验证并恢复17.12上受升级故障影响的Catalyst AP

目录

简介

互动式协助

情景

根本原因详细信息

受影响的代码和接入点

- 受影响的接入点
- 受影响的代码

固定代码

升级路径和漏洞适用性

- Bug not applicable and upgrade path
- Bug适用和升级路径

升级预检查

- 手动预检查
- 自动预检查
- 预检查结果

恢复

- 分区2中的低空间可用性
  - 删除接入点核心文件
  - 出厂时重置接入点
  - 删除cnssdaemon.log文件(Access Point devshell)
  - 接入点映像启动分区交换
- 接入点引导循环

何时创建TAC案例

常见问题解答

简介

本文档介绍当接入点受到Cisco Bug ID CSCwf25731和CSCwf37271影响时的验证和恢复过程。

互动式协助

如果您使用您的CCO凭证登录，Cisco AI Assistant for Support可以帮助您以交互方式确定此Bug是否适用于您的网络，以及是否适用于您的网络以确定恢复选项。开始使用：

1. 点击位于文档右下角的Cisco AI Assistant for Support图标。
   - 

2. 使用您的思科凭证登录。
3. 登录后，请刷新浏览器选项卡/文档。
4. 点击右下角的聊天机器人图标，开始询问与本文档相关的问题。
   - 

为了获得最佳效果，从简单的问题开始，然后逐渐增加复杂性。如果回答不满意，请点击向下缩略图图标给予反馈。如果Cisco AI Assistant for Support的答案不清楚，您可以随时参考此文档。

情景

如果升级或APSP应用于当前运行17.12.4/5/6/6a或以前运行这些版本的系统并运行相当长的时间，会导致受影响的接入点型号（请检查下面受影响的接入点列表）在某些情况下进入启动循环，这些情况由因接入点存储上的磁盘空间不足而导致的映像安装故障触发。虽然这不会影响日常操作或SMU，但在ISSU、完整控制器代码升级或APSP安装过程中仍存在重大风险，因为这些过程涉及接入点映像升级。

需要遵循其他流程，该流程需要执行本文档中提到的强制升级预检查步骤，因为不存在任何配置变通方法。

要解决此问题，在接入点尝试升级之前，必须在WLC中安装特定APSP版本修补程序（显示在下面的“固定代码”表中），或者使用清理APSP（适用于17.15.4d和17.18.2）（如果已移至更高版本，但运行了任何受影响的版本）。即使您不确定您的系统历史记录，强烈建议您在升级或APSP安装之前执行存储检查，以确定环境中是否存在受影响的版本。

根本原因详细信息

运行17.12.4到17.12.6a的接入点受到生成持久日志文件的库Bug的影响：/storage/cnssdaemon.log。此文件每天增长5 MB，并且不会通过重新启动来清除，最终会耗尽设备存储空间。因此，如果接入点从引导分区1(Part1)运行，并且由于日志文件导致引导分区2(Part2)已满，则升级过程将失败，因为它无法在引导分区2中存储新映像，可能导致引导循环。要防止这种情况，您必须清除存储或确保接入点已从分区2启动，然后通过执行本文档中的说明尝试任何进一步升级。

受影响的代码和接入点

受影响的接入点

以下接入点型号是唯一容易受此问题的型号。如果您的网络不使用任何这些特定型号，则您的环境不会受到影响，无需进一步操作。

- Catalyst 9124(I/D/E)
- Catalyst 9130(I/E)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E
- Catalyst 9164I
- Catalyst 9166(I/D1)
- Catalyst IW9167(I/E)

受影响的代码

要在网络中验证这一点，请从所有WLC中执行以下命令并验证WLC中的代码是否列在下表中。

```
WLC# show version | in Version
```

或者，您也可以从接入点执行相同操作。检查输出，查看主映像或备份映像是否正在运行表中列出的映像中的受影响映像。

```
AP# show version | in Image
```

受控制器影响的代码	受接入点影响的图像
17.12.4	从17.12.4.0到17.12.4.212
17.12.5	从17.12.5.0到17.12.5.208
17.12.6/6a	从17.12.6.0到17.12.6.200



注意：注意：通常，如果网络未运行且过去未运行17.12.4、17.12.5、17.12.6/6a，则问题不适用。

固定代码

下表列出了包含此Bug的修复程序的WLC软件版本及其相应的APSP（接入点服务包）。请注意，对于下面列出的版本，在撰写本文时，修复程序目前只能通过APSP安装提供。

控制器和APSP固定代码	接入点固定图像
17.12.4 + APSP13	17.12.4.213
17.12.5 + APSP9	17.12.5.209
17.12.6a + APSP1	17.12.6.201
17.12.7安	17.12.7.13
17.15.3 + APSP12	17.15.3.212
17.15.4b + APSP6	17.15.4.206
17.15.4d + APSP1	17.15.4.225
17.15.5	17.15.5.36
17.18.1 + APSP3	17.18.1.203
17.18.2 + APSP2	17.18.2.202
17.18.3	17.18.3.18
26.1.1	26.1.1.11

升级路径和漏洞适用性

使用下表来确定您当前的WLC和接入点软件版本是否适用于此Bug，以及要执行的升级步骤。如果当前部署与Bug applicable and upgrade path表中的任何这些版本匹配，则必须在尝试任何进一步升级之前执行升级预检查部分中说明的存储预检查。

Bug not applicable and upgrade path

下表显示您的WLC和接入点是否不适用于此Bug:

当前代码	目标代码	Bug适用性	升级前 — 需要进行预检查	目标/升级路径	升级预检查	备注
17.3.x / 17.6.x / 17.9.x	17.12.x	无	无	17.12.4 + APSPx 17.12.5 + APSPx17.12.6a + APSPx17.12.7	无	查看目标版本说明
17.9.x	任何（17.12.4/5/6/6a除	无	无	遵循目标升级路径	无	17.9.1到。5不支

	外）					持直接升级到17.15，请使用17.9.6或更高版本以获取更多信息，请参阅版本说明
17.12.1 到 17.12.3	任何（17.12.4/5/6/6a除外）	无	无	遵循目标升级路径	常规流程	查看目标版本说明
17.15+新部署	any	无	无	any	无	
17.18.+新部署	any	无	无	any	无	

Bug适用和升级路径

下表显示您的WLC和接入点是否适用于此Bug:

当前代码	目标代码	Bug适用性	升级前 — 需要进行预检查	目标/升级路径	升级预检查	备注
17.12.4/5/6/6a	17.12.x（4、5、6、6a等），APSP	Yes	Yes:请参阅升级预检部分	17.12.4 + APSP、17.12.5 + APSP、17.12.6a + APSP、17.12.7	Yes	安装固定APSP后，无需对未来17.12升级进行额外预检查
17.12.4/5/6/6a	17.15.x / 17.18.x	Yes	Yes:请参阅升级预检部分	升级相应的17.12.x APSP，然后升级到17.15.x + APSP或17.18.x + APSP	对于第一个17.12 APSP升级为“是”，对于后续升级为“否”。	
任何版本，但以	17.15.x	Yes	Yes:请参阅升级预	17.15.x +	Yes	

前的映像是17.12.4/5/6/6a之一			检部分	APSP		
任何版本，但以前的映像是17.12.4/5/6/6a之一	17.18.x	Yes	Yes:请参阅升级预检部分	17.18.x + APSP	Yes	

升级预检查

为了确保无线接入点在分区2（第2部分）中具有足够的可用空间用于代码或APSP安装，必须执行以下步骤以安全地恢复存储空间：

1. 识别：执行手动或自动预检查，以确定哪些特定接入点适用于此Bug。强烈建议进行自动预检查。
2. 恢复：对于第2部分中标记为空间不足的任何接入点，请遵循“空间恢复”部分中提到的恢复过程。
3. 验证：重新运行预检查，确认所有设备都运行正常，并且第2部分中的空间可用性问题已解决。
4. 升级:继续升级到固定代码部分列出的固定APSP。

