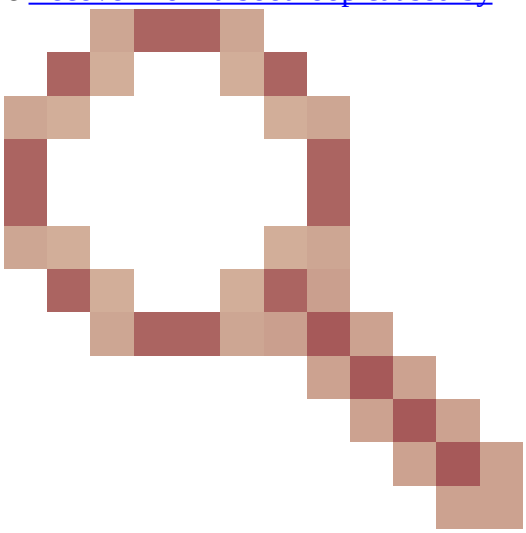
Safely Upgrade Access Points, Avoiding Image Corruption That Causes Boot Loop

Contents

Introduction

Some Cisco access points (APs) may download a corrupt image via CAPWAP from a 9800 series controller. Depending on the AP's software version, the AP may try to boot the corrupt image, resulting in a boot loop. This article explains which AP models and which network paths are susceptible to image corruption and how to upgrade safely.

If your APs are now in a boot loop due to this problem, see the article Recover from a boot loop caused by image corruption on Wave 2 and 11ax Access Points (CSCvx32806) for guidance on recovery steps.



How To Tell Whether an Upgrade Is Susceptible To Image Corruption

Your APs may be susceptible to downloading corrupted software, and then attempting to boot that software, if the following conditions pertain to your deployment:

Not Affected Products

- Wireless LAN Controllers (WLCs): APs downloading from AireOS Wireless LAN Controllers are not affected
- Mobility Express, Embedded Wireless Controller

- APs - Aironet 1800/1540/1100AC series Wave 2 11ac APs and Wave1 11ac Access Points (1700/2700/3700/1570/IW3700) are not affected (even if these APs are registering to 9800 WLCs, they are not impacted)
- Wi-Fi 6E APs introduced since 2023: IW9167, IW9165, C9163

Affected Products

- WLC : APs download from Cisco Catalyst 9800 Series Wireless LAN Controllers may be affected
- APs : The following AP models registering to Cisco Catalyst 9800 Series Wireless LAN Controllers are affected :
    - Aironet Wave2 11ac Access Points (2800/3800/4800/1560/IW6330/ESW6300)
    - Catalyst 9100 Series Wi-Fi6 Access Points (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
    - Catalyst 9100 Series Wi-FI6E Access Points (9136/9162/9164/9166)

Affected Versions: the Boot a Bad Image Syndrome

This problem, where the AP attempts to boot an image that it knows is corrupt, is addressed by the following Cisco bug IDs: CSCvx32806, CSCwc72021, CSCwd90081, which are fixed in the the following releases:

- 8.10.185.0 and above
- 17.3.7 and above
- 17.6.6 and above
- 17.9.3 and above
- 17.11.1 and above

Once the access point is upgraded to software with the above fixes, it may still download a corrupt image; however, it will not attempt to boot that image, but instead will continue to reattempt the download until it succeeds.

Affected Network Paths

The AP image corruption problem has not been seen with a LAN path between the 9800 and the APs - i.e. paths with a full 1500 byte IP MTU, with low latency and very low packet loss are not affected. The problem is more likely to occur over CAPWAP tunnels over a WAN, with the following path characteristics:

- high packet loss
- low CAPWAP MTU (less than 1485 bytes) - the lower the MTU, the higher the risk
    - low CAPWAP MTU may be a symptom of packet loss

How To Tell Whether Your Network Path Is At Risk

- On the 9800, check CAPWAP Path MTU with

  <#root>

```
9800-L#show capwap detailed
Name          APMAC           SourceIP        SrcPort DestIP          DestPort

MTU

   Mode      McastIf
-------------------------------------------------------------------------------------------
Capwap1       D4AD.BDA2.8240 192.168.203.203 5247    192.168.6.100   5248

1485

  multicast Mc1
Capwap2       084F.F983.4A40 192.168.203.203 5247    192.168.6.103   5253

1005

  multicast Mc1
```

