أستكشاف أخطاء هاتف حماية مستوى الإدارة (MPP) وإصلاحها في خدمة WxC للتزويد والتسجيل

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء هواتف MPP وإصلاحها في WxC لمشكلات التوفير والتسجيل عند إضافة الجهاز بواسطة عنوان MAC.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشبكة الأساسية
- هواتف إم بي

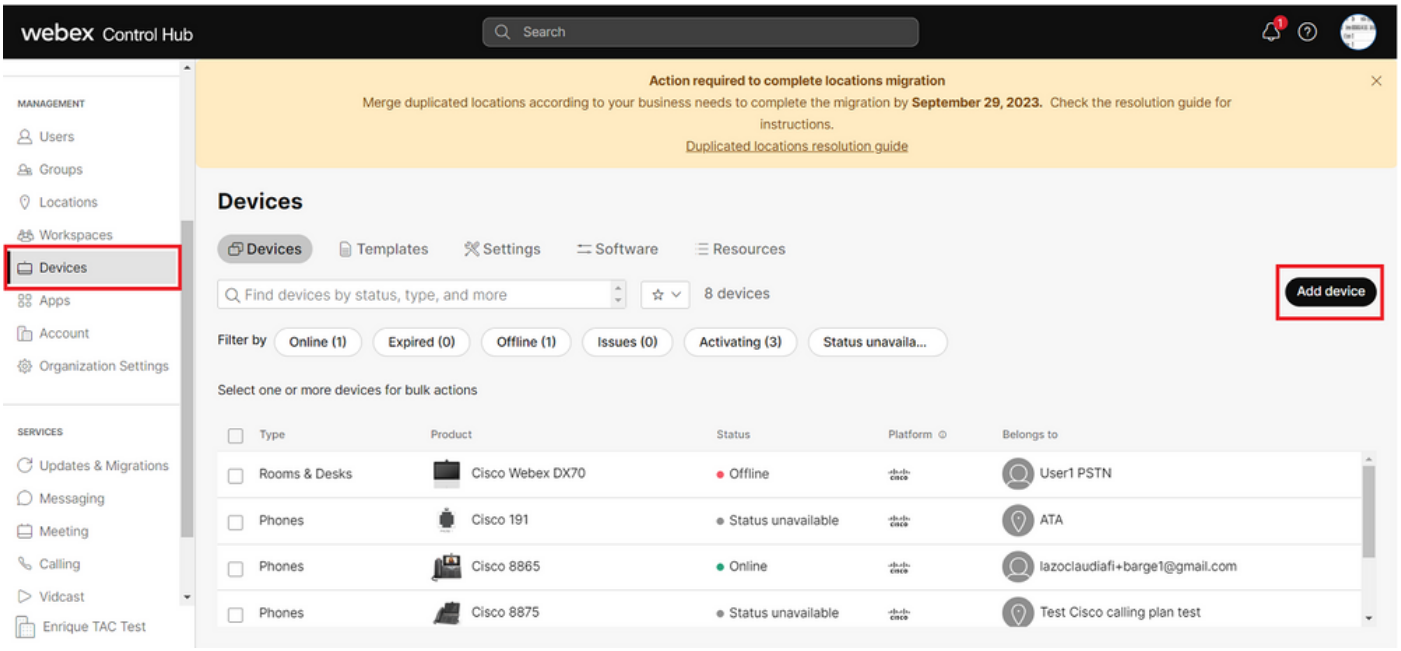
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى هواتف MPP فقط مثل 78xx و 88xx.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

