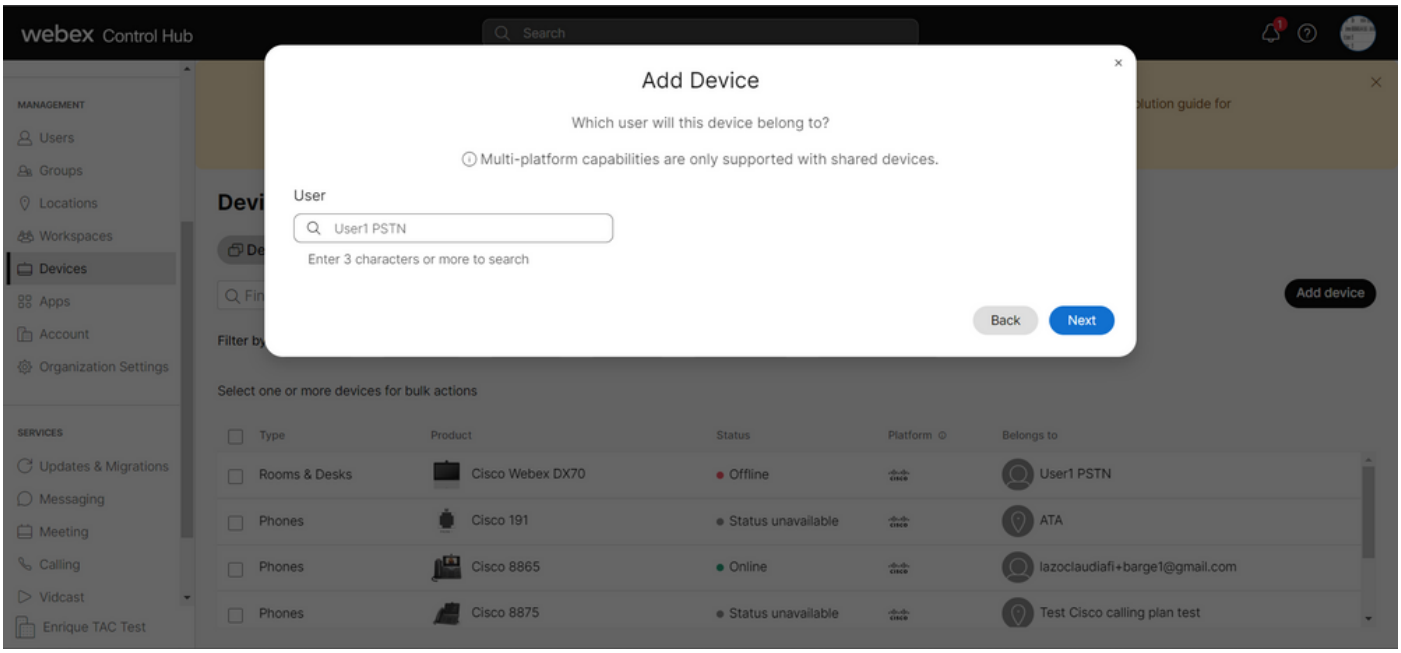
Devices 탭

2단계. 사용자에게 할당할 개인 사용을 선택하거나 작업 영역에 할당할 공유 사용을 선택합니다. 이 시나리오에서는 사용자가 사용됩니다.



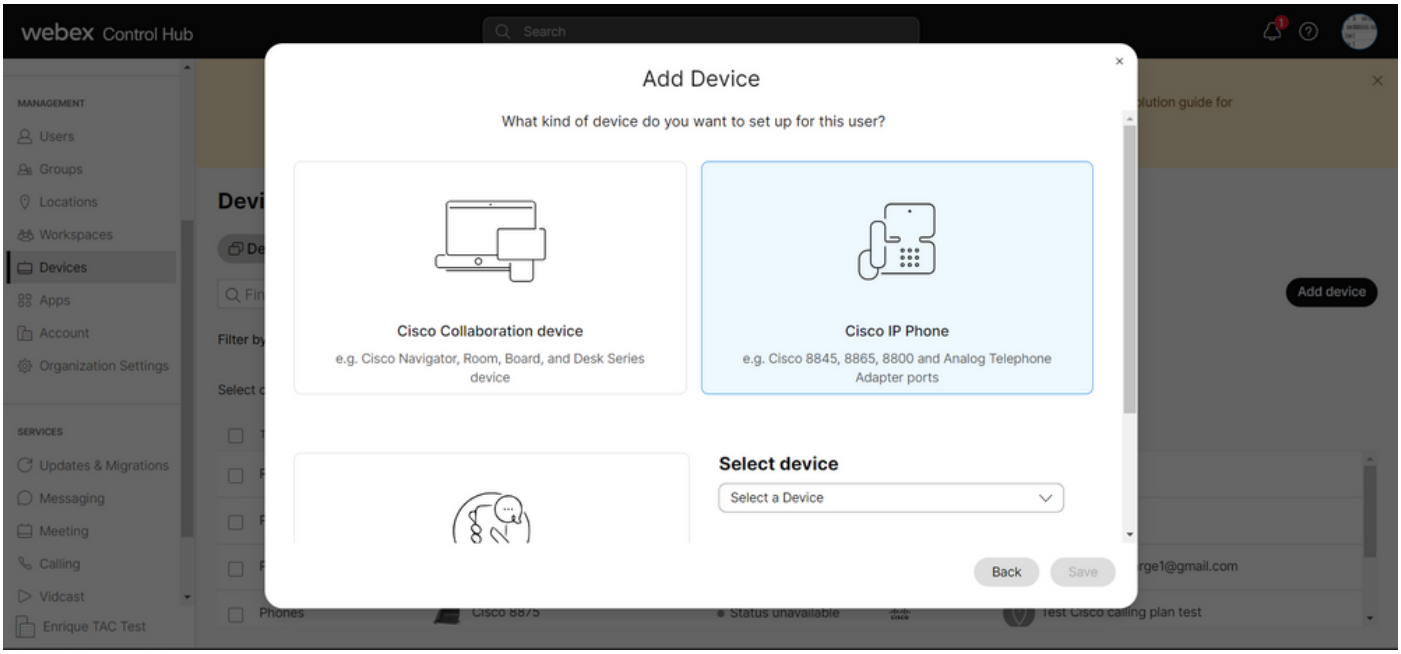
장치 추가

3단계. 이 장치에 할당 할 사용자를 검색 하고 선택 하고 다음을 클릭 합니다.