    - If a given AP's MTU is fluctuating, that is a strong indicator of risk
- Or **show ap config general | include CAPWAP\ Path\ MTU** (in **show tech-support wireless**)
    - Use Wireless Config Analyzer Express (WCAE) on the 9800's "show tech-support wireless" output to see the APs' MTU under Access Points > Configuration
- On the 9800, use “show ap uptime” and look for APs with a long "AP Up Time" and a short “Association Up Time”
    - If there is no reason for the APs to have a short Association Up Time (i.e. no reconfiguration), then this may indicate an at-risk network path

How To Upgrade Safely From an Unfixed AP Software Version

Note: If your deployment is susceptible to image corruption (i.e. affected AP models, running software without the fix for the Boot a Bad Image Syndrome, with at-risk WAN characteristics), then do not upgrade by simply upgrading the 9800 software, and having the APs rejoin and download the new software - they may be subject to image corruption and entering a boot loop. Instead, use one of these methods:

Upgrade using a WLC local to the APs

If possible, place a staging controller on the APs' LAN - this could be a 9800-CL, or (for Wave 2 / Wi-Fi 6 APs) an AP in EWC mode, and upgrade the APs to the target version. They will then be able safely to join the production controller.

Upgrade via an AireOS controller

If you have an AireOS controller running 8.10.190.0 or above, and if your AP models are supported by AireOS, join the APs to that controller. This will safely upgrade the APs to fixed software, and they will then be able safely to join the production controller.

Upgrade using archive download-sw

Stage the target AP image(s) on a TFTP / SFTP server that is accessible to the upgrading APs. AP image upgrades via TFTP or SFTP are not subject to the image corruption problem. APs can initiate an image download request from the AP CLI or (if the APs are joined to the controller) from the controller CLI.

1. Set up a TFTP or SFTP server in a location accessible to the APs. Note that TFTP performance is gated by latency, so downloads will be slow if the TFTP server is remote from the APs. As SFTP uses TCP, its throughput will be much better if using a high latency path. However, SFTP cannot be triggered from the WLC, as it requires an interactive dialog to enter the username and password.
2. Stage the desired AP image(s) on a TFTP or SFTP server. SeeTable 4 in the Compatibility Matrixfor the 15.3(3)J* AP version that maps to the desired IOS-XE version, then download the appropriate Lightweight AP Software image(s) for affected AP model(s) fromsoftware.cisco.com.
    1. For example, the 17.9.5 AP image for a CW9162 isap1g6b-k9w8-tar.153-3.JPN4.tar.
3. To upgrade via AP CLI: if the AP's CLI is accessible via console or SSH:
    1. Enter the TFTP or SFTP command:
       archive download-sw /no-reload tftp://<*ip-address*>/<*apimage*>
       or
       archive download-sw /no-reload sftp://<*ip-address*>/<*apimage*>
       Username:*USER*
       Password:*XXX*

This will overwrite the corrupted image with the valid image.