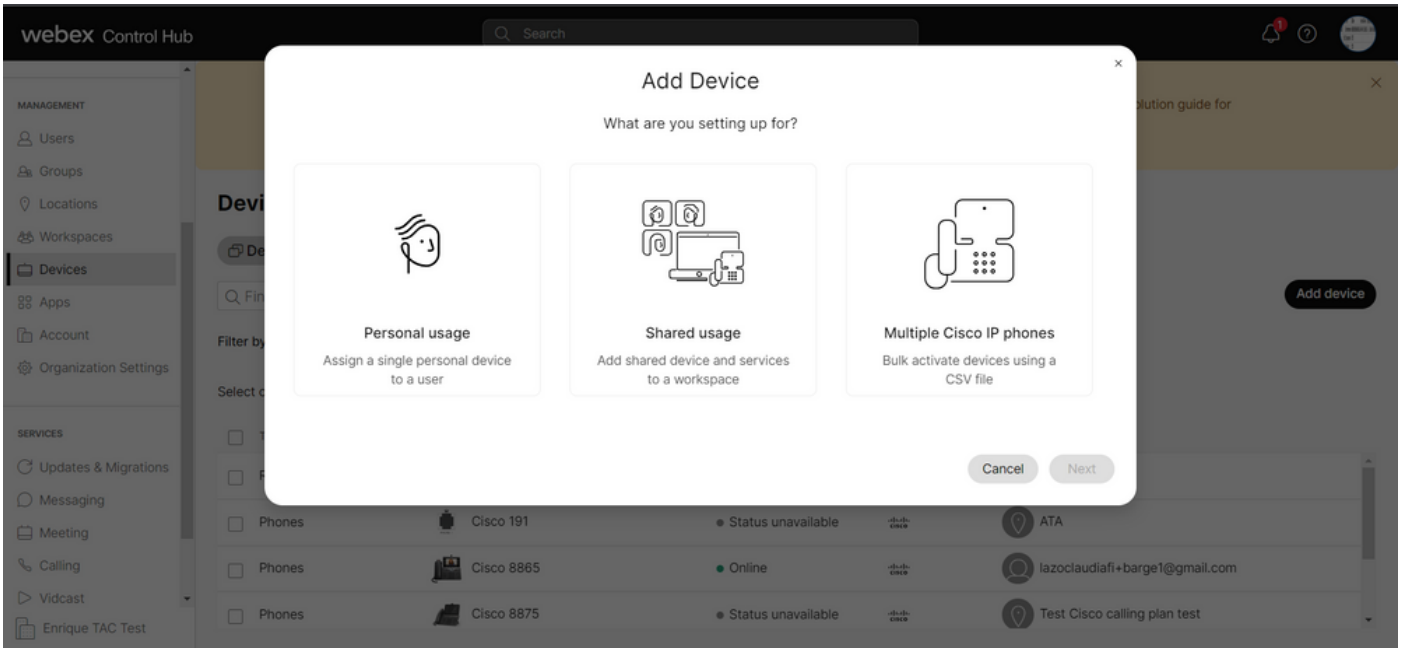
إضافة الجهاز في Control Hub

الخطوة 1. انتقل إلى admin.webex.com واستخدم بيانات اعتماد المسؤول. في المؤسسة، انتقل إلى الأجهزة > إضافة جهاز:



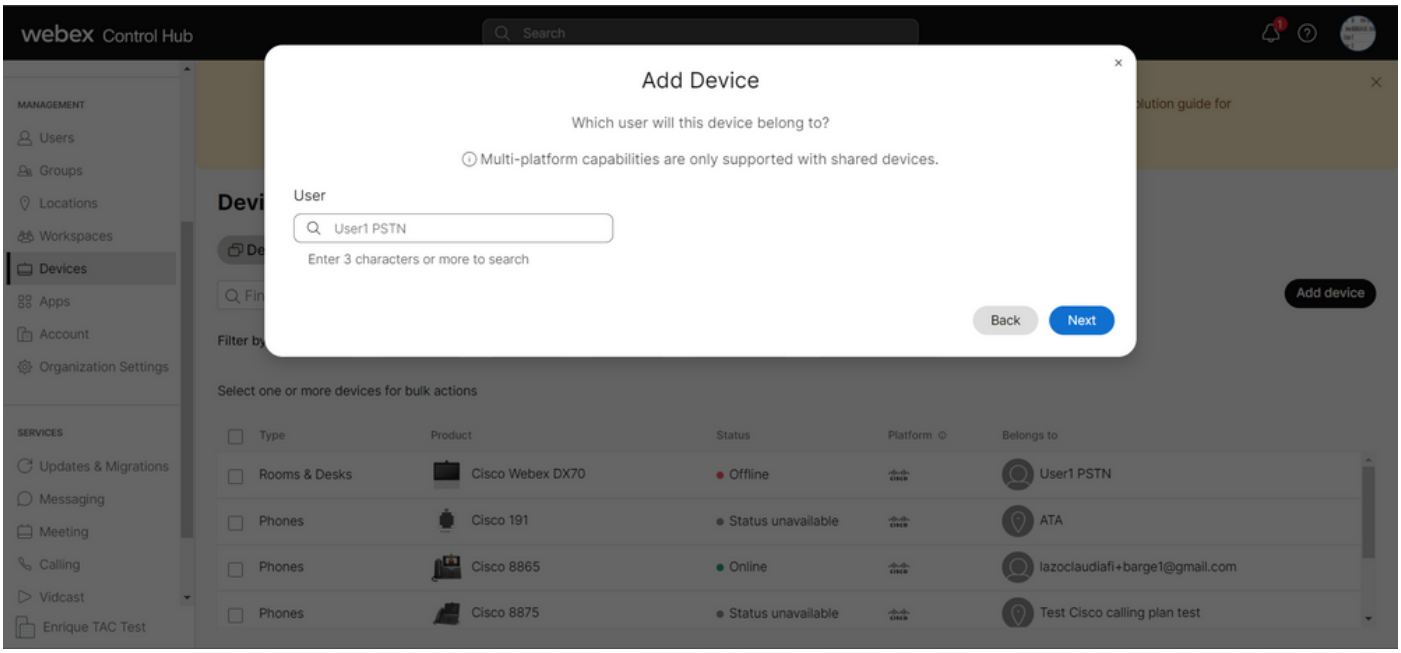
علامة تبويب الأجهزة

الخطوة 2. حدد الاستخدام الشخصي المراد تعيينه لمستخدم أو حدد الاستخدام المشترك ليتم تعيينه لمساحة عمل. (في هذا السيناريو، يتم إستخدام مستخدم.)