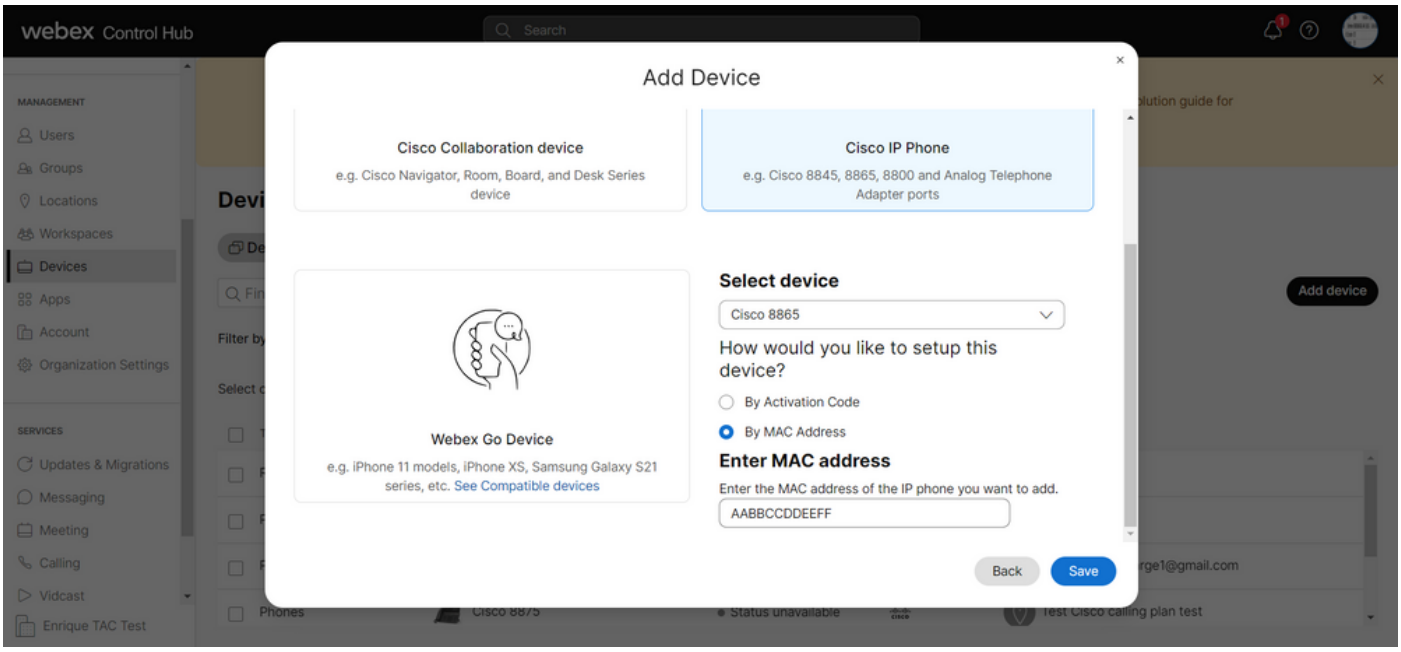
사용자 검색

4단계. Cisco IP Phone을 선택하고 디바이스 모델을 검색합니다.