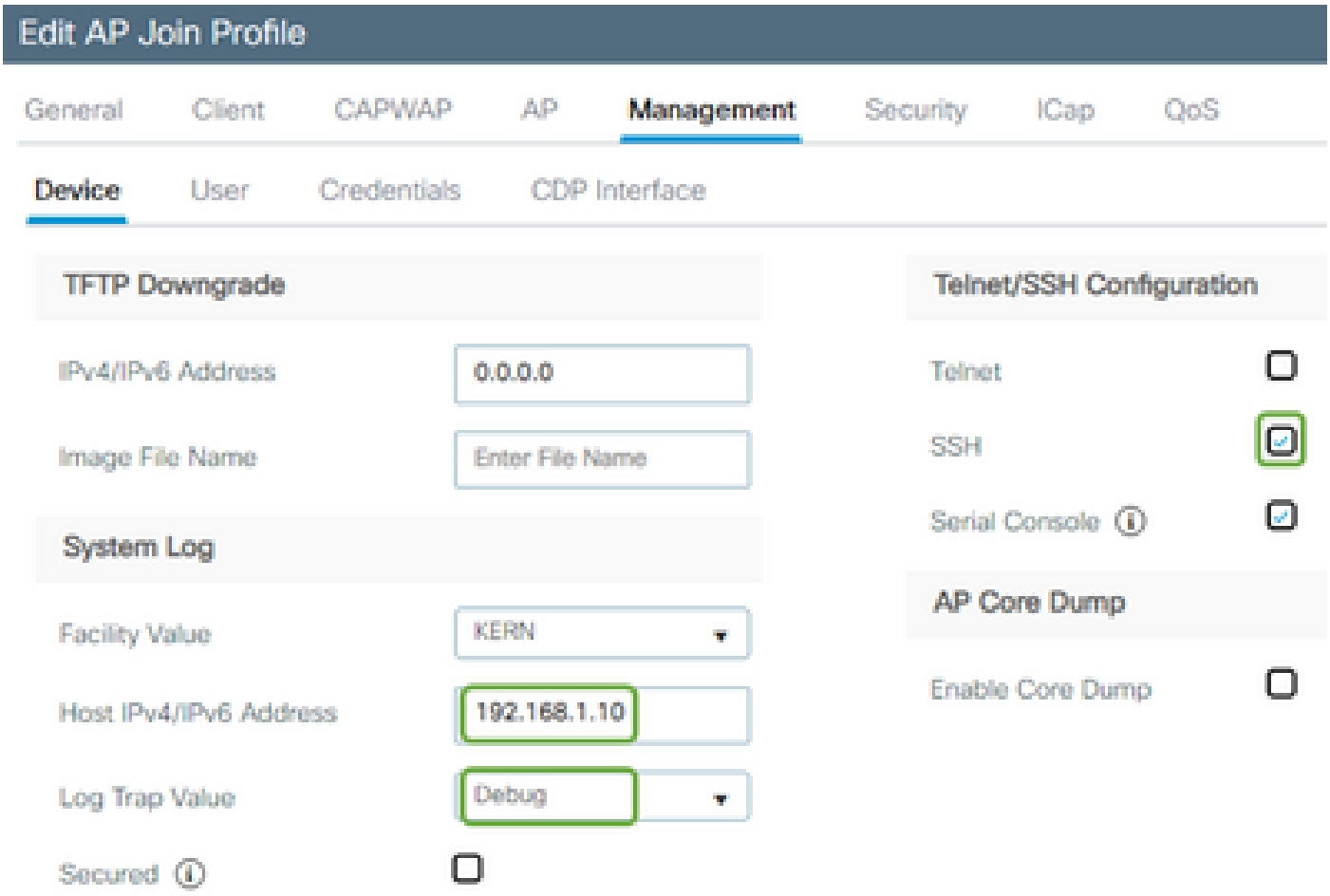
2. Once the image download completes, issue:
   `test capwap restart`
   This will restart the CAPWAP process, so that the AP will recognize the newly installed image.
3. To upgrade a large number of APs via "archive download-sw", rather than entering the command in each AP individually, you may use a scripting method. See **Upgrade APs Via WLAN Poller** below.

4. If the APs are joined to a controller, you can upgrade the APs from controller CLI (TFTP only):
   1. In IOS-XE:**`ap name`*`APNAME`*`tftp-downgrade`*`ip.addr.of.server imagename.tar`*
   2. In AireOS:**`config ap tftp-downgrade`*`ip.addr.of.server imagename.tar`*`APNAME`**
      1. Although CAPWAP downloads from AireOS are not susceptible to image corruption, if you are planning on migrating your APs from AireOS to 9800, you should first download an AP image with the fixes for Alt-boot and the Boot a Bad Image syndrome (8.10.190.0 or above), before joining the APs to the 9800.
   3. Monitor the TFTP or SFTP server logs to verify that each AP has successfully downloaded the image. Once the download completes, each AP will reload, running the newly downloaded image.