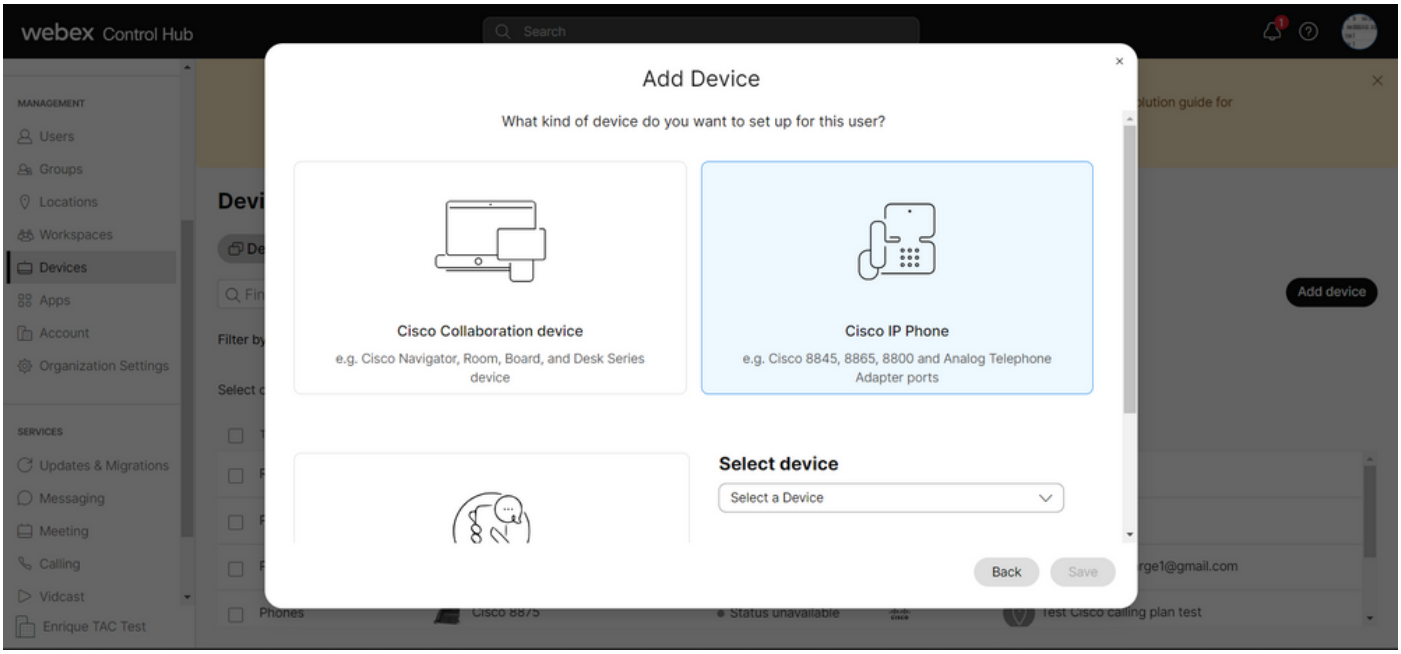
إضافة جهاز

الخطوة 3. ابحث عن المستخدم الذي تريد تعيينه على هذا الجهاز ثم انقر فوق التالي:



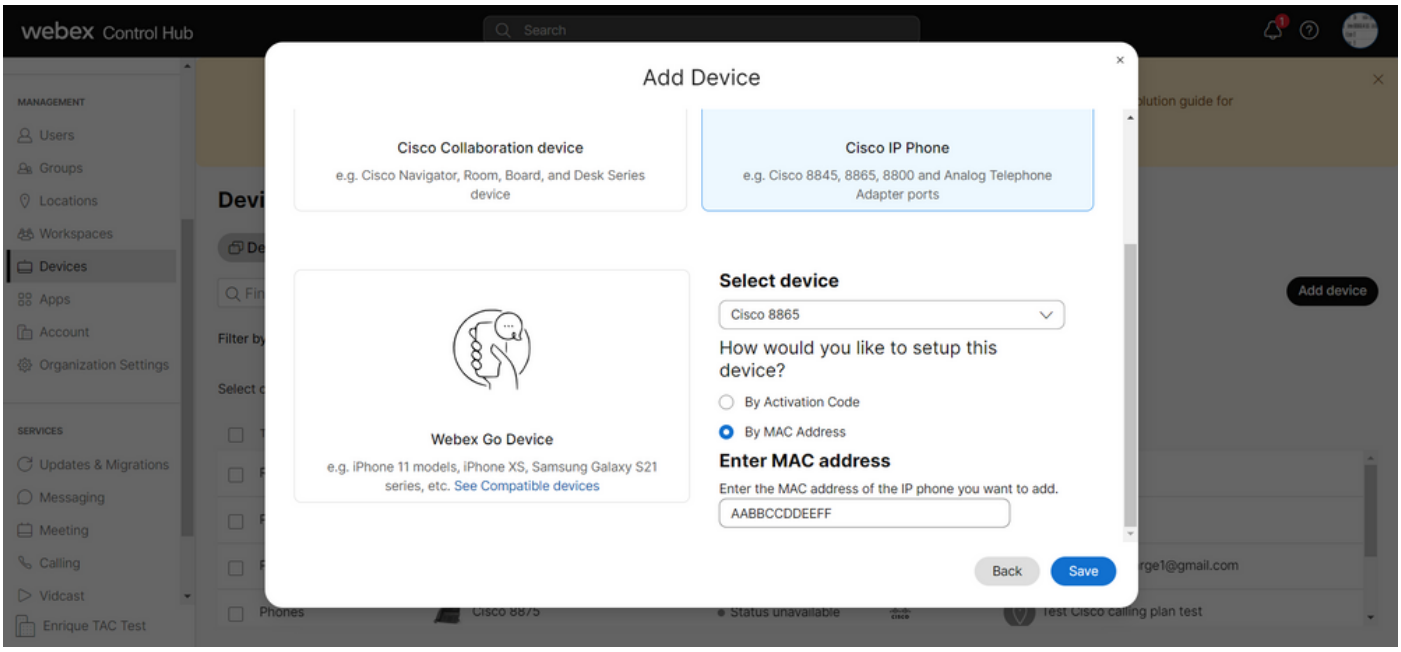
البحث عن مستخدم

الخطوة 4. حدد هاتف Cisco IP وابحث عن طراز الجهاز:



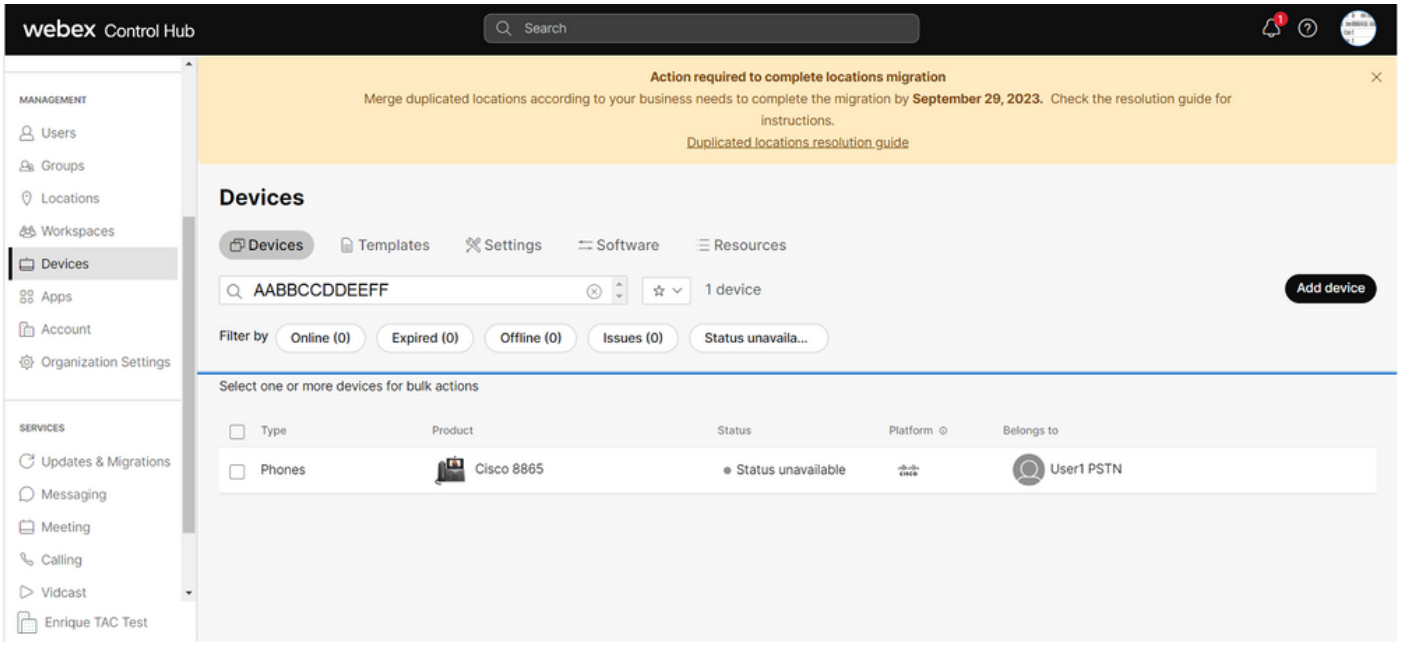
تحديد طراز الجهاز

الخطوة 5. بمجرد تحديد الجهاز، حدد الخيار حسب عنوان MAC وأدخل عنوان MAC للجهاز وانقر حفظ:



إضافة عنوان MAC

الخطوة 6. بمجرد أن يكون الجهاز في Control Hub، يمكنك التحقق من أنه تمت إضافته بشكل صحيح عندما تقوم بالبحث في عنوان MAC في شريط البحث:

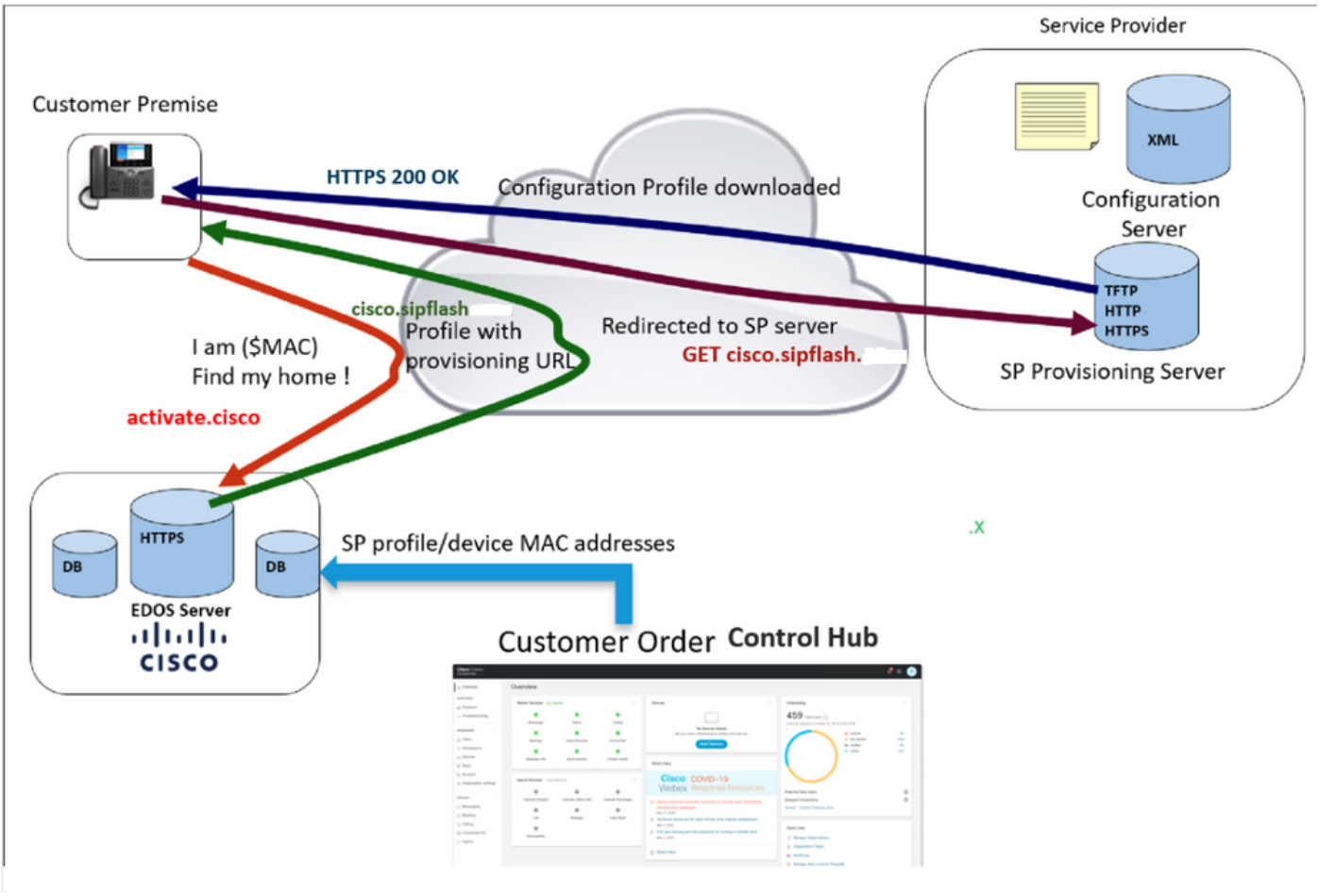


فحص الجهاز

تظهر الحالة على أنها "غير متوفرة" لأن الجهاز لا يزال غير موجود. بمجرد أن يكون الجهاز في Control Hub، فإن الخطوة التالية هي إعادة ضبط الجهاز في المصنع. بعد إعادة ضبط المصنع، يجب على الجهاز تقديم طلب إلى خوادم WxC للحصول على ملفات التكوين. (وهذه هي عملية توفير الموارد). يتم توفير الجهاز بنجاح عندما يعرض الجهاز رقم الهاتف و/أو الملحق في الشاشة.

إذا رأيت أن الجهاز لا يعرض التكوين المناسب، فإن عملية توفير الجهاز فشلت.

ملخص موجز لعملية توفير الجهاز في مركز الإتصال العالمي WXc



الرسم التخطيطي للتوفير

أستكشاف أخطاء عملية توفير جهاز في WXc وإصلاحها

لا يمكن لجهاز حماية مستوى الإدارة (MPP) تزويد WxC إذا تم تكوينه باستخدام:

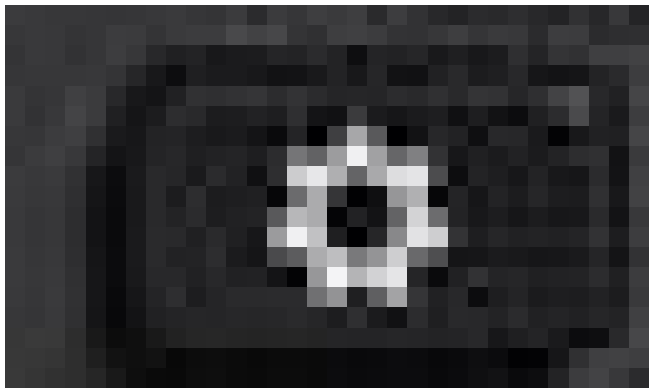
- خادم TFTP تم تكوينه في خادم DHCP
- إذا تم تكوين الخيار (OPT66 أو OPT160 أو OPT159 أو OPT150) وتوفيره بواسطة خادم DHCP

لمعرفة ما إذا كان الهاتف قد أخذ تكوين TFTP من خادم DHCP، يلزم إستخدام سجلات فريق إعادة الإعمار.

إنشاء سجلات PRT من جهاز MPP

الإرسال من سجلات فريق إعادة الإعمار من الهاتف. توضح الخطوات التالية كيفية إنشاء سجلات إعادة الإعمار.

إنشاء فريق إعادة البناء من الجهاز



الخطوة 1.على الجهاز، اضغط على الزر التطبيقات

زر الإعدادات

.

الخطوة 2.انتقل إلى الحالة > مشكلة التقرير.

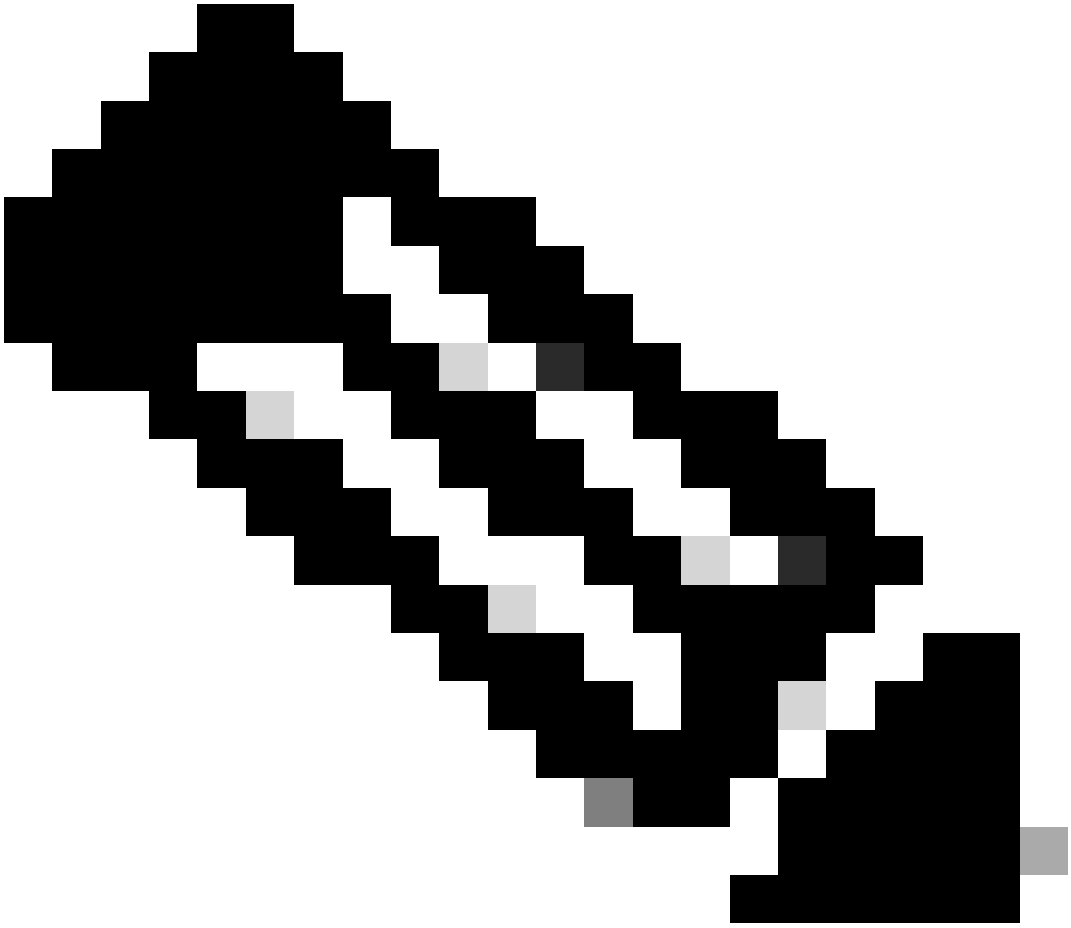
الخطوة 3. أدخل تاريخ المشكلة ووقتها.

