Upgrade and Downgrade of Catalyst 9800 Controllers: Tips and Tricks

Contents

Introduction

This document describes things to watch out for when upgrading or downgrading a Catalyst 9800 Wireless LAN Controller (WLC).

Before You Proceed

This document does not aim at replacing the release notes which must always be the go-to document when upgrading. The aim is to facilitate the upgrade through several releases by highlighting the most impactful changes between releases.

This document does not replace reading the release notes of your target software release. Back up your configuration and take all necessary precautions before proceeding with an upgrade.

By default, the HTTP server of the 9800 is not statically mapped to a specific certificate/trustpoint which can lead to changes after the upgrade. Set the HTTP server to a static trustpoint (preferably to a certificate you issued for the purpose, or to the MIC certificate otherwise) in the configuration before upgrading.

The Special Case of Engineering Special Versions

Engineering special builds do not support ISSU upgrades from them. This document only focuses on public releases published to Cisco.com, therefore, if you are on an engineering special build, refer to the release notes you received along with them in order to receive support for all your upgrade questions.

Upgrade

You can directly read the notes under the destination software version you are aiming at. Tips that are applicable through several releases are repeated each time for your convenience. Do not upgrade through more than three releases at once. For example, upgrading from 16.12.1 to 17.3.2 is covered in this document, however, it does not cover upgrades from 16.12 to 17.4. In such a scenario, navigate through 17.3 and check the notes under the 17.3 section, perform the upgrade, then look at the 17.4 section and prepare the second upgrade. In conclusion, the tips listed are not repeated anymore after three major releases, even if still valid, as the document assumes you proceed through intermediate major releases.

Gibraltar

16.12.2

- From Cisco IOS® XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses the default policy tag, it then goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, it can lead

to a controller crash.

- Do not deploy OVA files directly to VMware ESXi 6.5. It is recommended that you use an OVF tool to deploy the OVA files.

16.12.3

- 16.12.3 is the first release to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses the default policy tag, it then goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, it can lead to a controller crash.

- Do not deploy OVA files directly to VMware ESXi 6.5. It is recommended that you use an OVF tool in order to deploy the OVA files.

16.12.4

- 16.12.3 and 17.2.1 are the first releases to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it then goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, it can lead to a controller crash.

- Do not deploy OVA files directly to VMware ESXi 6.5. It is recommended that you use an OVF tool in order to deploy the OVA files.

16.12.5, 16.12.6a, and 16.12.7

Identical to the 16.12.4 release.

Amsterdam

17.1.1

- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- From this release, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.

17.2.1

- 16.12.3 and 17.2.1 are the first releases to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it can go down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.

17.3.1

- 16.12.3 and 17.2.1 are the first releases in order to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- From 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.
- If you have configured FIPS mode, ensure that you remove the `security wpa wpa1 cipher tkip` configuration

from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to accomplish so sets the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you must reconfigure WLAN with AES.

- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments. It is only possible to increase the disk space size through a reinstall with a 17.3 image.
- Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- For local MAC address authentication (of clients or APs), only the format aaaabbbbcccc (without separator) is supported as of 17.3.1. This means authentication fails if you add a MAC address with separators in the web UI or CLI.
- From this release onwards, APs reload after 4 hours if they cannot join a WLC, cannot ping their gateway, and ARP their gateway (all three must fail for the AP to reboot). This is an enhancement (Cisco bug ID CSCvt89970) to the previous ICMP-only gateway verification from earlier releases.
- From 17.3.1 onwards, the new way to configure country codes for access points is the Wireless country <1 country code> command that you can repeat several times with different country codes. This allows to increase in the maximum amount of country code way over 20. The commands ap country are still present and still work, however, consider changing them to the Wireless country commands as the ap country commands are deprecated in a future version.