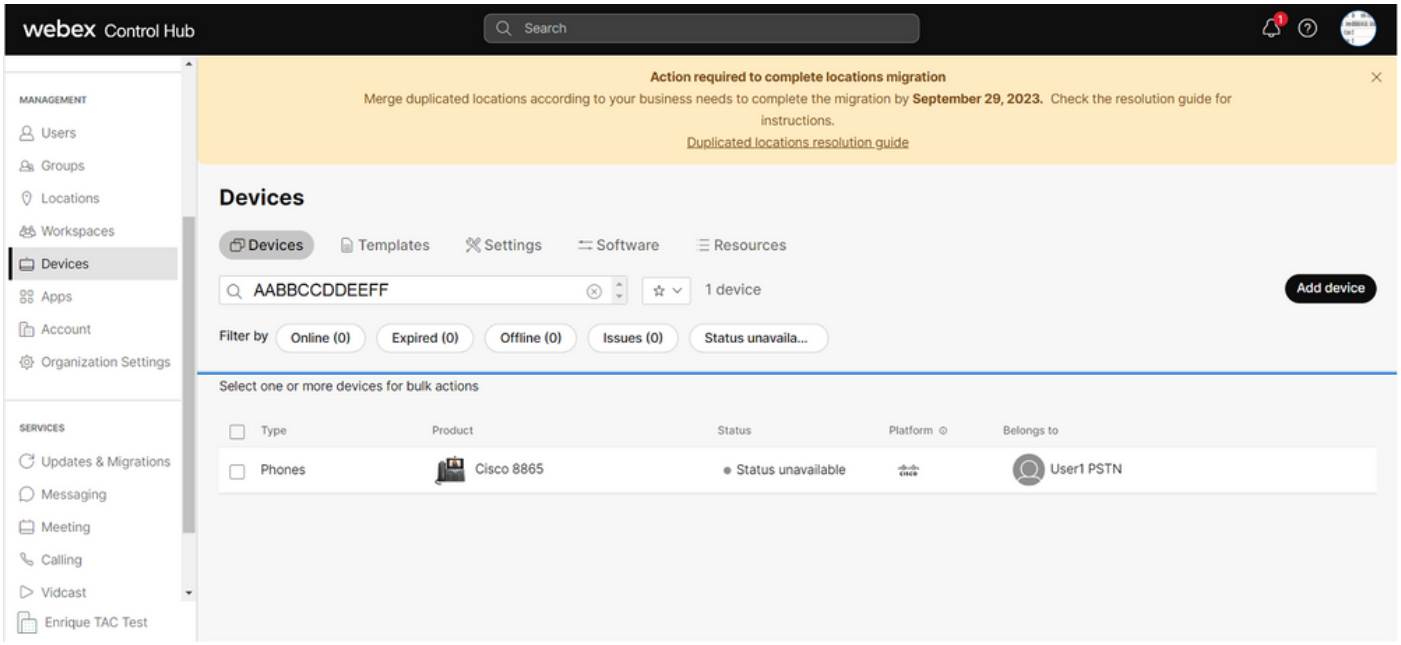
장치 모델 선택

5단계. 디바이스가 선택되면 By MAC Address(MAC 주소 기준) 옵션을 선택하고 디바이스의 MAC 주소를 입력한 후 Save(저장)를 클릭합니다.



MAC 주소 추가

6단계. 디바이스가 Control Hub에 있으면 검색 표시줄에서 MAC 주소를 검색할 때 올바르게 추가되었는지 확인할 수 있습니다.

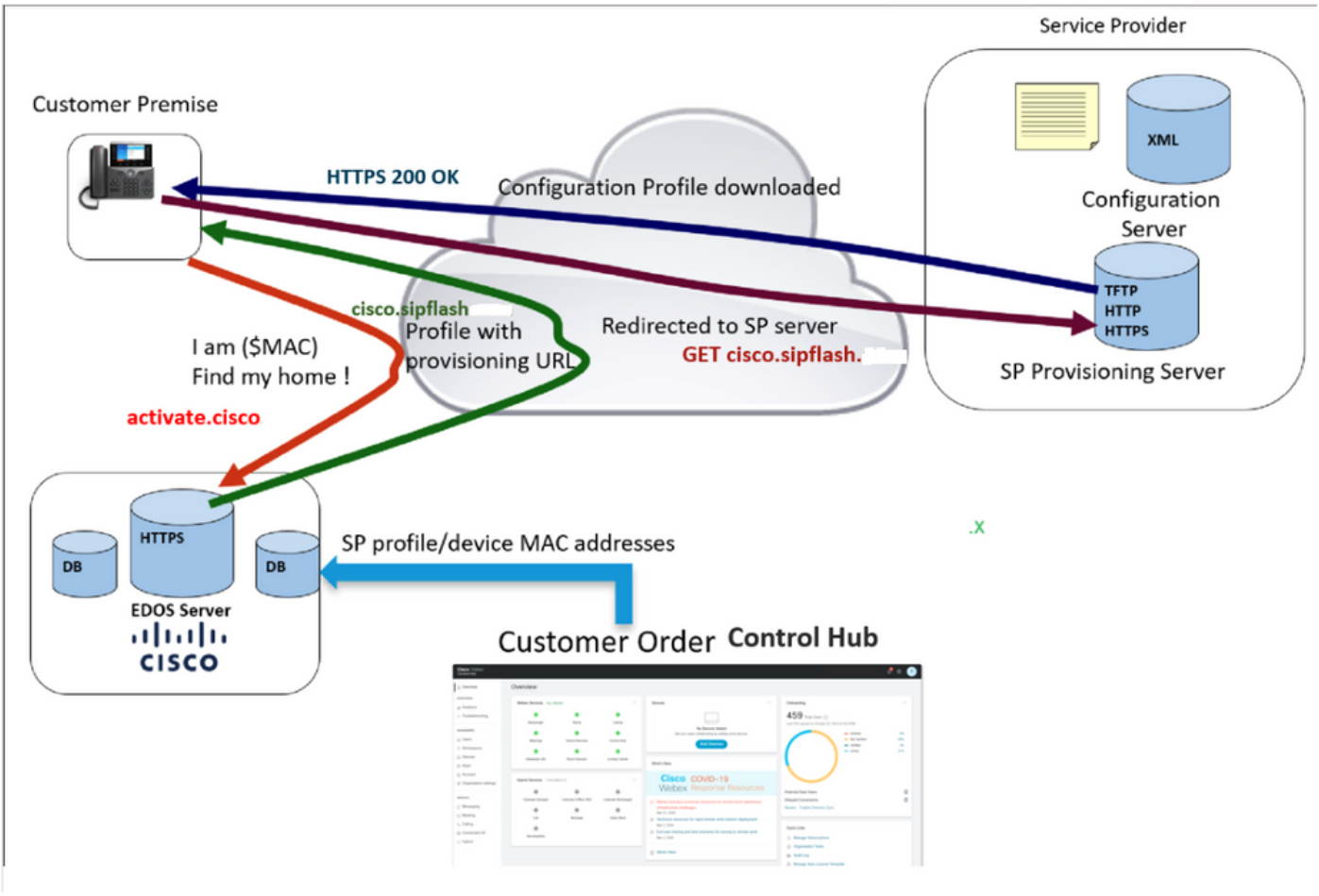


장치 확인

디바이스가 아직 프로비저닝되지 않았으므로 상태가 "Unavailable(사용할 수 없음)"으로 표시됩니다. 디바이스가 Control Hub에 있는 경우 다음 단계는 디바이스를 공장 출하 시 재설정하는 것입니다. 공장 초기화 후 디바이스에서 WxC 서버에 요청하여 컨피그레이션 파일을 가져와야 합니다. 제공 프로세스입니다. 디바이스가 화면에 전화 번호 및/또는 내선 번호를 표시하면 디바이스가 성공적으로 프로비저닝됩니다.