有两种预检查方法：

- 手动
- 自动

建议使用自动化方法，因为它可节省时间并避免人为错误。

手动预检查

1.从WLC中，您可以检查“主”和“备份”映像列，以确认您的接入点是否正在运行任何受影响的版本（请检查上面的“受影响的代码”部分）。

```
WLC# show ap image
Total number of APs  : 4

AP Name             Primary Image          Backup Image            Predownload Status   Predownload Ver
-------------------------------------------------------------------------------------------------------
Ap117.12.5.41        17.12.4.201              None                    0.0.0.0              N/A
Ap217.12.5.41        17.12.4.201              None                    0.0.0.0              N/A
Ap317.12.5.41        17.12.4.201              None                    0.0.0.0              N/A
Ap417.12.5.41        17.12.4.201              None                    0.0.0.0              N/A
```

您还可以直接在接入点级别执行类似的验证，方法是运行以下命令检查两个映像分区：

```
AP# show version
AP Running Image     :17.12.5.41
Primary Boot Image   : 17.12.5.41
Backup Boot Image    : 17.12.5.209
```

检验活动引导分区。使用“show boot”命令并确认“BOOT path-list”指向第1部分；这表示接入点当前正从主分区运行，并尝试升级到可能触发问题的辅助部分(part2)。

```
AP# show boot
--- Boot Variable Table ---
BOOT path-list: part1
```

2.通过检查/dev/ubivol/part2分区验证当前文件系统使用情况。如果“可用”列显示小于85M，则分区没有足够的空间安装APSP，这会导致升级失败并可能触发引导循环。

```
AP# show filesystems
Filesystem                Size      Used Available Use% Mounted on
devtmpfs                880.9M         0    880.9M   0% /dev
/sysroot                883.8M    219.6M    664.1M  25% /
tmpfs                     1.0M     56.0K    968.0K   5% /dev/shm
tmpfs                   883.8M         0    883.8M   0% /run
tmpfs                   883.8M         0    883.8M   0% /sys/fs/cgroup
/dev/ubivol/part1       372.1M     79.7M    292.4M  21% /part1
/dev/ubivol/part2       520.1M    291.3M    228.9M  56% /part2
```

3.验证两个分区的映像完整性，以确保它们未损坏。主映像和备份映像的所有字段必须显示“正常”状态；如果有任何字段显示其他内容，请停止该过程，并转到何时打开TAC案例部分。

```
AP# show image integrity
/part1(Backup) 17.12.5.209
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
/part2(primary) 17.12.5.41
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
```

列出从part1启动并在/dev/ubivol/part2中显示可用空间少于85M的所有接入点，因为它们将需要空间恢复。您可以转到本文档的恢复部分。

自动预检查

对于自动预检查，请使用WLANPoller工具。此工具允许您同时在所有无线接入点上运行所需的命令，以确定受影响的无线接入点；您可以从以下链接直接下载：https://developer.cisco.com/docs/wireless-troubleshooting-tools/wlan-poller-wlan-poller/

注意：下载与您的操作系统（Windows、Intel Mac或ARM Mac）兼容的WLANoller版本。确保主机与接入点具有SSH连接。

步骤:

0 - SSH：这些步骤假设在所有AP加入配置文件中启用了SSH访问，并且未阻止对接入点的SSH。

1. 解压缩 — 将WLANPoller文件解压缩到您的首选目录。解压后，您会发现两个目录和一个名为：

- 数据
- confd
- WlanPollerGUI

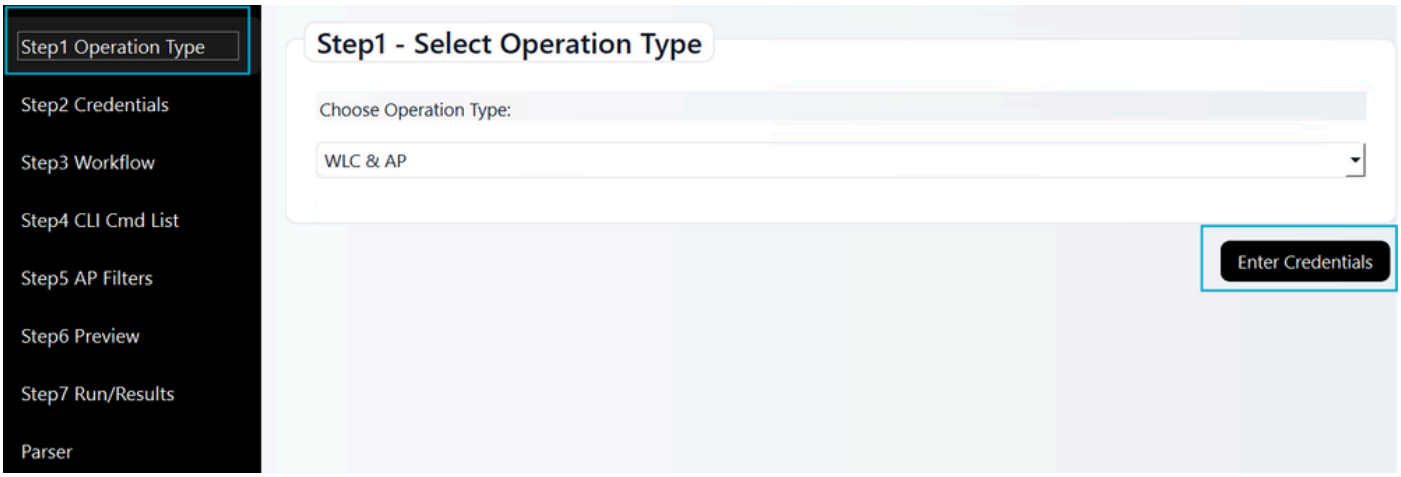
注意：如果在使用本地Windows工具解压缩后运行应用程序时遇到错误，请使用第三方实用程序（如7-Zip）解压缩文件。

注意：要使MacOS运行应用，请打开具有根访问权限的终端，然后导航到提取WLANoller的目录。执行以下命令：sudo ./Wpgui_Mac_Arm64_Ver505/WlanPollerGUI.app/Contents/MacOS/WlanPollerGUI

---

2. Configuration — 启动WlanPollerGUI应用程序并配置设置，如下所示：

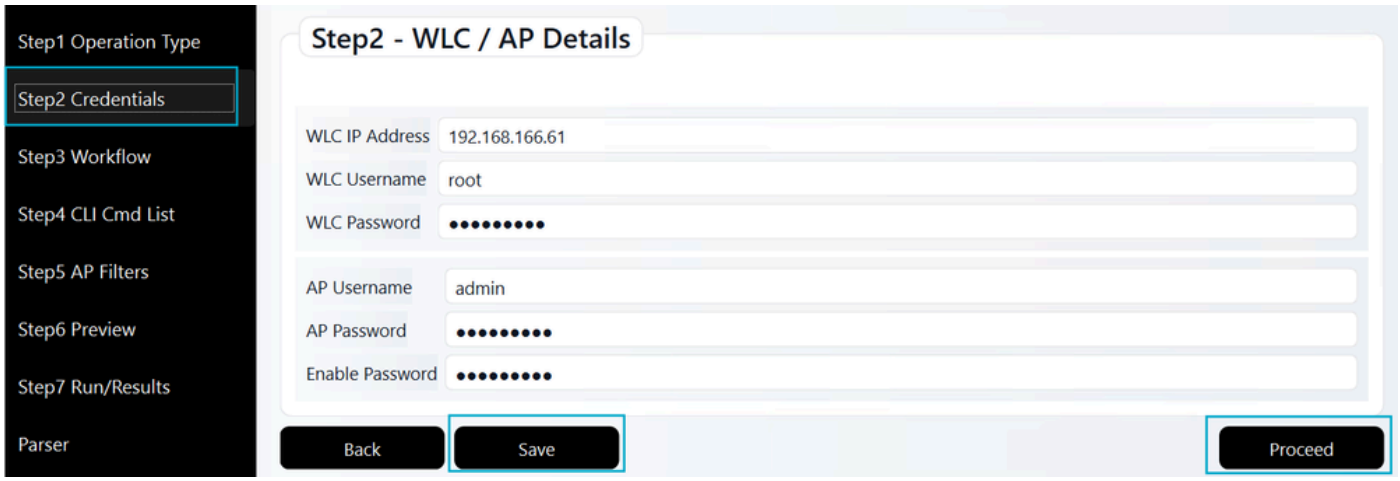
操作类型:选择WLC和AP。对于Access PointOnly选项，以逗号分隔格式上传列出接入点的“.txt”文件（例如192.168.166.105、Timpadil9166）。 然后，单击Enter Credentials。