Upgrade the APs via Predownload, Monitoring for errors

Load the target image on the 9800, and use AP predownload to push the new image onto the AP, while monitoring for instances of AP image corruption.

Step 1. Verify that SSH is enabled under the AP Join Profile(s) on the C9800 WLC. Set up a syslog server in the network. Configure theIPaddress of the syslog server under AP Join Profile for allthesitesand set the log trap value to Debug. Verify that the syslog server is receiving syslogs from AP.



Step 2. Download the software image to the C9800 WLC to prepare for predownload via CLI:

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

Step 3. Run the AP image pre-download on the Cisco C9800 WLCs:

```
C9800# ap image predownload
```

Note: Depending on the scale and type of deployment this can take anywhere from a few minutes to a few hours. Do not reboot the controller or APs, until you've validated that their images are valid!

Step 4. Once the pre-download for all the APs has completed, check for either of these two log messages on the syslog server:

- ***Image signing verify success.***
- ***Image signature verification failure: -3***

Also, check the output of the command **`show ap image summary`**, checking for any instances of **Failed to Download**. If the counter is nonzero, then find the failed APs via **show ap image | include**

Failed.

Caution: If any APs log ***Image signature verification failure***, or if any APs failed to download, then **DO NOT PROCEED FURTHER WITH THE UPGRADE PROCESS**. If all APs showed the"***Image signing verify success***"message, then all APs have correctly downloaded the image, and you may safely proceed with the 9800 upgrade.

Step 5. If any APs showed verification failure or failed to download, then, to avoid a boot loop, you will need to overwrite the image in the Backup partition of the AP with an archive download of a separate AP image by using the following process.

If the number of failed APs is small, then you can simply SSH to each AP and initiate the following steps.

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Note: "test capwap restart" is needed so that the AP's CAPWAP process will recognize that the image in the backup partition has been updated. This will cause a brief service interruption, as the CAPWAP connection with the 9800 is restarted. If this is an operational concern, this step can be deferred to a maintenance window.

Upgrade APs using WLAN Poller

If the number of APs to upgrade via **archive download-sw** is large, you can use an automated process using the WLAN Poller.

Step 1a. Install the WLAN Poller on a Mac or Windows Machine.

Step 1b. Populate the aplist csv file with the relevant failed APs.

Step 1c. Populate the cmdlist file with the below commands (You can always add more at your discretion):

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Step 1d. Execute the WLAN Poller.

Step 1e. Once its execution has completed, please check every AP's log file to validate successful completion.

Step 2. Immediately activate image on the C9800 WLC and reload.

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

Step 3. Commit image on the C9800 WLC. Skipping this step will cause WLC to rollback to previous software image

```
C9800#install commit
```

Frequently Asked Questions

Q. I ran a predownload some days ago, but have not rebooted my Cisco C9800 WLC and APs yet. I don't have syslogs to verify whether the image is corrupted. How do I verify whether the image is corrupted?

A. Check show logging on the APs/syslog. If you see no success or failure messages in the show logging output, you can use the "show flash syslogs" command to file the syslog output from when you performed the predownload. If you see the "***Image signing verify success***" message, then you know that this AP has downloaded the image successfully.

Q: I have a centralized deployment with APs in Local mode. Do I still need to execute the steps listed in the Workaround/Solutions section?

A: This issue has only been reported when upgrading APs over a WAN connection. APs in Local mode and over local networks are highly unlikely to run into this issue, so it is not required to follow this procedure for upgrades, if you are confident that there is very little packet loss between the controller and the APs.

Q: I have new out-of-box APs. How can I deploy them without encountering this issue?