17.3.2

- 16.12.3 and 17.2.1 are the first releases to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- From 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.
- If you have configured FIPS mode, ensure that you remove the security wpa wpa1 cipher tkip configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to accomplish so sets the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you must reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments. It is only possible to increase the disk space size through a reinstall with a 17.3 image.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- For local MAC address authentication (of clients or APs), only the format aaaabbbbcccc (without separator) is supported as of 17.3.1. This means authentication fails if you add a MAC address with separators in the web UI or CLI.
- From 17.3.1 onwards, APs reload after 4 hours if they cannot join a WLC, cannot ping their gateway, and ARP their gateway (all three must fail for the AP to reboot). This is an enhancement (Cisco bug ID CSCvt89970) to the earlier ICMP-only gateway verification from the earlier releases.
- From 17.3.1 onwards, the new way to configure country codes for access points is the Wireless country <1 country code> command that you can repeat several times with different country codes. This allows to

increase in the maximum amount of country codes way over 20. The commands ap country are still present and running, however, consider changing them to the Wireless country commands as the ap country commands are deprecated in a future version.

17.3.3

- 16.12.3 and 17.2.1 are the first releases to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses the default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.
- If you have configured FIPS mode, ensure that you remove the security wpa wpa1 cipher tkip configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to accomplish so sets the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you must reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments. It is only possible to increase the disk space size through a reinstall with a 17.3 image.
- Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- For local MAC address authentication (of clients or APs), only the format aaaabbbbcccc (without separator) is supported as of 17.3.1. This means authentication fails if you add a MAC address with separators in the web UI or CLI.
- From 17.3.1 onwards, APs reload after 4 hours if they cannot join a WLC, cannot ping their gateway, and ARP their gateway (all three must fail for the AP to reboot). This is an enhancement (Cisco bug ID CSCvt89970) of the earlier ICMP-only gateway verification from the earlier releases.
- From 17.3.1 onwards, the new way to configure country codes for access points is the Wireless country <1 country code> command that you can repeat several times with different country codes. This allows to increase in the maximum amount of country code way over 20. The commands ap country are still present and working, however, consider changing them to the Wireless country commands as the ap country commands are deprecated in a future version.
- WLC can crash if your APs have hostnames longer than 32 characters (Cisco bug ID CSCvy11981).

17.3.4

- 16.12.3 and 17.2.1 are the first releases in order to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports larger files to be uploaded through the web UI.
- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under

the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.

- From 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.
- If you have configured FIPS mode, ensure that you remove the security wpa wpa1 cipher tkip configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to accomplish so sets the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you must reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments. It is only possible to increase the disk space size through a reinstall with a 17.3 image.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- For local MAC address authentication (of clients or APs), only the format aaaabbbbcccc (without separator) is supported as of 17.3.1. This means authentication fails if you add a MAC address with separators in the web UI or CLI.
- From 17.3.1 onwards, APsl reloads after 4 hours if they cannot join a WLC, cannot ping their gateway, and ARP their gateway (all three must fail for the AP to reboot). This is an enhancement (Cisco bug ID CSCvt89970) to the previous ICMP-only gateway verification from the earlier releases.
- 17.3.1 onwards, the new way to configure country codes for access points is the Wireless country <1 country code> command that you can repeat several times with different country codes. This allows to increase in the maximum amount of country code way over 20. The commands ap country are still present and working, however, consider changing them to the Wireless country commands as the ap country commands are planned to be deprecated in a future version.
- When upgrading to 17.3.4 and later, it is advised to have the 16.12.5r bootloader/rommon installed on controllers where it is applicable (the 9800-80). (The 9800-40 does not have a rommon 16.12.5r at this time and does not need a rommon upgrade.)
- Controller upgrade, from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU, can fail if the snmp-server enable traps hsrpcommand is configured. Ensure that you remove the snmp-server enable traps hsrp command from the configuration before starting an ISSU upgrade because the snmp-server enable traps hsrp command is removed from Cisco IOS XE Bengaluru 17.4.x.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the ip http active-session-modules none command is enabled, you are unable to access the controller GUI using HTTPS. In order to access the GUI using HTTPS, run these commands:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