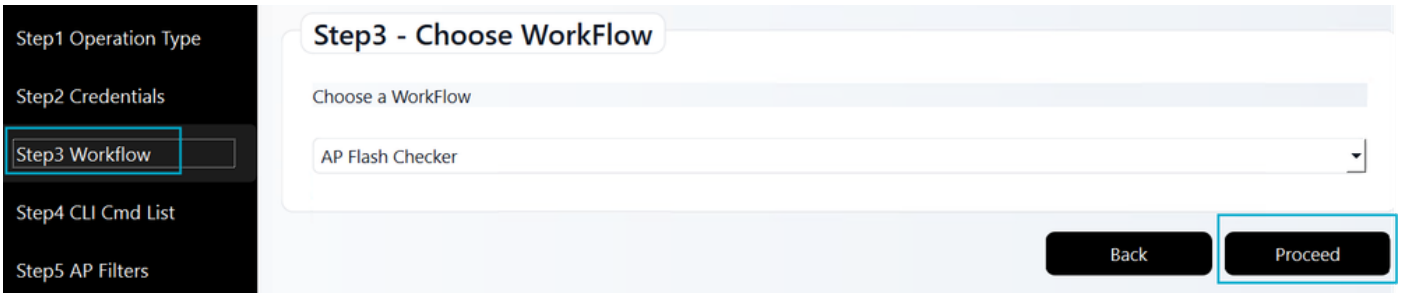
对于Access Point Only模式，请确保您的“.txt”文件符合以下示例：



凭证:输入WLC IP地址和凭证。包括来自接入点加入配置文件的接入点用户名、密码和启用密码。单击Save，然后单击Proceed。

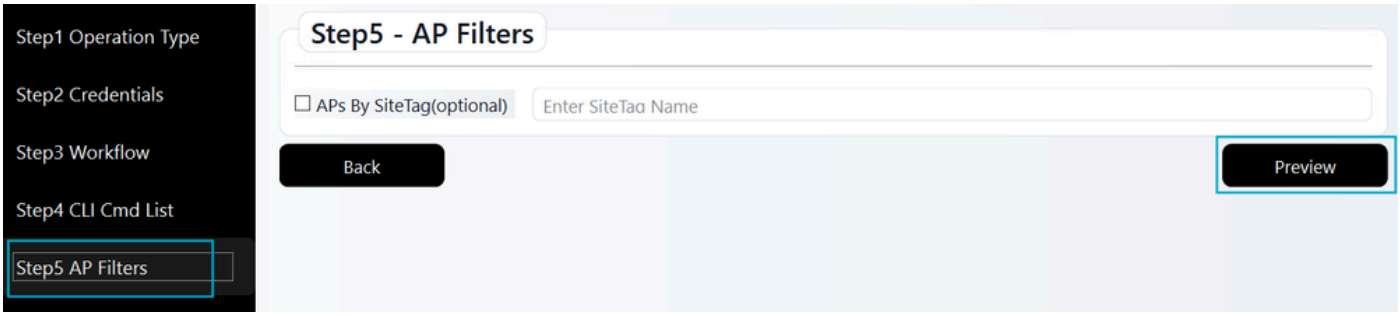


工作流:选择Access Point Flash Checker工作流程以运行所需的诊断命令。然后，点击继续。

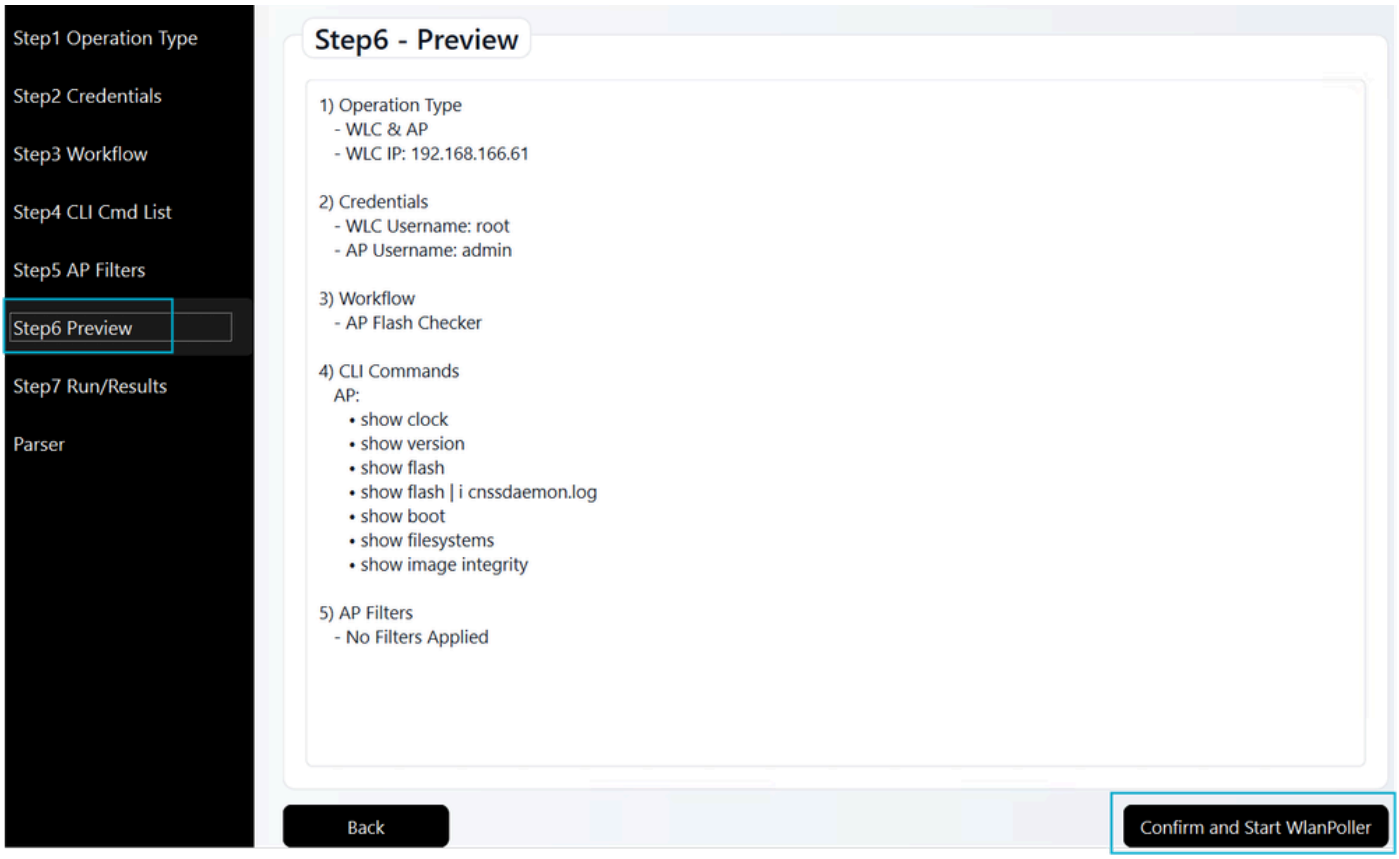


CLI Cmd列表：自动跳过此步骤；所需的命令列表已包含在Access Point Flash Checker工作流程中（第3步）。

接入点过滤器:此可选步骤允许您按特定站点进行过滤。如果使用它，请选中该框并输入Site Tag name（区分大小写）。 完成后，如果跳过此步骤，请单击Preview。