디바이스가 적절한 컨피그레이션을 표시하지 않는 경우 디바이스를 프로비저닝하는 프로세스가 실패했습니다.

WxC에서 디바이스를 프로비저닝하기 위한 프로세스의 간략한 요약



프로비저닝 다이어그램

WxC에서 장치 프로비저닝을 위한 프로세스 트러블슈팅

MPP 장치가 다음과 같이 구성된 경우 WxC로 프로비저닝할 수 없습니다.

- DHCP 서버에 구성된 TFTP 서버
- DHCP 서버에서 옵션(OPT66, OPT160, OPT159 또는 OPT150)을 구성하고 제공하는 경우

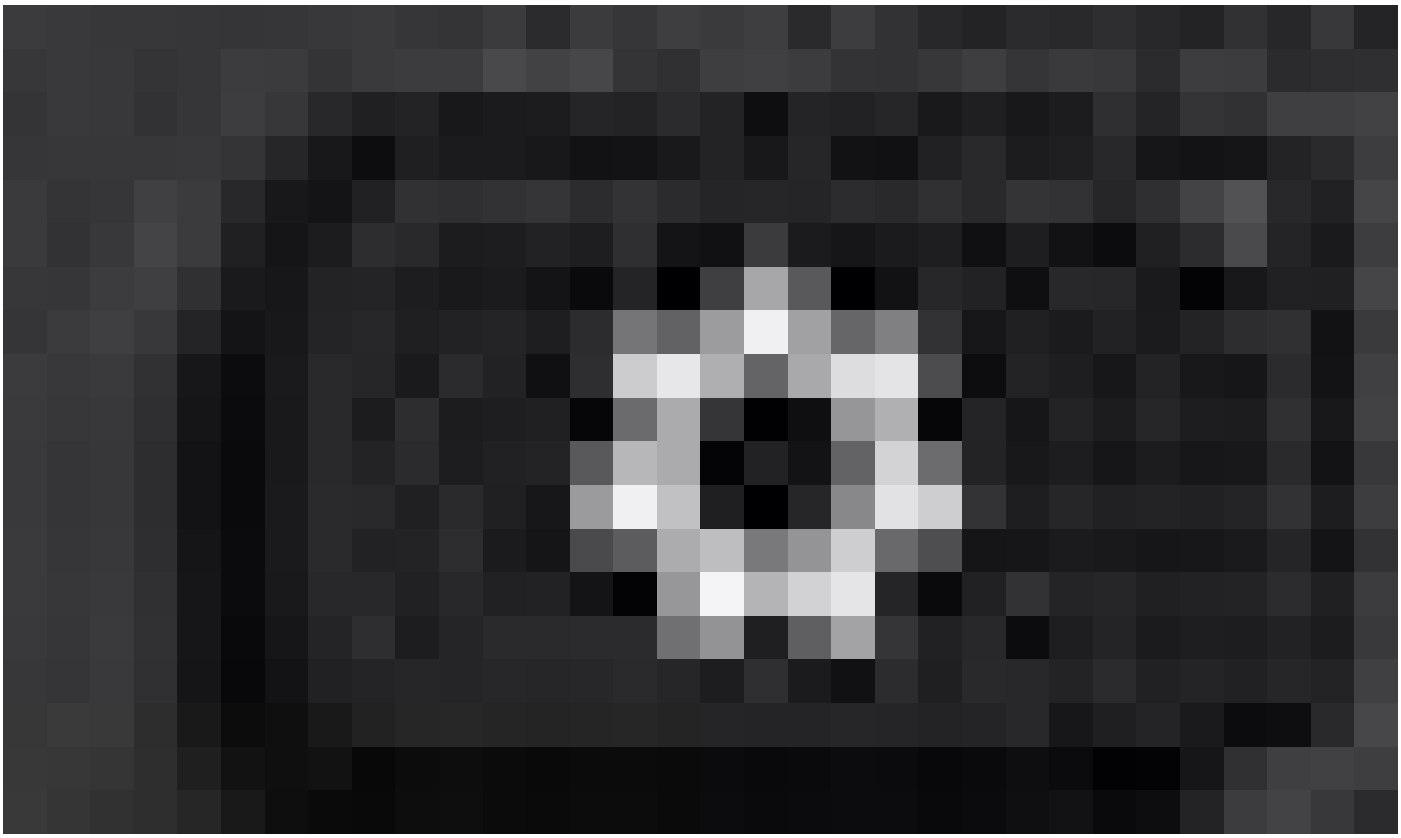
전화기가 DHCP 서버에서 TFTP 컨피그레이션을 가져왔는지 확인하려면 PRT 로그가 필요합니다.

MPP 디바이스에서 PRT 로그 생성

전화기의 PRT 로그에서 제출합니다. 다음 단계에서는 PRT 로그를 생성하는 방법을 보여줍니다.

디바이스에서 PRT 생성

1단계. 디바이스에서 Applications(애플리케이션)button Settings(버튼 설정) 버튼



을 누릅니다

.

2단계. Status(상태) > Report Problem(문제 보고)으로 이동합니다.