الخطوة 4.حدد وصفا من القائمة.

الخطوة 5.PressSubmit.

ما إن يتم تقديم السجلات، راجع الخطوات التالية لتنزيل سجلات فريق إعادة الإعمار:

الخطوة 1. تسجيل الدخول إلى https://IP_ADDRESS_PHONE/



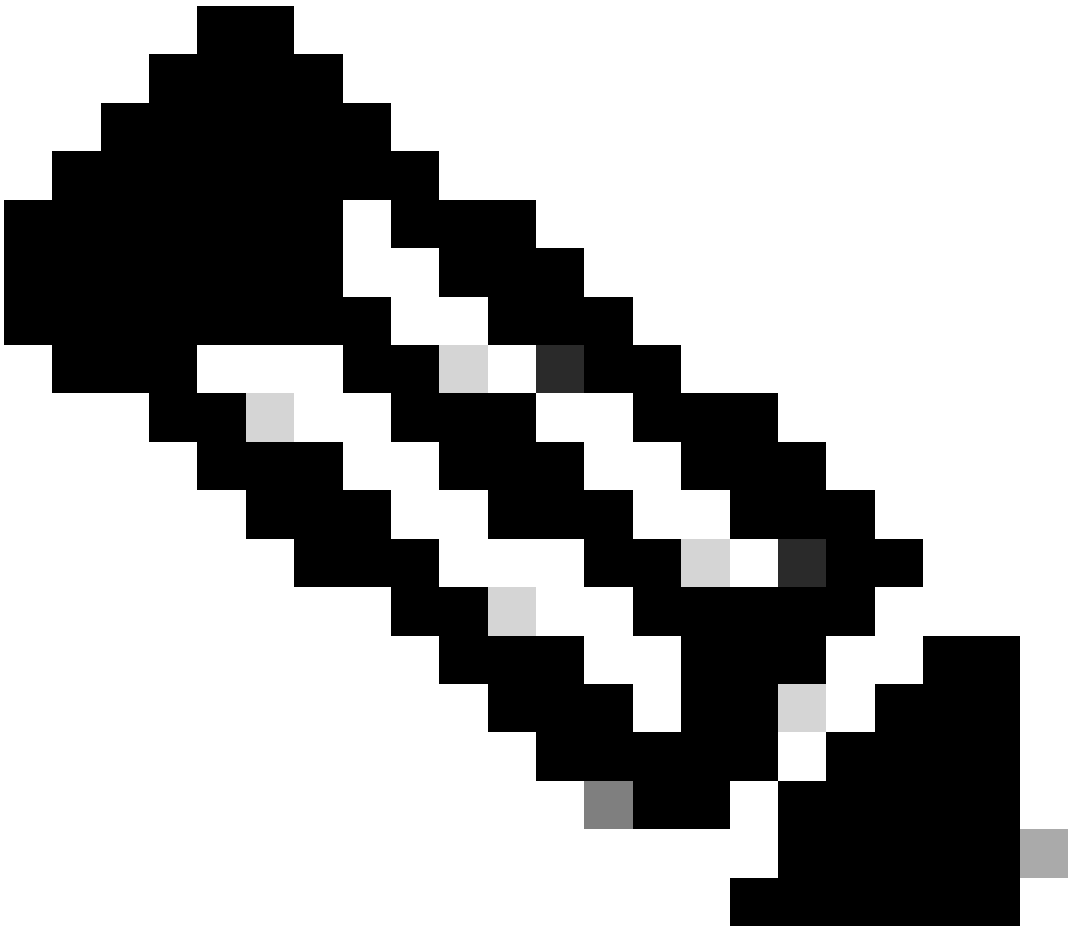
ملاحظة: ملاحظة: إذا كان عنوان IP غير معروف، يمكن الحصول عليه من الإعدادات > الحالة > حالة الشبكة > حالة IPv4

الخطوة 2. انتقل إلى المعلومات > معلومات تصحيح الأخطاء > تنزيل سجل فريق إعادة البناء الإقليمي (انقر بزر الماوس الأيمن على الارتباط وحدد حفظ باسم...)

Web Gui

سجلات فريق إعادة الإعمار

عند فتح السجلات، يمكنك مشاهدة طريقة عرض كهذه:



ملاحظة: يمكنك فتح السجلات باستخدام برنامج مثل WinRAR نظرا لضغط السجلات.