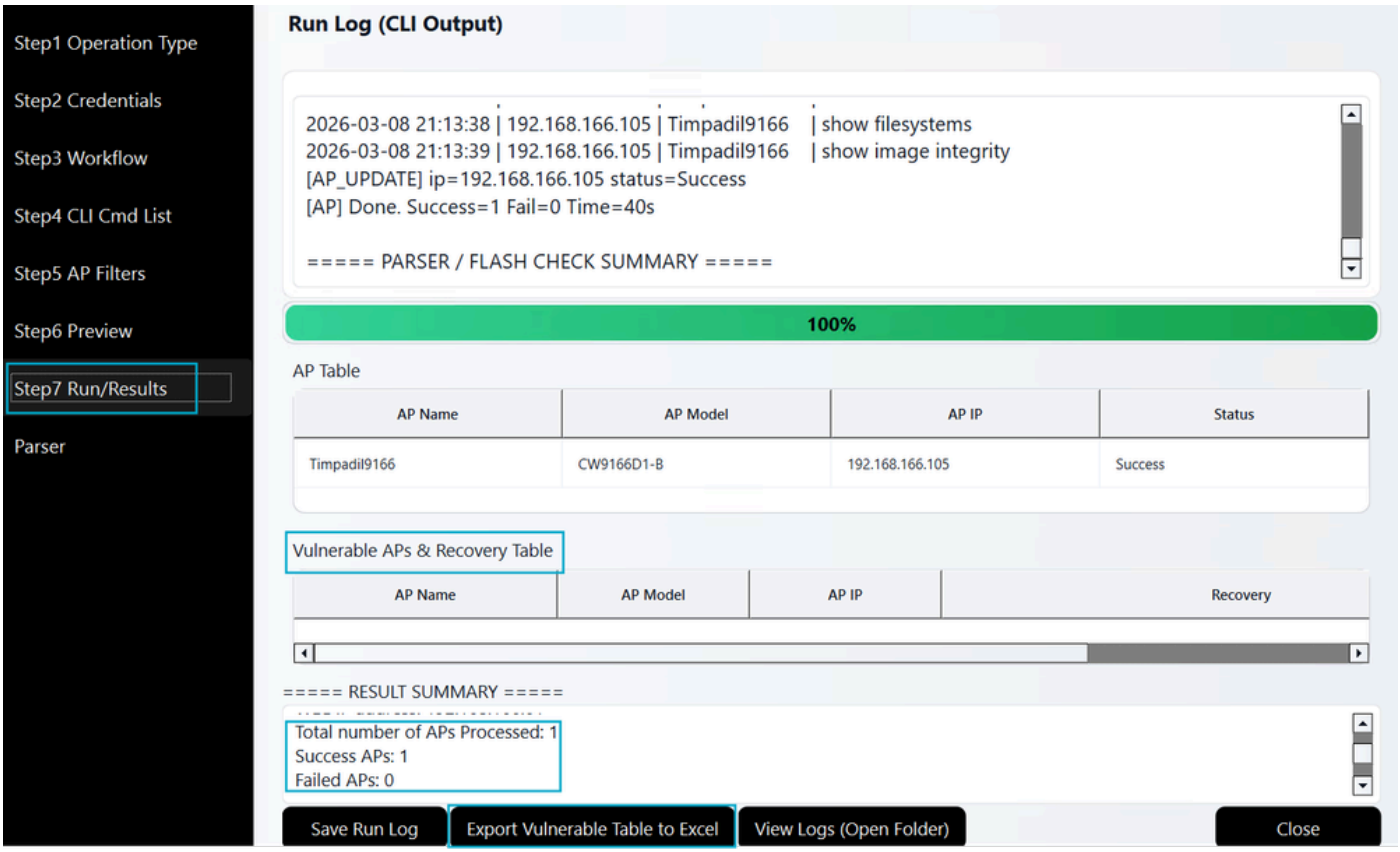


预览：在此处查看您的WLANoller设置。所需的CLI命令会从上一个工作流程步骤中预先填充。确认详细信息后，单击Confirm and Start WLANoller开始SSH连接和数据收集。



3.结果:该工具可建立与接入点的SSH连接，以运行必要的命令。显示的结果可帮助您识别需要恢复的接入点。此数据的记录会自动保存在WLANoller提取目录内的data子文件夹中。

注意：Export Vulnerable Table to Excel功能仅列出需要恢复的接入点。如果未列出接入点，则表示它未受影响。



预检查结果

根据扫描，WLANPoller将受影响的接入点分为以下选项之一：

- 安全状态，但接入点在备份分区中有错误映像:接入点当前可以安全升级，您可以继续进行代码/APSP安装。但是，请注意，备份分区仍包含易受攻击的映像。
- 使用映像分区交换进行恢复：接入点当前从分区1启动，但分区2没有足够的空间进行升级。需要接入点引导分区交换。
- 使用devshell恢复:接入点需要通过devshell进行恢复，因为分区中没有足够的空间来安装新代码或APSP。
- 此AP的映像完整性检查失败:分区1或分区2中的映像未通过完整性检查。可能需要手动干预。

恢复

根据预检查结果，您可以选择最适合您的网络的适当恢复选项，如下所示：

结果	恢复选项
安全状态，但接入点在备份分区中有错误映像	信息性，您可以继续进行代码/APSP安装
使用映像分区交换进行恢复	有4个选项：

	1.删除接入点核心文件。 2.工厂重置接入点。 3.接入点映像引导分区交换。 4.删除cnssdaemon.log文件(Access Point devshell)。 选择最适合您的环境和资源可用性的恢复选项。
使用devshell恢复	有2个选项： 1.删除cnssdaemon.log文件(Access Point devshell)。 2.工厂重置接入点。 选择最适合您的环境和资源可用性的恢复选项。
此接入点的映像完整性检查失败	按照以下步骤操作：何时创建TAC案例

根据接入点的当前状态，有两条恢复路径。接入点的状态可以是：

1. 分区2中的低空间可用性：在尝试安装代码/APSP时，在升级前阶段（在升级预检查期间找到）会发生这种情况。
2. 接入点引导循环：如果在空间不足的情况下尝试了代码/APSP安装，则升级后会发生这种情况。

下文将介绍接入点每种可能状态的详细恢复步骤。

分区2中的低空间可用性

如果升级预检查识别使用分区1启动且分区2中空间不足的接入点，请使用以下方法之一在该分区中释放空间。

- 删除接入点核心文件：接入点将核心转储存储在/dev/ubivol/part2中。如果这些文件存在，则删除它们可能会释放足够的空间。删除后，必须重新运行升级预检以验证可用空间是否符合安装要求。
- 出厂时重置接入点：执行出厂重置会将接入点恢复为其默认配置。此过程会暂时从存储中清除cnssdaemon.log文件，通常会在分区2（第2部分）中提供足够的空间以成功安装代码/APSP。
- 删除cnssdaemon.log文件(Access Point devshell):此过程涉及访问接入点devshell以手动删除cnssdaemon.log文件。请注意，这需要管理访问并与TAC协调才能进入devshell环境。