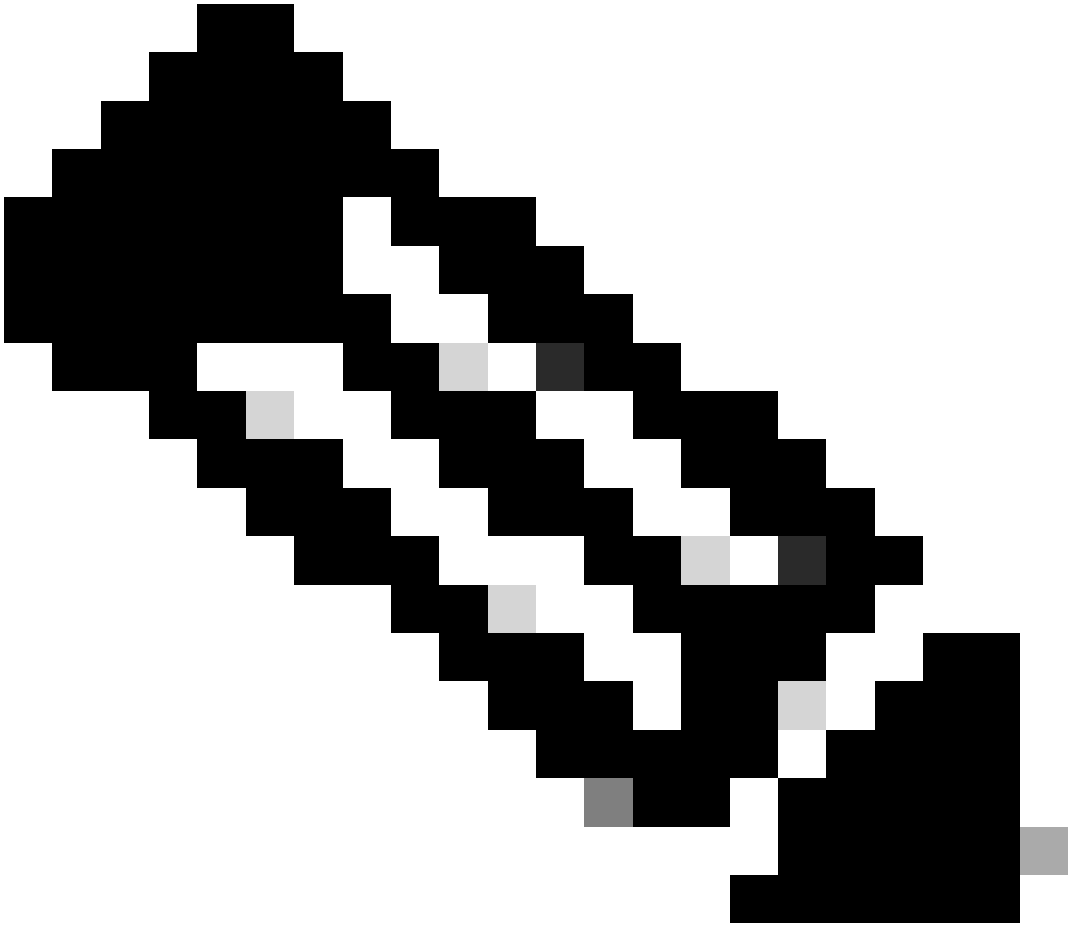
3단계.문제의 날짜와 시간을 입력합니다.

4단계. 목록에서 Description(설명)을 선택합니다.

5단계.Submit(제출)을 누릅니다.

로그가 제출되면 PRT 로그를 다운로드하는 다음 단계를 참조하십시오.

1단계. https://IP_ADDRESS_PHONE/에 로그인



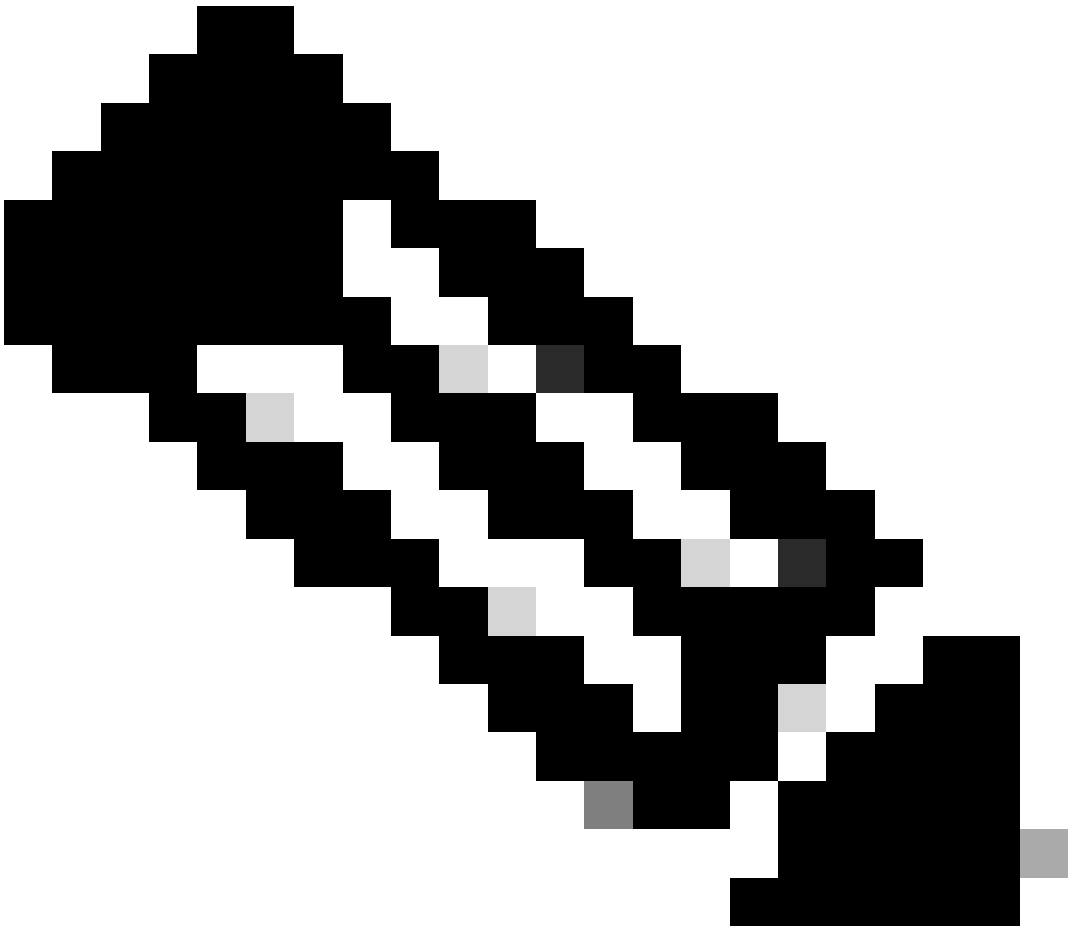
참고: 참고: IP 주소를 알 수 없는 경우 Settings(설정) > Status(상태) > Network Status(네트워크 상태) > IPv4 Status(IP4 상태)에서 확인할 수 있습니다.