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...	

لتحليل العملية الخاصة بتوفير الجهاز، يلزم فتح السجل الذي يسمى logCat. ويمكن فتحه باستخدام محرر نصوص مثل Notepad أو Notepad++.
يمكن إستخدام الدالة "Find" من محرر النصوص للعثور على ما إذا كان الهاتف يحتوي على خادم TFTP تم تكوينه. أستخدم DHCP-tftpsvr1 أو DHCP-tftpsvr2 للعثور على السطر المحدد لهذا السجل. إذا أخذت نظرة والأسطر الأخرى من السجلات، يمكن العثور على مزيد من المعلومات حول تكوين 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:
```

كما ترى في السجل، تم تكوين عنوان IP TFTP في خادم DHCP. وهذا سبب محاولة الهاتف التوفير إلى خادم TFTP هذا بدلا من خوادم الاتصال عبر Webex.

```
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
```

بعد إزالة أي تكوين TFTP أو أي تكوين OPT من خادم DHCP، يجب عليك إعادة ضبط الجهاز في المصنع لبدء العملية لتوفير الجهاز باستخدام WxC مرة أخرى.
المحاولة الأولى التي يقوم بها الهاتف مع عملية توزيد الجهاز هي تقديم طلب إلى عنوان URL activate.cisco.com. يقوم الهاتف بإجراء استعلام إلى خادم DNS لحل المجال. إذا فشل حل DNS، يمكن أن يبدو كما يلي:

<#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
```

إذا كان الهاتف قادرا على حل المجال، فقد يبدو كما يلي:

```
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
```

بعد إستلام الـ 200 OK من طلب GET إلى activate.cisco.com يقدم الهاتف طلبا إلى cisco.siplash.com. إنها نفس العملية، الهاتف يحاول حل المجال وإذا فشل فسيبدو هكذا:

```
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"
```

إذا كان الهاتف قادرا على حل المجال، فقد يبدو كما يلي:

```
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 الخاص ب Trobuleshoot (توفير عناوين URL)

إذا كنت في نفس الشبكة حيث تواجه الأجهزة مشاكل في تحليل DNS، يمكن إستخدام NSLOOKUP للتحقق مما إذا كان خادم DNS قادرا على حل المجال. افتح واجهة سطر الأوامر وقم باالخطوات التالية:

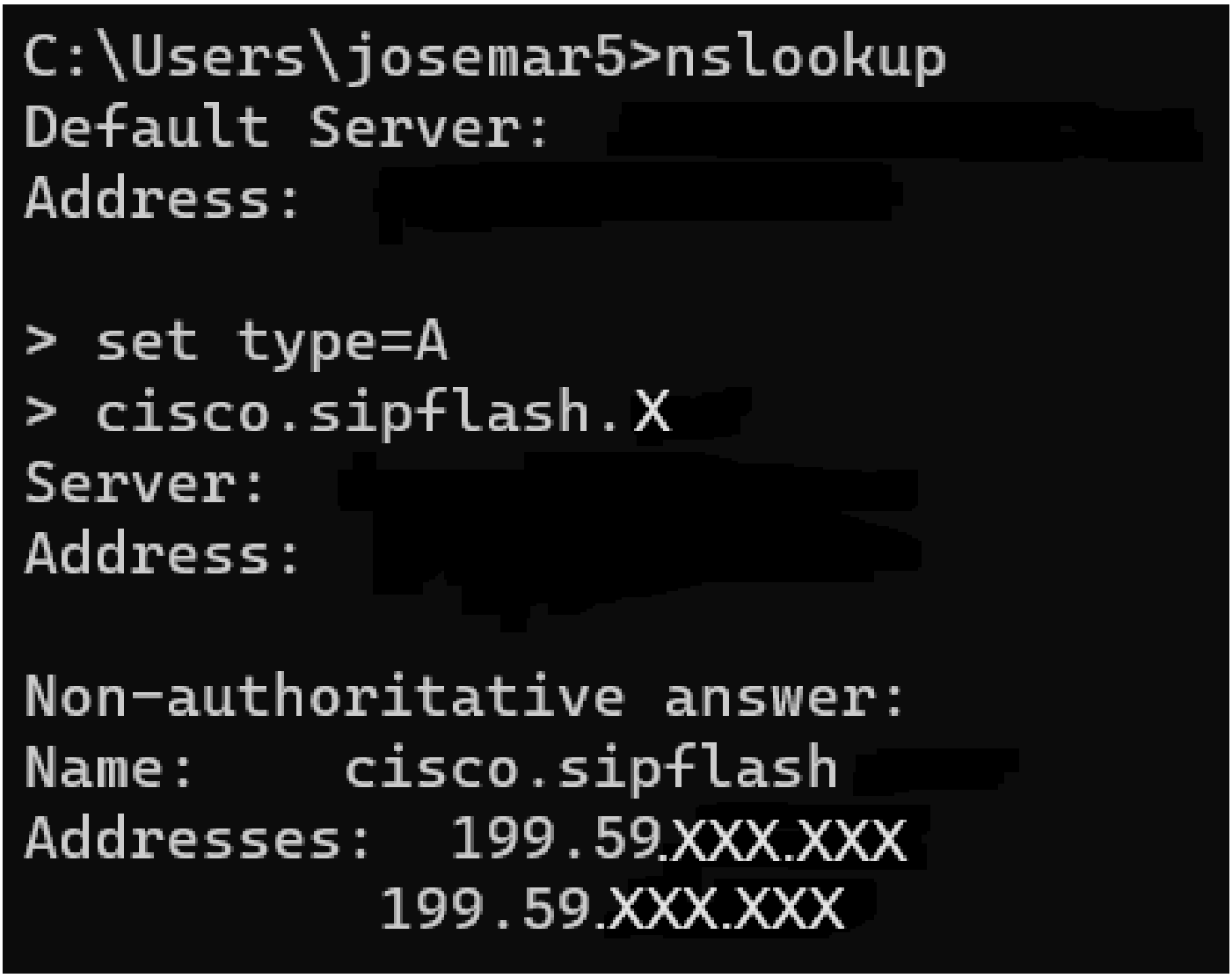
- nslookup -> إدخال
- ضبط نوع=a -> إدخال
- activate.cisco.com

إذا كان الكمبيوتر الشخصي قادرا على حل المجال، فقد يبدو كما يلي:

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

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

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

nslookup activate.cisco

يمكن إجراء العملية نفسها ل Cisco.sipflash.x لحل المجال:



nslookup cisco sipflash

إذا تعذر على الكمبيوتر حل المجالات، فراجع خادم DNS.

Trobleshoot تسجيل جهاز حماية مستوى الإدارة (MPP) في WxC

على هذا المثال، يكون الوكيل الصادر هو da02.hosted-us10.bcld.webex.com. يجب حل الهاتف لمجال SRV:

```
1721 NOT Sep 04 22:50:32.068857 (2059-2271) voice-[SIP_resolveHostName] host=da02.hosted-us10.bcld.webex
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
```

إذا كان الهاتف قادرا على حل مجال SRV، فإنه يحصل على أسماء المضيف:

```
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
```

من أحد أسماء المنازل تلك يأخذ الهاتف واحدا منهم ليسجل الجهاز في 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
```

يجب أن يحصل الجهاز على رسالة غير مصرح بها رقم 401 من جانب 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
```

يرسل الجهاز السجل برأس التخويل:

```
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
```

وبعد ذلك، يحصل الجهاز على SIP 200 موافق:

```
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
```

بعد هذه العملية، يجب أن يكون الجهاز قيد التشغيل ومسجل لخدمات WxC.

أستكشاف أخطاء DNS وإصلاحها (تسجيل عناوين URL)

إذا كنت في نفس الشبكة حيث تواجه الأجهزة مشاكل في تحليل DNS، يمكن إستخدام NSLOOKUP للتحقق مما إذا كان خادم DNS قادرا على حل المجال. افتح واجهة سطر الأوامر وقم باالخطوات التالية:

- nslookup -> إدخال
- ضبط نوع=SRV -> إدخال
- _sips._tcp.da02.hosted-us10.bcld.webex.com

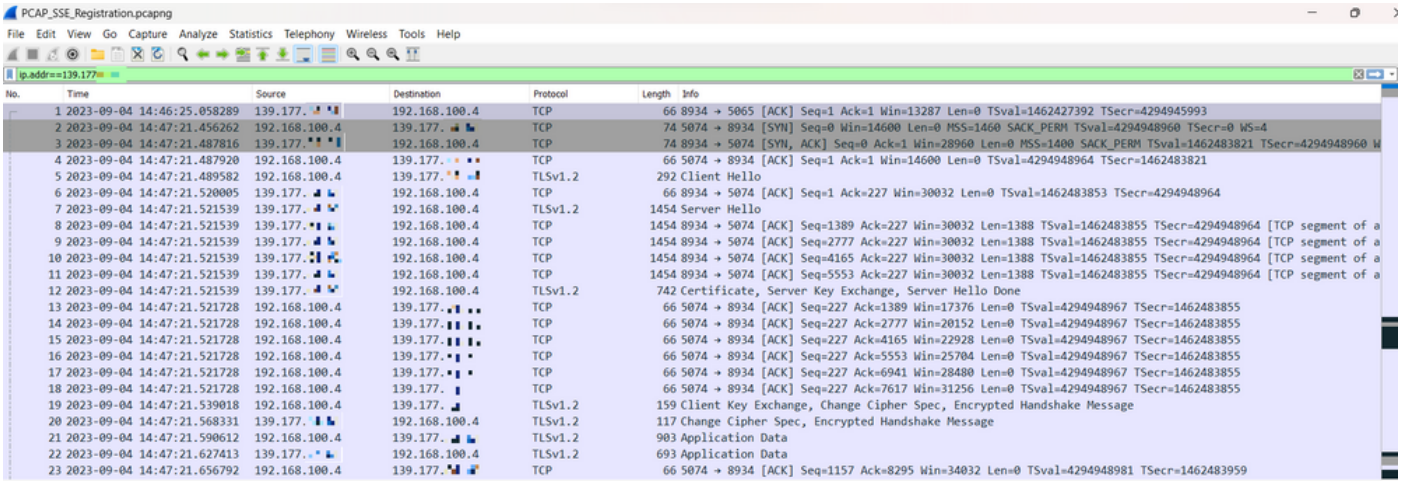
إذا كان الكمبيوتر قادرا على حل المجال، فقد يبدو كما يلي:

```
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:
```

OBP ل NSLOOKUP SRV

التقاط الحزمة (عملية التسجيل)

يمكنك أخذ عنوان IP الذي يملكه الهاتف للتسجيل، ويمكن إستخدام عامل التصفية في التقاط الحزمة للنظر في مصافحة TLS:



PCAP SSE

يمكن أن يساعد التقاط الحزمة لمعرفة ما إذا فشلت مصافحة TLS.

دعم TAC بالاتصال ب Cisco Webex

إذا كنت بحاجة إلى الدعم لتحليل السجلات والعثور على السبب الجذري للمشكلة، فيرجى الاتصال بفريق TAC لاستدعاء Cisco Webex.

معلومات الدعم ذات الصلة

[معلومات مرجع المنفذ للاتصال عبر Webex]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).