17.3.5

- Due to Cisco bug ID CSCwb13784, if your path MTU is lower than 1500 bytes, APs possibly are not able to join. Download the SMU patch available for 17.3.5 in order to fix this problem.
- 16.12.3 and 17.2.1 are the first releases in order to enforce the support of only the SFPs listed as supported in the documentation. SFPs not listed cause a port-down situation. Verify the list of supported SFPs and ensure your SFPs are compatible in order to avoid the data ports being down after the upgrade.
- The upgrade file for this release can be too big for HTTP upload (when doing a web UI upgrade) if you are in the 16.12.1 release. Use another transfer method or proceed through 16.12.2 which supports

larger files to be uploaded through the web UI.

- From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses a default policy tag, it goes down due to the default mapping change. In order to restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- 17.1 onwards, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway in order to check for connectivity. You must ensure traffic filtering between the APs and the default gateway (like ACLs) to allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs reload at 4-hour intervals.
- If you have configured FIPS mode, ensure that you remove the security wpa wpa1 cipher tkip configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to accomplish so sets the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you must reconfigure WLAN with AES.
- Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments. It is only possible to increase the disk space size through a reinstall with a 17.3 image.
- Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- For local MAC address authentication (of clients or APs), only the format aaaabbbbcccc (without separator) is supported as of 17.3.1. This means authentication fails if you add a MAC address with separators in the web UI or CLI.
- 17.3.1 onwards, APsl reloads after 4 hours if they cannot join a WLC, cannot ping their gateway, and ARP their gateway (all three must fail for the AP to reboot). This is an enhancement (Cisco bug ID CSCvt89970) to the earlier ICMP-only gateway verification from the earlier releases.
- 17.3.1 onwards, the new way to configure country codes for access points is the Wireless country <1 country code> command that you can repeat several times with different country codes. This allows to increase in the maximum amount of country code way over 20. The commands ap country are still present and working, however, consider changing them to the Wireless country commands as the ap country commands are planned to be deprecated in a future version.
- When upgrading to 17.3.4 and later, it is advised to have the 16.12.5r bootloader/rommon installed on controllers where it is applicable (the 9800-80). (The 9800-40 does not have a rommon 16.12.5r at this time and does not need a rommon upgrade.)
- Controller upgrade, from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU, can fail if the snmp-server enable traps hsrpcommand is configured. Ensure that you remove the snmp-server enable traps hsrp command from the configuration before starting an ISSU upgrade because the snmp-server enable traps hsrp command is removed from Cisco IOS XE Bengaluru 17.4.x.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the ip http active-session-modules none command is enabled, you are unable to access the controller GUI using HTTPS. In order to access the GUI using HTTPS, run these commands:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

Bengaluru

17.4.1

- 17.4.1 onwards, Wave 1 Cisco IOS-based APs are not supported anymore (1700,2700,3700,1570) except IW3700.
- Your WLANs can be shut down after the upgrade if they are non-WPA (guest, open, or CWA SSIDs) and have adaptive FT configured. The solution is to remove the adaptive FT configuration before the

upgrade (Cisco bug ID CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID, so there is no loss of anything by removing it.
- WLC can crash if your APs have hostnames longer than 32 characters (Cisco bug ID CSCvy11981).

17.5.1

- 17.4.1 onwards, Wave 1 Cisco IOS-based APs are not supported anymore (1700,2700,3700,1570) except IW3700.
- Cisco IOS XE Bengaluru Release 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue with the upgrade version that uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from the Cisco DNA Centre.
- Your WLANs can be shut down after the upgrade if they are non-WPA (guest, open, or CWA SSIDs) and have adaptive FT configured. The solution is to remove the adaptive FT configuration before the upgrade (Cisco bug ID CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID, so there is no loss of anything by removing it.
- WLC can crash if your APs have hostnames longer than 32 characters (Cisco bug ID CSCvy11981).
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the ip http active-session-modules none command is enabled, you are unable to access the GUI using HTTPS. In order to access the GUI using HTTPS, run these commands:
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
- If you encounter the "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" error from the GUI after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate.
- The procedure to generate a new self-signed trustpoint is as shown:

```
configure terminal
no crypto pki trustpoint <trustpoint_name>
no ip http server
no ip http secure-server
ip http server
ip http secure-server
ip http authentication <local/aaa>
! use local or aaa as applicable.
```