2단계. Info(정보) > Debug Info(디버그 정보) > Download the PRT log(PRT 로그 다운로드)로 이동합니다(링크를 마우스 오른쪽 버튼으로 클릭하고 Save As...).

웹 GUI

PRT 로그

로그를 열면 다음과 같은 보기가 표시됩니다.



참고: 로그가 압축되기 때문에 WinRAR과 같은 프로그램으로 로그를 열 수 있습니다.

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 로그 보기

디바이스를 프로비저닝하기 위한 프로세스를 분석하기 위해 logcat이라는 로그를 열어야 합니다. Notepad 또는 Notepad ++와 같은 텍스트 편집기로 열 수 있습니다.
전화기에 TFTP 서버가 구성되어 있는지 확인하기 위해 텍스트 편집기의 "Find" 기능을 사용할 수 있습니다. DHCP -tftpsvr1 또는 DHCP-tftpsvr2를 사용하여 해당 로그의 특정 행을 찾습니다. 로그의 다른 행과 함께 살펴보는 경우 DHCP 컨피그레이션에 대한 자세한 내용을 확인할 수 있습니다.

```
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:
```

로그에서 볼 수 있듯이 TFTP IP 주소는 DHCP 서버에 구성됩니다. 따라서 전화기에서 Webex Calling 서버 대신 이 TFTP 서버에 프로비전하려고 했습니다.

```
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 서버에서 TFTP 컨피그레이션 및 OPT 컨피그레이션을 제거한 후, WxC를 사용하여 디바이스를 프로비저닝하는 프로세스를 다시 시작하려면 디바이스를 공장 초기화해야 합니다.
전화기에서 디바이스를 프로비저닝하는 첫 번째 시도는 URL activate.cisco.com에 요청을 하는 것입니다. 전화기에서 도메인을 확인하기 위해 DNS 서버에 쿼리합니다. DNS 확인이 실패할 경우 다음과 같이 표시될 수 있습니다.

<#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
```

전화기에서 도메인을 확인할 수 있는 경우 다음과 같이 표시됩니다.

```
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.com에 대한 GET 요청에서 200 OK를 수신한 전화기는 cisco.siplash.com에 요청을 합니다. 동일한 프로세스이며, 전화기에서 도메인 확인을 시도하지만 실패하면 다음과 같이 표시될 수 있습니다.