- 启动分区交换：如果分区2（第2部分）没有足够的空间来安装代码/APSP，但已经包含功能映像，您可以从第2部分启动接入点，并将安装目标定位到分区1（第1部分），分区1（第1部分）通常具有可用空间。

请查看每个选项的详细信息，确保您了解要求。选择最适合您的网络环境和运营需求的方法。

删除接入点核心文件

通过SSH访问每个接入点可以手动删除核心文件。或者，您可以使用WLANPoller自动执行此过程，并在批量模式下同时为多个接入点执行删除。

手动模式

通过SSH访问每个接入点并执行下列命令：

```
AP# delete /force cores
AP# reload
Proceed with reload? [confirm] yes
```

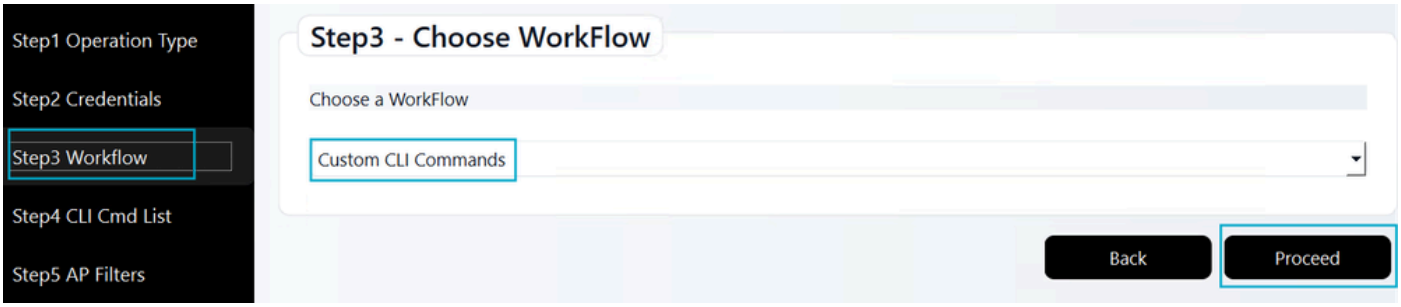
自动模式

启动WLANPoller应用程序并执行以下步骤：

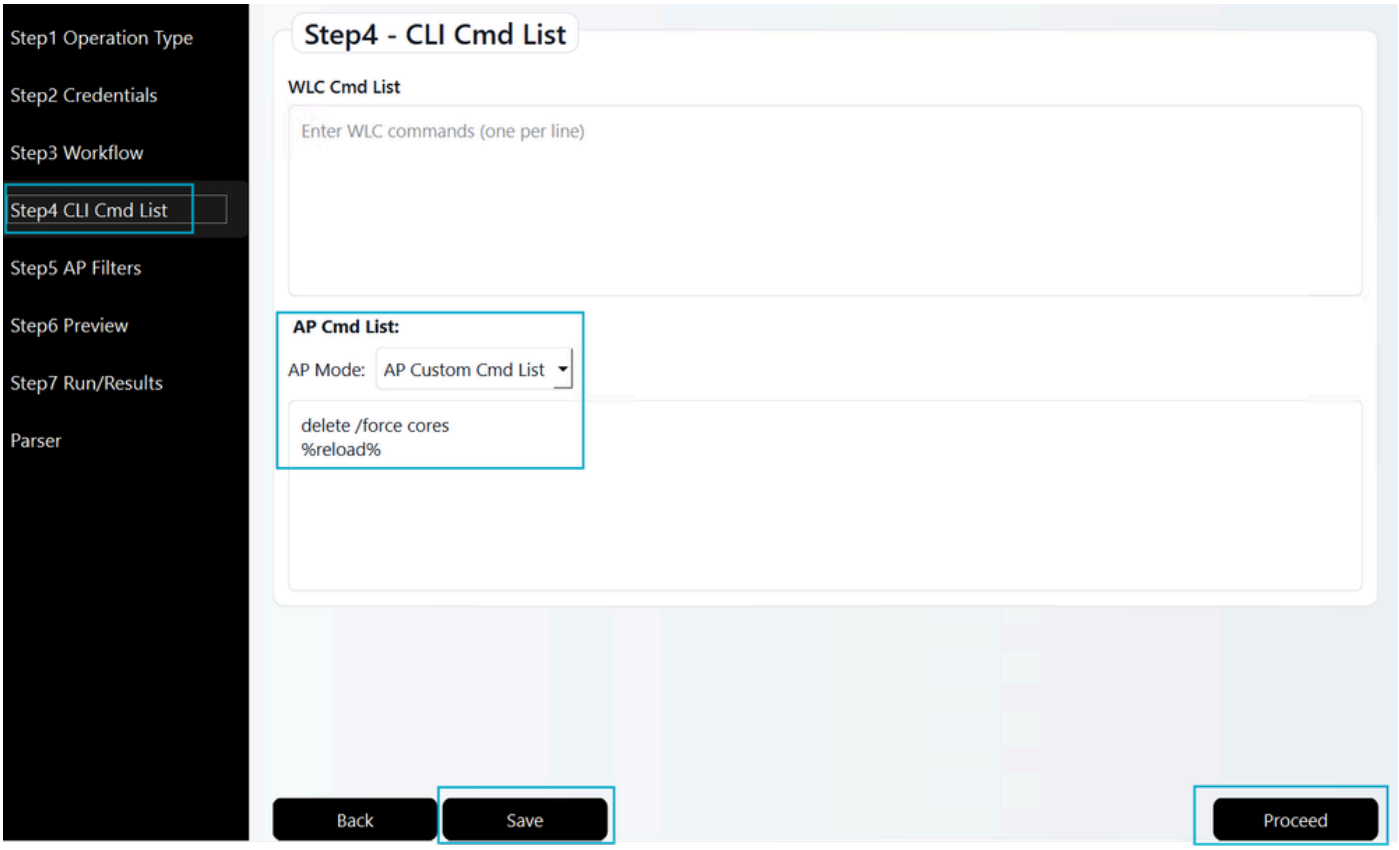
操作类型:选择操作类型WLC和AP。

凭证:输入WLC和接入点凭证。

工作流:将选择更新为自定义CLI命令，然后单击继续。



CLI Cmd列表:输入以下与所示完全相同的接入点命令。单击Save，然后单击Proceed。



接入点过滤器:取消选中所有复选框，除非您的环境需要特定过滤器，然后单击Preview。

预览:查看摘要，然后单击确认并启动WLANoller。

成果：验证所有目标接入点的WLANoller执行是否成功完成。

恢复后，请重复该部分中所述的升级预检查。检查受影响的接入点是否仍显示低空间可用性。如果是，请转向适合您资源的下一个选项；如果从列表中清除它们，则恢复成功，您可以在这些接入点中继续执行代码/APSP。

出厂时重置接入点

将接入点重置为出厂默认设置会临时删除cnssdaemon.log文件。为确保成功安装代码/APSP，请在出厂重置后48小时内继续安装代码/APSP。

有三种方法可在出厂时重置接入点：

- 通过WLC（CLI或GUI）。

- 通过接入点CLI，
- 通过接入点物理重置按钮。



警告：出厂重置会删除所有永久配置（例如，主机名、高可用性设置、标签、LSC等）。重新加入WLC后，您必须重新配置接入点。确保CAPWAP发现（DHCP选项43、DNS等）工作正常，以便接入点可以在重置后成功找到并加入控制器。

通过WLC CLI

```
WLC# clear ap config <APNAME> keep-ip-config
```

通过WLC GUI

导航到配置>无线>接入点。选择所需的接入点，然后导航到高级>设置为出厂默认设置。选择Clear Config except Static IP选项，然后单击Update & Apply to Device。