17.6.1

- 17.4.1 onwards, Wave 1 Cisco IOS-based APs are not supported anymore (1700,2700,3700,1570) except IW3700.
- Cisco IOS XE Bengaluru Release 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue with the upgrade version that uses the newly named receivers, and these are not recognized in the downgrade. The new

configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from the Cisco DNA Centre.

- Your WLANs can be shut down after the upgrade if they are non-WPA (guest, open, or CWA SSIDs) and have adaptive FT configured. The solution is to remove the adaptive FT configuration before the upgrade (Cisco bug ID CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID, so there is no loss of anything by removing it.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.
- An AP who joined a 17.6.1 or later WLC is unable to join an AireOS WLC anymore unless it runs 8.10.162 and later, or 8.5.176.2 and later 8.5 code.
- Upgrading to 17.6,1 and later, it is advised to have the 16.12.5r bootloader/rommon installed on controllers where it is applicable (the 9800-80). (The 9800-40 does not have a rommon 16.12.5r at this time and does not need a rommon upgrade.)
- Controller upgrade, from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU, can fail if the snmp-server enable traps hsrpcommand is configured. Ensure that you remove the snmp-server enable traps hsrp command from the configuration before starting an ISSU upgrade because the snmp-server enable traps hsrp command is removed from Cisco IOS XE Bengaluru 17.4.x.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the ip http active-session-modules none command is enabled, HTTPS access to the controller GUI does not work. In order to access the GUI using HTTPS, run these commands:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- If you encounter the "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" error from the GUI after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate.
- The procedure to generate a new self-signed trustpoint is as shown:

```
configure terminal
no crypto pki trustpoint <trustpoint_name>
no ip http server
no ip http securffwe-server
ip http server
ip http secure-server
ip http authentication <local/aaa>
! use local or aaa as applicable.
```

17.6.2

- 17.4.1 onwards, Wave 1 Cisco IOS-based APs are not supported anymore (1700,2700,3700,1570) except IW3700.
- Cisco IOS XE Bengaluru Release 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue with the upgrade version that uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from the Cisco DNA Centre.
- Your WLANs can be shut down after the upgrade if they are non-WPA (guest, open, or CWA SSIDs) and have adaptive FT configured. The solution is to remove the adaptive FT configuration before the upgrade (Cisco bug ID CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID,

so there is no loss of anything by removing it.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.
- An AP who joined a 17.6.1 or later WLC is unable to join an AireOS WLC anymore unless it runs 8.10.162 and later, or 8.5.176.2 and later 8.5 code.
- Upgrading to 17.6,1 and later, it is advised to have the 16.12.5r bootloader/rommon installed on controllers where it is applicable (the 9800-80). (The 9800-40 does not have a rommong 16.12.5r at this time and does not need a rommon upgrade.)
- Controller upgrade, from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU, can fail if the snmp-server enable traps hsrpcommand is configured. Ensure that you remove the snmp-server enable traps hsrp command from the configuration before starting an ISSU upgrade because the snmp-server enable traps hsrp command is removed from Cisco IOS XE Bengaluru 17.4.x.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the ip http active-session-modules none command is enabled, HTTPS controller GUI access does not work. In order to access the GUI using HTTPS, run these commands:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, a controller crash can occur.

- If you encounter the "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" error from the GUI after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate.

- The procedure to generate a new self-signed trustpoint is as shown:

```
configure terminal
no crypto pki trustpoint <trustpoint_name>
no ip http server
no ip http secure-server
ip http server
ip http secure-server
ip http authentication <local/aaa>
! use local or aaa as applicable.
```

Cupertino

This section assumes you are starting from 17.6.1 or later and upgrading to a Cupertino release. If you are upgrading directly from an earlier release (which can be supported, check the release notes in order to be certain), read the 17.3 and 17.6 section caveats.