```
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"
```

전화기에서 도메인을 확인할 수 있는 경우 다음과 같이 표시됩니다.

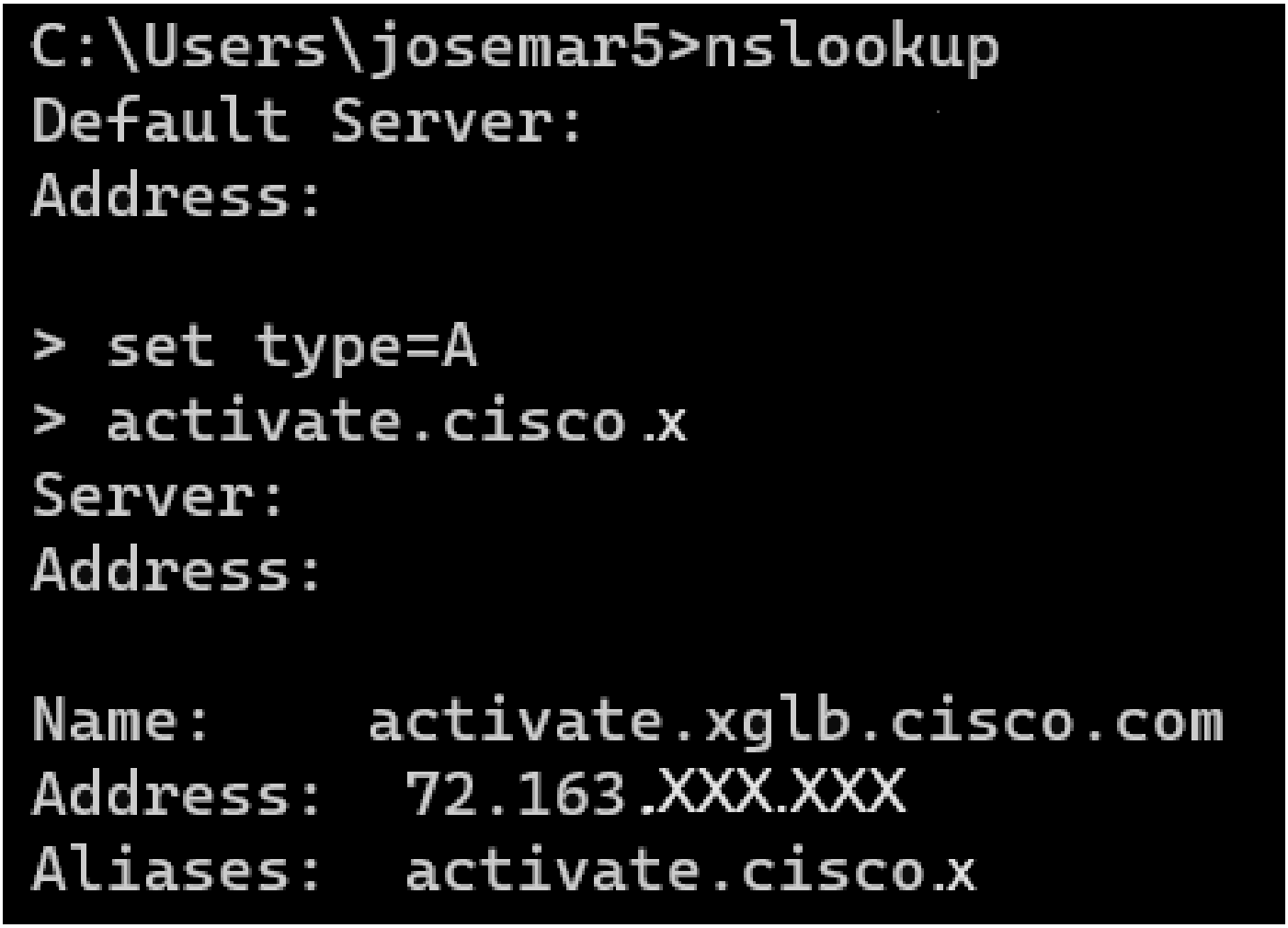
```
1980 NOT Sep 04 22:49:28.832733 (968-1290) voice-reqByCurlInternal sending http request out..., url: ht
1981 INF Sep 04 22:49:28.833577 dnsmasq[560]: query[A] cisco.sipflash.x from 127.0.0.1
1982 INF Sep 04 22:49:28.833628 dnsmasq[560]: forwarded cisco.sipflash.x to 192.168.100.1
1985 INF Sep 04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

Trobuleshoot DNS(프로비저닝 URL)

디바이스가 DNS 확인에 문제가 있는 동일한 네트워크에 있는 경우 nslookup을 사용하여 DNS 서버가 도메인을 확인할 수 있는지 확인할 수 있습니다. 명령줄 인터페이스를 열고 다음 단계를 수행합니다.

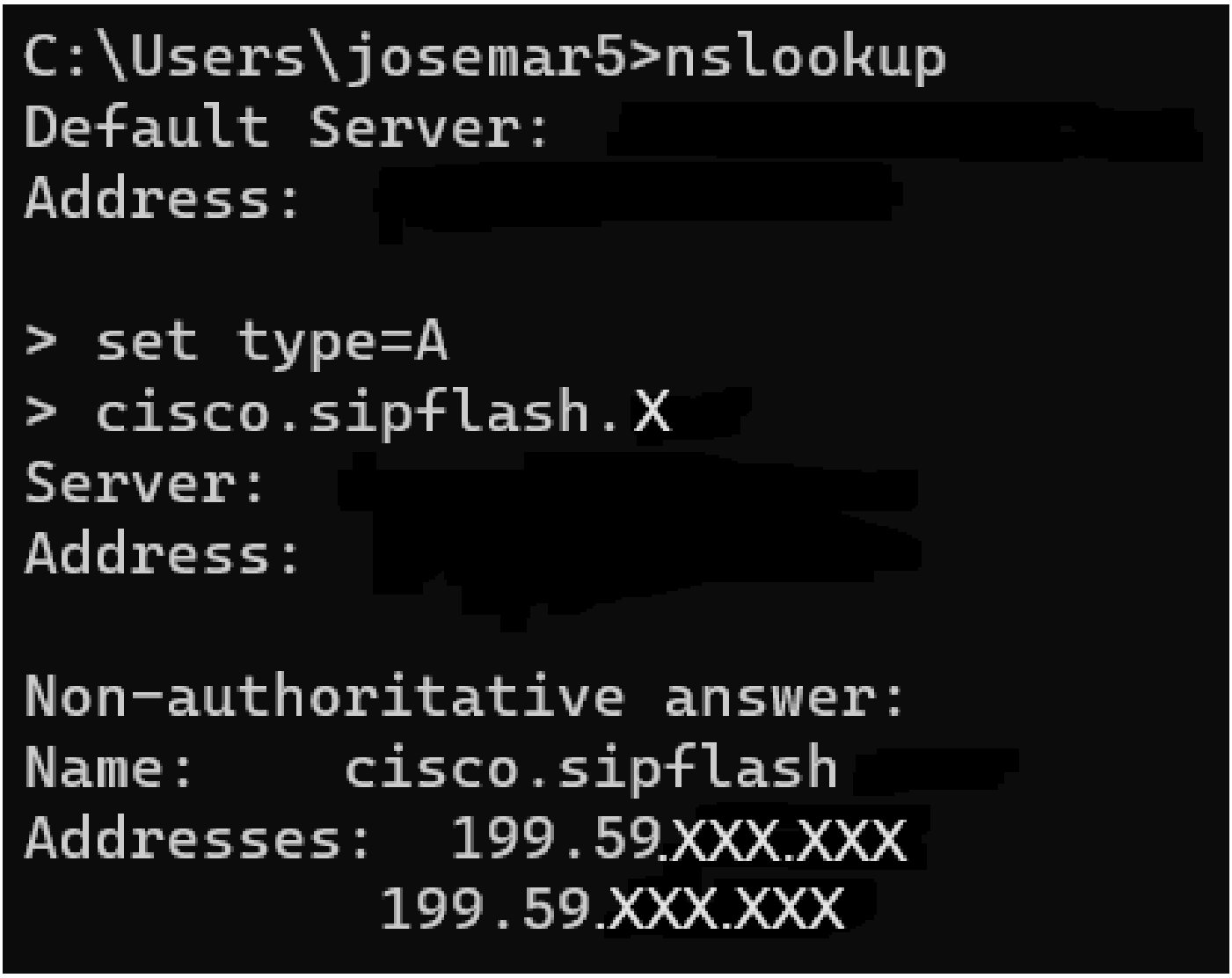
- nslookup -> Enter
- set type=A -> Enter
- activate.cisco.com