通过接入点CLI

```
AP# capwap ap erase all
WARNING :" capwap ap erase all" is altered to perform DATA WIPE on COS AP.
The following files will be cleared as part of this process
1) Config ,Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
5) Pktlogs
6) Manually created files
Are you sure you want continue? [confirm] yes
AP# reload
Proceed with reload command (cold)? [confirm] yes
```

通过接入点模式按钮

1.断开接入点与其电源的连接。

2.按住Mode按钮。

3.重新连接电源，同时继续按住按钮。

4.接入点状态LED变为稳定红色后，再按住“模式”按钮10秒。

5.松开按钮。

6.接入点使用出厂默认设置重新启动。

注意：模式按钮按下的时间非常关键。如果按该按钮的时间少于20秒，将不会删除cnssdaemon.log文件。反之，如果保存超过60秒，接入点不会重置为出厂默认设置。请确保按住此按钮30到50秒以成功重置

删除cnssdaemon.log文件(Access Point devshell)

技术支持中心(TAC)可以通过直接从受影响接入点上的devshell清除cnssdaemon.log文件来执行手动恢复。根据影响的规模，有两种方法：

- 少数受影响的接入点:对于少量受影响的接入点，TAC可以使用以下两种方法之一继续操作：
  - 手动devshell访问:通过devshell分别访问每个接入点以手动清除cnssdaemon.log文件。
  - 自动（批量）devshell访问:使用RADKit工具自动清除所有受影响接入点的cnssdaemon.log文件。
- 大量受影响的接入点：TAC应使用RADKit工具，这允许以自动方式批量卸载访问所有受影响的接入点，以高效执行清理过程。

注意：我们建议将RADKit用于接入点devshell恢复过程，以确保整个环境的最大效率和操作一致性。

通过以下链接访问RADKit下载和安装说明：

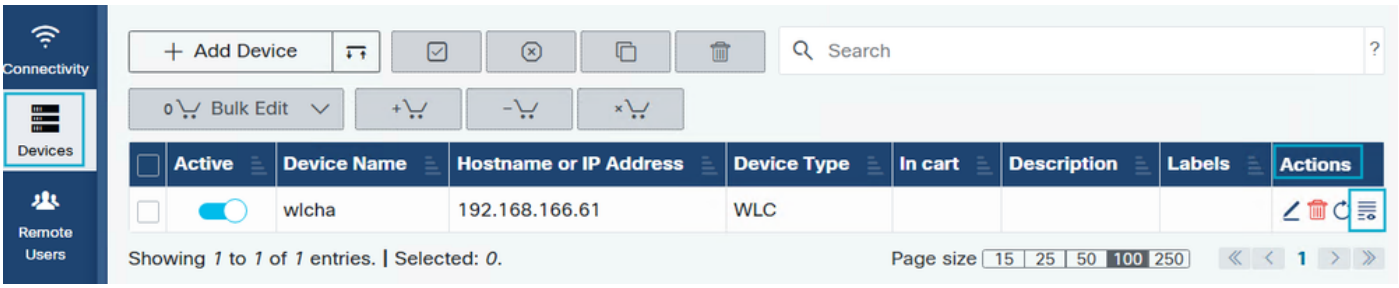
- RADKit下载
- RADKit安装

要通过RADKit删除接入点中的cnssdaemon.log文件，请确保资产中列出了所有接入点。这是仅管理员的任务，无法由TAC远程执行。使用以下步骤将接入点批量添加到RADKit资产中:

1. RADK中的WLCit:确保WLC已添加到RADKit资产中。如果您需要此流程方面的帮助，请通过官方

RADKit文档在此处执行添加设备部分

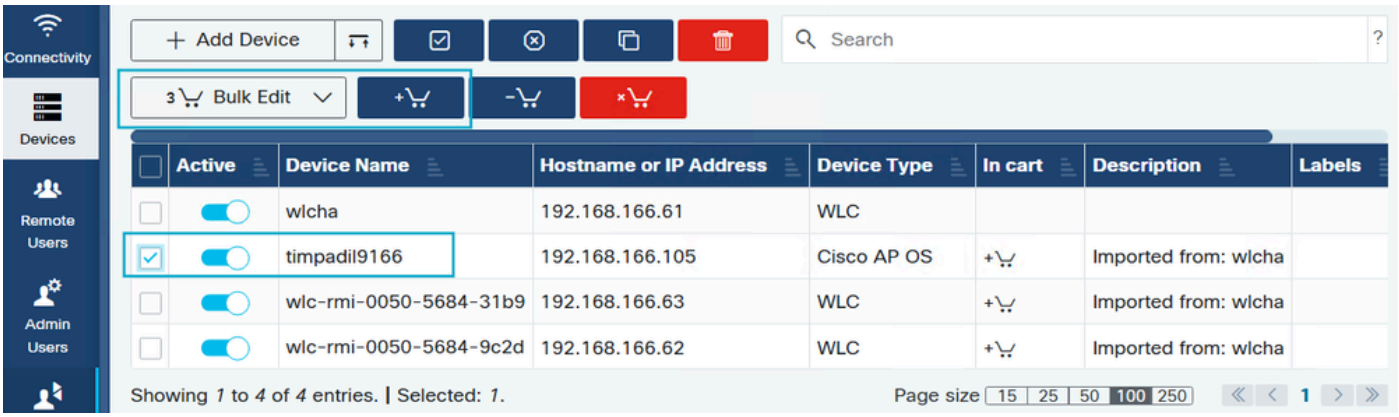
2. WLC库存图标:在设备选项卡下，找到您的WLC，然后单击操作列中的资产图标。