17.7.1

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, a controller crash can occur.
- 17.7.1 requires AP country codes to be configured in AP joins profiles.
- Due to Cisco bug ID CSCvu22886, if you have 9130 or 9124 APs, you must go through 17.3.5a when upgrading to 17.7.1 or later from a release earlier than 17.3.4.
- From Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller,

ensure that you complete Resource Utilization Measurement (RUM) reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the Cisco Smart Software Manager (CSSM). Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.

17.8.1

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, a controller crash can occur.
- 17.7.1 requires AP country codes to be configured in AP joins profiles.
- Due to Cisco bug ID CSCvu22886, if you have 9130 or 9124 APs, you must go through 17.3.5a when upgrading to 17.7.1 or later from a release earlier than 17.3.4.
- Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete RUM reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the CSSM. Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.

17.9.x

- APs running Cisco IOS-XE 17.9.3 can encounter issues when attempting to upgrade their software due to insufficient space in the /tmp directory. When the /tmp space on the AP becomes full, it prevents the download of the new AP image. In such instances, it is recommended that you reboot the AP.

- 11AC Wave 2 APs can get into a boot loop when upgrading software over a WAN link. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- 17.9.3 and later releases bring back support for Cisco IOS-based access points (x700 series and 1570). They were not supported between 17.4 and 17.9.2. Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to Cisco IOS XE Bengaluru 17.6.x or Cisco IOS XE Cupertino 17.9.x and later using ISSU can fail if the domain command is configured. Ensure that you run the no domain command before starting an ISSU upgrade because the domain command has been removed from Cisco IOS XE Bengaluru 17.6.x.
- Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete RUM reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the CSSM. Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- 17.3 onwards, the 9800-CL requires 16 GB of disk space in order to function properly. You cannot increase the size dynamically if your WLC instance started with an 8 GB OVA (from before 17.3). The only way is to create a new WLC from an OVA dated later than 17.3.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.
- The Cisco Catalyst 9800-L Wireless Controller can fail to respond to the break signals received on its

console port during boot time, preventing users from getting to the rommon. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) rommon for the Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the rommon, see the Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- If this error message is displayed after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

  Use these commands in the order specified in order to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# no crypto pki trustpoint trustpoint_name
  3. device(config)# no ip http server
  4. device(config)# no ip http secure-server
  5. device(config)# ip http server
  6. device(config)# ip http secure-server
  7. device(config)# ip http authentication local/aaa

- Verify that your mobility MAC address is set with the wireless mobility mac-address command.
- These protocols are now supported through the service port in 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP
  - HTTPS
  - LDAP

    - Licensing for Smart Licensing feature to communicate with CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (including CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- The AP image for 17.9 is bigger than the AP flash originally allowed. If you see the AP complaining about not having enough space when downloading the 17.9 image, it is probably because you did not respect the upgrade path through 17.3.5 as advised in the release notes or that your AP is running an older AireOS image. Either transiting through a 17.3.5 or a later WLC or upgrading the AireOS image to the latest resizes the AP flash in order to allow to download the 17.9 image.

Dublin

17.10.1

- The Cisco Centralized Key Management (CCKM) feature is being deprecated from Cisco IOS XE Dublin 17.10.x.
- Smart Call Home is getting deprecated in favor of Smart Transport for licensing.

- APs running Cisco IOS-XE 17.9.3 or later can encounter issues when attempting to upgrade their software due to insufficient space in the /tmp directory. When the /tmp space on the AP becomes full, it prevents the download of the new AP image. In such instances, it is recommended that you reboot the AP.