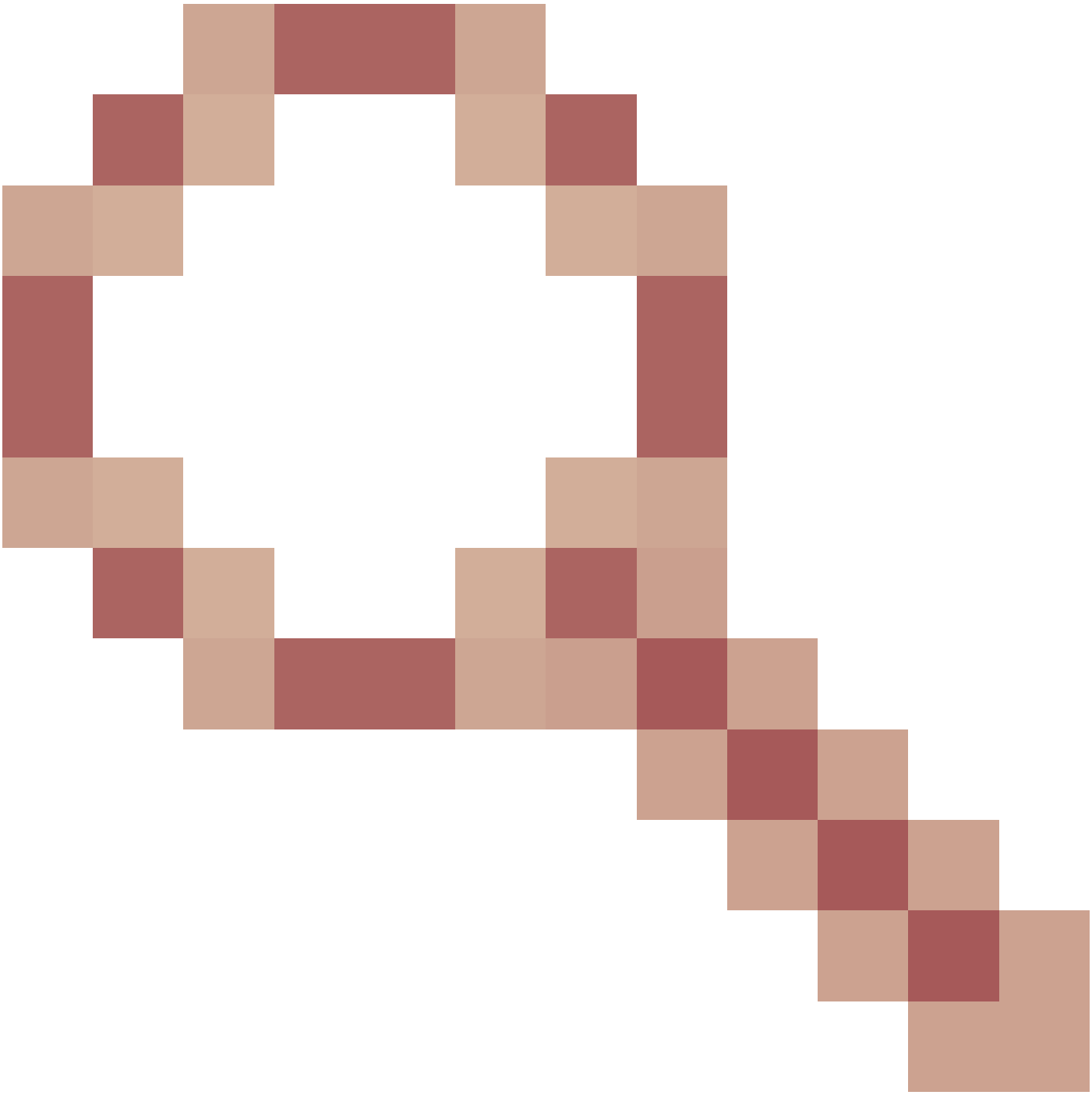
A: New, out-of-box APs downloading code over WAN will also be susceptible to this issue, unless they were manufactured after December 2023.

Q: What is Cisco doing in the long run to address this problem with CAPWAP image downloads from the 9800 getting corrupted?

A: Once the AP is already running 17.11 or above, it can use the Out-of-Band Image Download feature to pull the image from the controller using HTTPS. TCP transmits data reliably, using a sliding window – so it’s also a lot faster over a WAN, than CAPWAP (or TFTP)

Q. I have APs that are now in a boot loop. How can I recover them?

A: See the article Recover from a boot loop caused by image corruption on Wave 2 and 11ax Access Points (CSCvx32806



).