PC에서 도메인을 확인할 수 있는 경우는 다음과 같습니다.



nslookup activate.cisco

cisco.sipflash.x에서 도메인을 확인하는 동일한 프로세스를 수행할 수 있습니다.



nslookup cisco sipflash

PC에서 도메인을 확인할 수 없는 경우 DNS 서버를 확인합니다.

WxC에서 MPP 디바이스의 등록을 Trobleshoot합니다.

이 예에서 아웃바운드 프록시는 da02.hosted-us10.bcld.webex.com입니다. 전화기에서 SRV 도메인 확인을 시도합니다.

```
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
```

전화기가 SRV 도메인을 확인할 수 있으면 호스트 이름을 가져옵니다.

```
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
```

이러한 호스트 이름 중 하나에서 전화기는 다음 호스트 이름 중 하나를 사용하여 WxC SBC에 de 디바이스를 등록합니다.

```
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
```

디바이스는 WxC 측에서 401 Unauthorized(401 무단) 메시지를 받아야 합니다.

```
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
```

디바이스는 Authorization 헤더가 포함된 REGISTER를 전송합니다.

```
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
```

그런 다음 디바이스에서 SIP 200 OK를 가져옵니다.

```
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
```

이 프로세스가 끝나면 디바이스가 가동되어 WxC 서비스에 등록되어야 합니다.

DNS 문제 해결(URL 등록)

디바이스가 DNS 확인에 문제가 있는 동일한 네트워크에 있는 경우 nslookup을 사용하여 DNS 서버

가 도메인을 확인할 수 있는지 확인할 수 있습니다. 명령줄 인터페이스를 열고 다음 단계를 수행합니다.

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

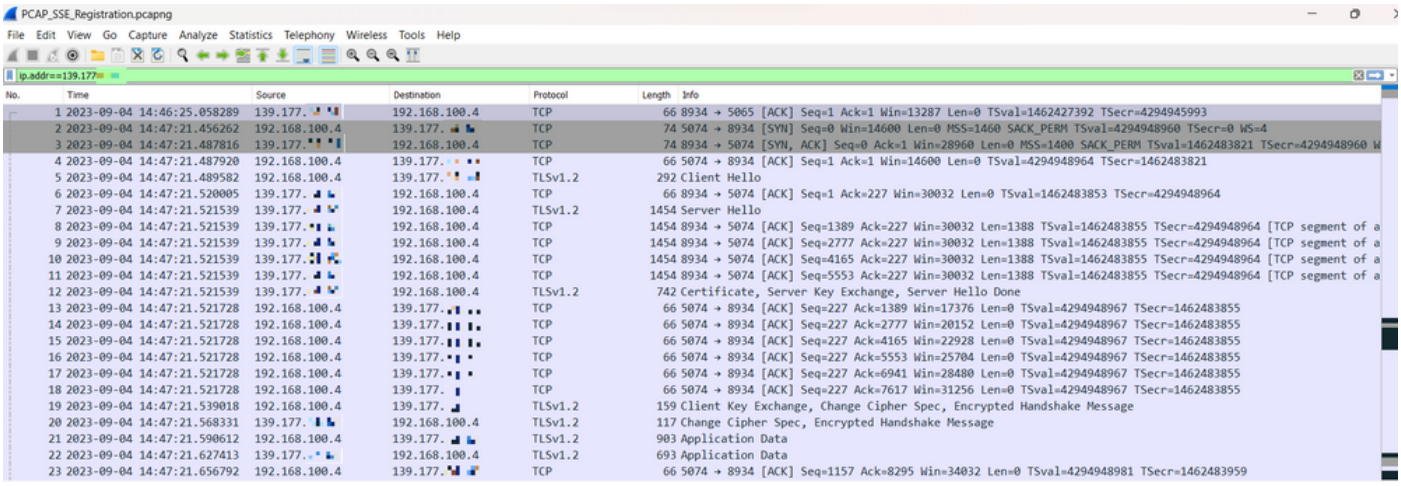
PC에서 도메인을 확인할 수 있는 경우 다음과 같이 표시됩니다.

```
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

패킷 캡처(등록 프로세스)

전화기가 등록을 위해 가지고 있는 IP 주소를 가져올 수 있으며, 패킷 캡처에서 필터를 사용하여 TLS 핸드셰이크를 확인할 수 있습니다.



캡 SSE

패킷 캡처는 TLS 핸드셰이크가 실패했는지 확인하는 데 도움이 될 수 있습니다.

Cisco Webex Calling TAC 지원

로그를 분석하고 문제의 근본 원인을 찾기 위해 지원이 필요한 경우 Cisco Webex Calling TAC 팀에 문의하십시오.

지원 관련 정보

[Webex 통화에 대한 포트 참조 정보]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.