  Wave 2 APs can get into a boot loop when upgrading software over a WAN link. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- From Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete RUM reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the CSSM. Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- 17.3 onwards, the 9800-CL requires 16 GB of disk space in order to function properly. You cannot increase the size dynamically if your WLC instance started with an 8 GB OVA (from before 17.3). The only way is to create a new WLC from an OVA dated later than 17.3.

- The Cisco Catalyst 9800-L Wireless Controller can fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the rommon. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. The problem is fixed in the 16.12(3r) rommon for the Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the rommon, see the **Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers** section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- If this error message is displayed after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use these commands in the order specified in order to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# no crypto pki trustpoint trustpoint_name
  3. device(config)# no ip http server
  4. device(config)# no ip http secure-server
  5. device(config)# ip http server
  6. device(config)# ip http secure-server
  7. device(config)# ip http authentication local/aaa

- Verify that your mobility MAC address is set with the wireless mobility mac-address command.
- These protocols are now supported through the service port in 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP
  - HTTPS

    - LDAP
    - Licensing for Smart Licensing feature to communicate with CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (including CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- The AP image for 17.9 is larger than the AP flash originally allowed. If you see the AP complaining about not having enough space when downloading the 17.9 image, it is probably because you did not respect the upgrade path through 17.3.5 as advised in the release notes, or that your AP is running an older AireOS image. Either transiting through a 17.3.5 and later WLC or upgrading the AireOS image to the latest resizes the AP flash in order to allow to download of the 17.9 image.

17.11.1

- The CCKM feature is being deprecated from Cisco IOS XE Dublin 17.10.x.
- Smart Call Home is getting deprecated in favor of Smart Transport for licensing
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.

- APs running Cisco IOS-XE 17.9.3 or later can encounter issues when attempting to upgrade their software due to insufficient space in the /tmp directory. When the /tmp space on the AP becomes full, it prevents the download of the new AP image. In such instances, it is recommended that you reboot the AP.

  Wave 2 APs can get into a boot loop when upgrading software over a WAN link. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete RUM reporting and that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the CSSM. Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- 17.3 onwards, the 9800-CL requires 16 GB of disk space in order to function properly. You cannot increase the size dynamically if your WLC instance started with an 8 GB OVA (from before 17.3). The only way is to create a new WLC from an OVA dated later than 17.3.
- The Cisco Catalyst 9800-L Wireless Controller can fail to respond to the break signals received on its

console port during boot time, preventing users from getting to the rommon. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. It can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) rommon for the Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the rommon, see the **Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers** section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- If this error message is displayed after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

  Use these commands in the order specified in order to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# no crypto pki trustpoint trustpoint_name
  3. device(config)# no ip http server
  4. device(config)# no ip http secure-server
  5. device(config)# ip http server
  6. device(config)# ip http secure-server
  7. device(config)# ip http authentication local/aaa

- Verify that your mobility MAC address is set with the wireless mobility mac-address command.
- These protocols are now supported through the service port in 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP
  - HTTPS

    - LDAP
    - Licensing for Smart Licensing feature to communicate with CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (including CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- The AP image for 17.9 is larger than the AP flash originally allowed. If you see the AP complaining about not having enough space when downloading the 17.9 image, it is probably because you did not respect the upgrade path through 17.3.5 as advised in the release notes, or that your AP is running an older AireOS image. Either transiting through a 17.3.5 and later WLC or upgrading the AireOS image to the latest resizes the AP flash in order to allow to download of the 17.9 image.

17.12.1

- The CCKM feature is being deprecated from Cisco IOS XE Dublin 17.10.x.
- Smart Call Home is getting deprecated in favor of Smart Transport for licensing.
- When you upgrade the GUI from one release to another, it is recommended that you clear the browser cache for all GUI pages to reload correctly.

- APs running Cisco IOS-XE 17.9.3 or later can encounter issues when attempting to upgrade their software due to insufficient space in the /tmp directory. When the /tmp space on the AP becomes full, it prevents the download of the new AP image. In such instances, it is recommended that you reboot the AP.