3.批量导入：选择Bulk Import按钮以开始向RADKit添加无线接入点。

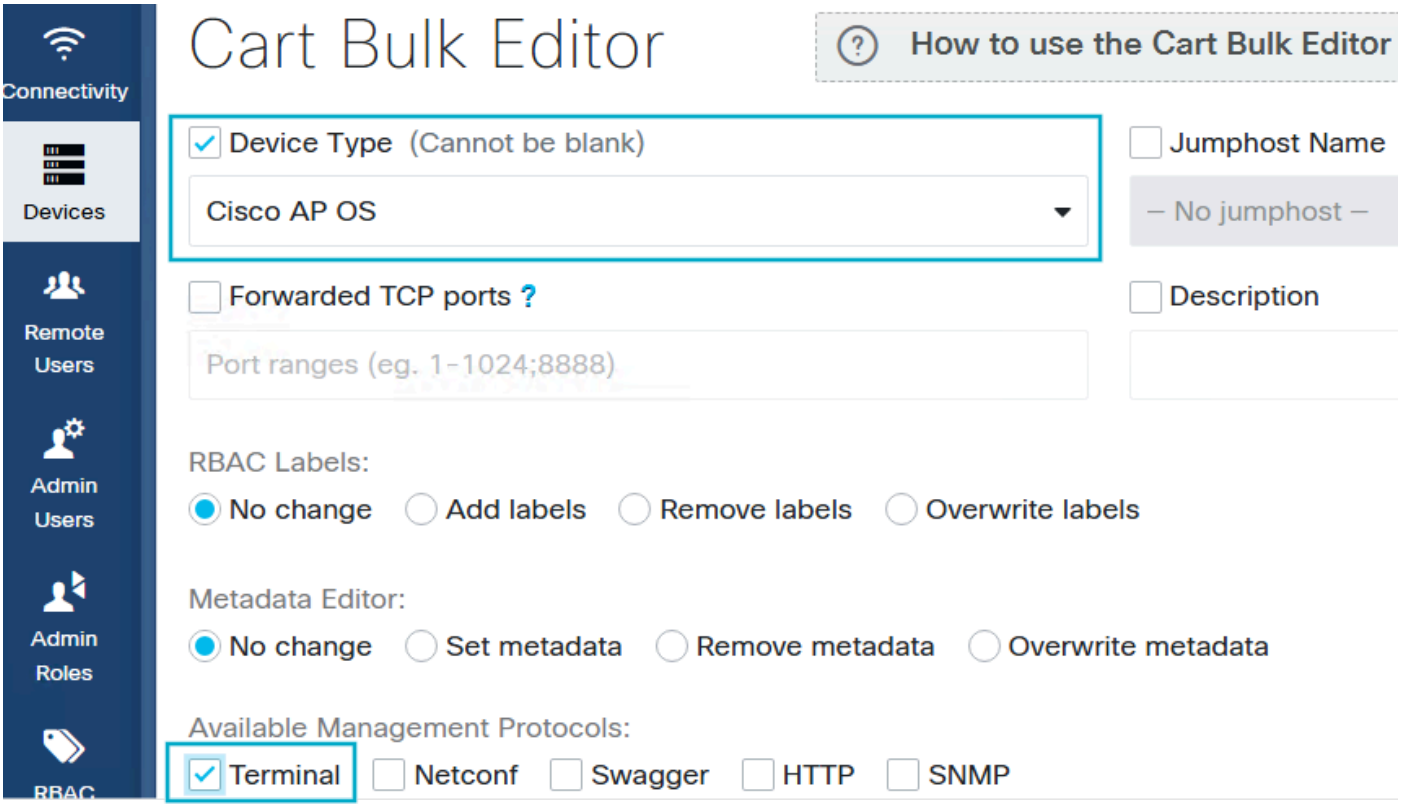


4.批量配置：选中需要cnssdaemon.log文件删除的所有接入点的复选框。单击Add to Cart图标（带加号的购物车），然后选择Bulk Edit按钮。

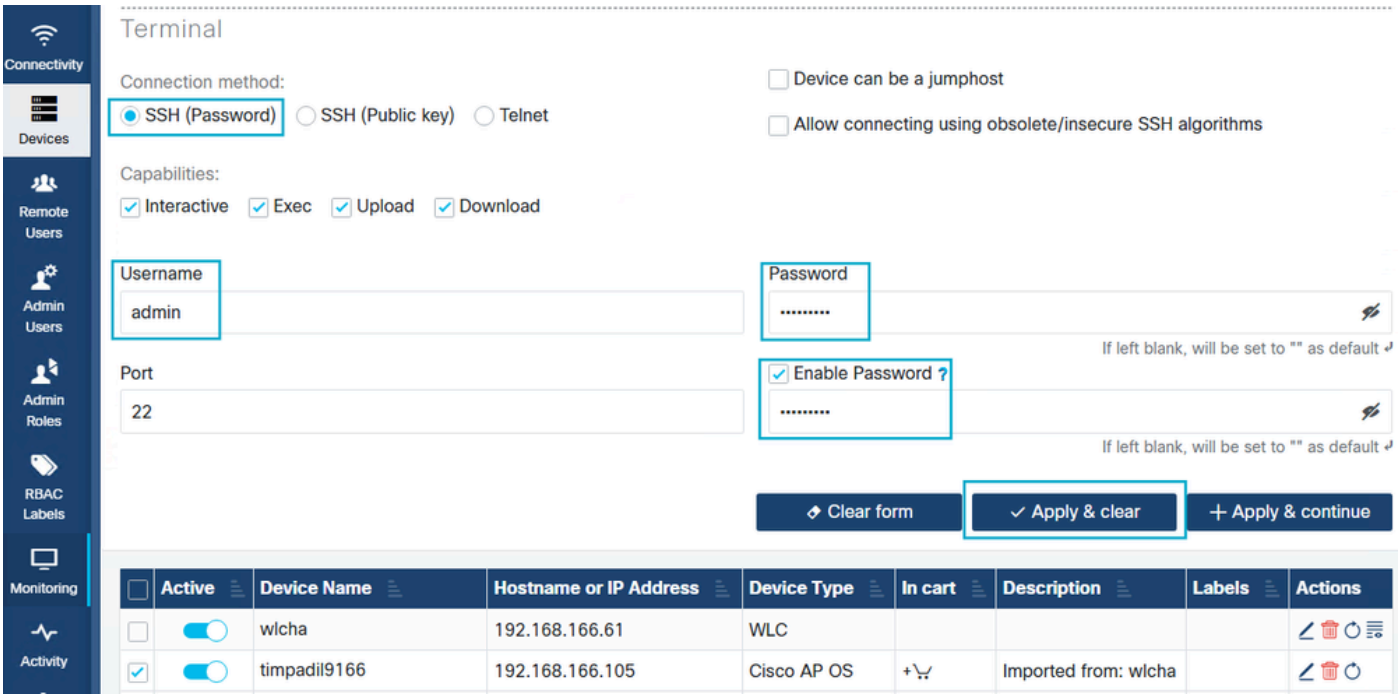


5.启用终端并配置SSH:在Cart Bulk Editor中，选中Device Type并选择Cisco AP OS。启用Terminal切换以允许无线接入点的SSH配置。

注意：如果启用了基于角色的访问控制(RBAC)，请单击Add Labels，并确保Read-only出现在Selected Labels字段中（如果此标签尚不存在，请创建此标签）。 如果禁用RBAC，则不需要此标记步骤。



6.配置SSH凭证:单击SSH（密码）并输入接入点凭据。选中启用密码复选框并输入密码。单击应用并清除以保存这些设置并关闭窗口。确认通过AP加入配置文件在WLC中启用了SSH，并且用户名和密码是最新且正确的。



7. 添加远程用户：通过执行官方RADKit文档中的添加远程用户步骤，添加分配给您的TAC案例的工程师的Cisco CCO ID。

8.目标接入点列表：收集受影响接入点的确切名称(注意：区分大小写)，并将文件上传到您的TAC案例。

使用接入点名称进行设置和文件上传后，Cisco TAC将拥有通过RADKit执行批量删除cnssdaemon.log文件所需的远程访问。

注意：TAC也可以使用RADKit清理工具，即使您有airgap radkit。但是，这仍需要您从可以访问Webex API的计算机上运行radkit客户端，以便让Cisco TAC工程师签署devshell质询。

接入点映像启动分区交换

引导分区交换可以由接入点手动执行，也可以通过WLANoller通过接入点批量自动执行。

手动

通过SSH连接到接入点并运行以下命令：

```
AP# config boot path 2
AP# reload
```

```
Proceed with reload? [confirm] yes
```

自动

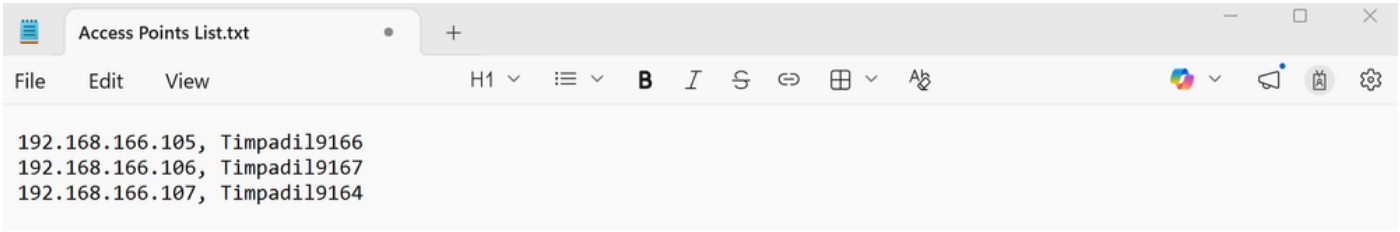
使用WLANoller将引导部分命令批量运行到不同的接入点。

1. 隔离受影响的接入点 — 确保受影响的接入点没有与WLC的连接：
    - 确保在接入点加入配置文件中启用了SSH，且接入点可通过SSH访问（或使用控制台）
    - 确保接入点没有与WLC的连接，但您仍然可以通过SSH访问接入点。这可以通过在网关中使用ACL或将接入点移动到隔离Vlan来实现。如果接入点获得WLC的访问权限，则接入点可以恢复为引导分区1（第1部分），并返回到受影响的状态。

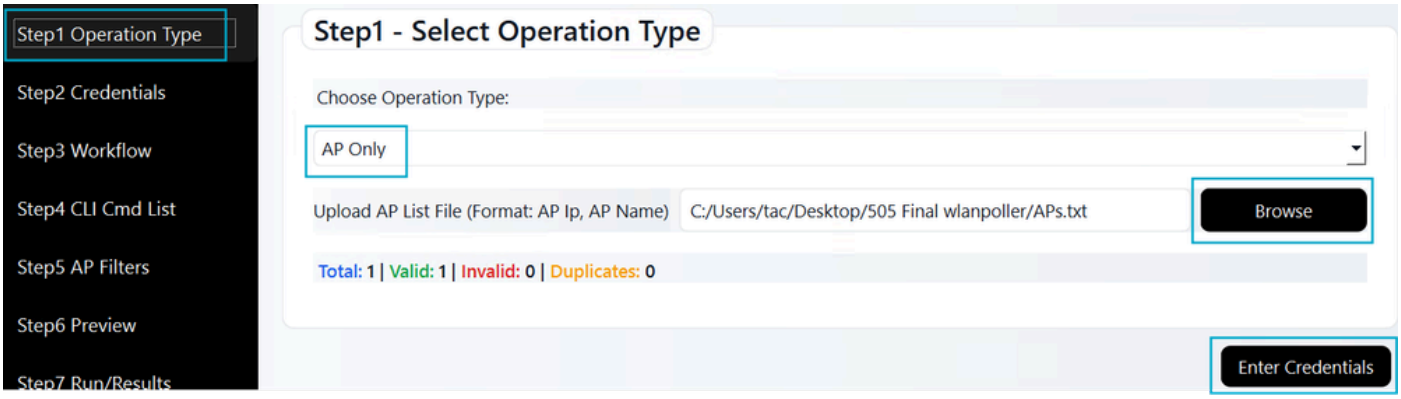
2.配置引导路径2并重新启动受影响的接入点 — 配置WlanPoller，通过命令行指示受影响的接入点将引导部分从1更改为2，然后重新启动。

操作类型:选择选项AP Only，然后在文本编辑器（最好是）中添加接入点IP地址和名称（区分大小写），单击Browse，然后选择具有接入点IP地址和名称的文件。然后点击输入凭证。

接入点列表格式：



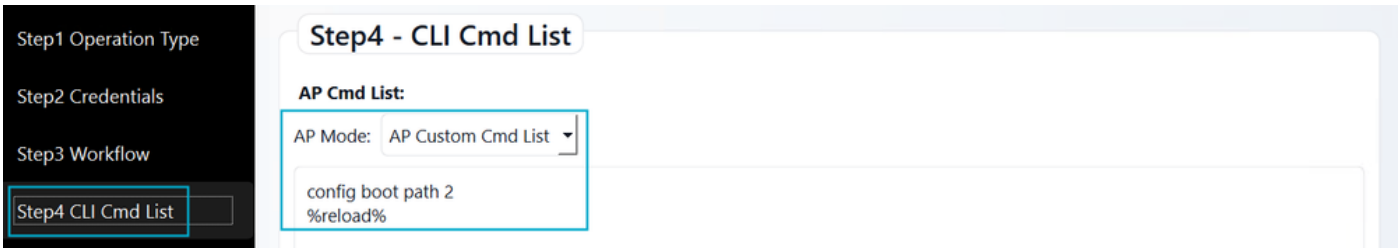
操作类型选择：



凭证:输入接入点凭证，单击Save，然后单击Proceed。

工作流:选择自定义CLI命令，然后单击继续。

CLI Cmd列表:配置命令，使接入点通过part2启动并重新加载。然后单击Save，然后单击Proceed。



预览:预览显示将运行到接入点的2个命令。单击Confirm and Start WlanPoller。

3. Upgrade — 以当前代码在WLC中安装所需的APSP，或者，如果您要升级该代码，请移动到新代码并确保也安装了APSP。

4.重接 — 控制器升级完成后，拆下接入点和WLC之间的通信制动器。接入点将加入WLC并在引导部分1中自动下载新的固定映像。

接入点引导循环

如果您没有首先执行升级预检查，而是执行代码/APSP安装，并且您的接入点最终进入引导循环，则有两个选项可供选择：

1. 按出厂重置无线接入点一节中所述的使用模式按钮重置无线接入点。
2. 获取控制台访问权限并打开TAC案例，以便TAC可以继续恢复接入点。

何时创建TAC案例

如果出现以下任何情况，请打开TAC案例：

- 恢复失败：如果在您的环境中无法实施恢复过程，或者如果恢复过程失败。
- 完整性问题：手动或自动预检查返回“映像完整性检查：糟糕”。
- 存储耗尽：如果在升级/APSP安装后分区“/dev/ubivol/part2”仍显示使用率极高。

常见问题解答

问:此问题是否只适用于完全代码升级，或者是否也影响APSP安装？

A：此问题同时影响这两种情况。如果您的环境满足此Bug的条件，则问题可能会在完全代码升级或APSP安装（包括带有错误修复的APSP）期间发生。 请完成升级预检查部分，以确定您是否需要在执行任何更新或APSP之前执行恢复步骤。

问:我的WLC和接入点在17.9.x（或更早版本）上，我需要升级到17.12.x，必须做什么？

A：您可以执行从17.9.x到17.12.x的直接升级。但是，如果您的接入点型号容易感染此漏洞，请确保在升级后立即安装推荐的APSP。

问:我的WLC和接入点在17.9.x（或更早版本）上，我需要升级到17.15.x或更高版本。

A：有两种可能的方案：

- 直接升级：如果您的环境允许直接升级（请通过目标代码的发行说明进行验证），请继续升级，然后为该目标代码安装APSP。
- 中间升级：如果必须按照升级路径进行升级（例如，17.9.x → 17.12.x → 17.15.x），我们建议在同一天内完成到17.15.x的整个序列。由于cnssdaemon.log文件每天增长5 MB，因此完成升级可快速防止文件达到临界大小。如果无法进行当天升级，则必须在17.12.x阶段安装APSP，然后最终继续到17.15.x并安装其各自的APSP。

问:我已经在17.15.x上。这是否意味着我不受此漏洞的影响？

A：不必要。如果您的接入点以前运行版本17.12.4、17.12.5或17.12.6/6a（在9800-L/40/80/CL上），则有问题的日志文件可能已经生成并保留在存储中。我们强烈建议按照Upgrade Prechecks（升级预检查）部分进行操作，以确保清除所有残留文件。

问:我使用9800-M、9800-H1或9800-H2平台（17.15中首次支持这些平台），是否受到影响？

A：有两种可能的方案：

- 首次加入WLC:如果您的接入点加入9800-M/H1/H2作为其第一个控制器，则不会受到影响。
- 以前加入的WLC:如果这些接入点在迁移到9800-M/H1/H2之前已连接到运行受影响版本(17.12.4/5/6/6a)的其他控制器，则它们可能仍然携带有问题的文件。在这种情况下，请按照升级预检查部分操作。

问:我们有单独的WLC用于实验室测试和交错升级，如何处理？

A：确保您环境中的所有WLC都运行相应的APSP。由于cnssdaemon.log文件每天增长5 MB，因此任何加入运行受影响代码的WLC的接入点（即使是暂时用于测试），都有可能受到此Bug的影响。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。