  Wave 2 APs can get into a boot loop when upgrading software over a WAN link. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- 17.12.1 and later releases bring back support for Cisco IOS-based access points (x700 series and 1570). They were not supported between 17.4 and 17.9.2. Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Cisco IOS XE Cupertino 17.7.1 onwards, for the Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete RUM reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the CSSM. Failure to accomplish this leads to a maximum of 50 APs being able to join a 9800-CL until a license report is ACKed.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.

- 17.3 onwards, the 9800-CL requires 16 GB of disk space in order to function properly. You cannot increase the size dynamically if your WLC instance started with an 8 GB OVA (from before 17.3). The only way is to create a new WLC from an OVA dated later than 17.3.
- The Cisco Catalyst 9800-L Wireless Controller can fail to respond to the break signals received on its console port during boot time, preventing users from getting to the rommon. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) rommon for the Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the rommon, see the **Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers** section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- If this error message is displayed after a reboot or system crash, it is recommended that you regenerate the trustpoint certificate:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

  Use these commands in the order specified in order to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# no crypto pki trustpoint trustpoint_name
  3. device(config)# no ip http server
  4. device(config)# no ip http secure-server
  5. device(config)# ip http server
  6. device(config)# ip http secure-server
  7. device(config)# ip http authentication local/aaa

- Verify that your mobility MAC address is set with the wireless mobility mac-address command.
- These protocols are now supported through the service port in 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI

    - HTTP
    - HTTPS
    - LDAP
    - Licensing for Smart Licensing feature to communicate with CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (including CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+

- The AP image for 17.9 is bigger than the AP flash originally allowed. If you see the AP complaining about not having enough space when downloading the 17.9 image, it is probably because you did not respect the upgrade path through 17.3.5 as advised in the release notes, or that your AP is running an older AireOS image. Either transiting through a 17.3.5 and later WLC or upgrading the AireOS image to the latest resizes the AP flash in order to allow to download the 17.9 image.
- Once an AP upgrades to 17.12 or later release, its console baud rate does not change immediately. However, if factory reset (or if a new AP out of the box joins a 17.12 or later WLC), it uses a 115200 console baud rate by default.

Downgrade

Downgrades are not officially supported and configuration loss of new features can occur. However, as downgrades can happen in the real world, this document still lists the most common traps in order to avoid downgrading. In order to find the information you need, check the version you are downgrading from (the version before the downgrade).

Gibraltar

16.12.2

- Nothing to point out here.

16.12.3

- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

16.12.4

- If you downgrade from this release to a lower one, the WLC can end up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990/Cisco bug ID CSCvv87417.
- The Cisco Catalyst 9800 Wireless Controller can reload if downgraded from 17.x to 16.12.4a. In order to avoid this, it is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

Amsterdam

17.1.1

- If you downgrade from this release to a lower one, the WLC can end up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990/CSCvv8741.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

17.2.1

- If you downgrade from this release to a lower one, the WLC can end up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990/Cisco bug ID CSCvv87417.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with a higher range than four disappear.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

17.3.1

- If you downgrade from this release to a lower one, the WLC can end up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990

  /CSCvv8741.

- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with a higher range disappear.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you can face the day-0 wizard again if you had the 'wireless country' command configured as it did not exist before 17.3.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.
- It is not possible to shut down the WLAN policy profile when you downgrade from Cisco IOS XE Amsterdam 17.3.x (supporting local switching IPv6 AVC) to Cisco IOS XE Gibraltar 16.12.x (where local switching IPv6 AVC is not supported). In such instances, it is recommended that you delete the existing WLAN policy profile and create a new one.

17.3.2

- If you downgrade from this release to a lower one, the WLC ends up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990/Cisco bug ID CSCvv87417.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that

are configured with a higher range disappear.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you can face the day-0 wizard again if you had the 'wireless country' command configured as it did not exist before 17.3.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.
- It is not possible to shut down the WLAN policy profile when you downgrade from Cisco IOS XE Amsterdam 17.3.x (supporting local switching IPv6 AVC) to Cisco IOS XE Gibraltar 16.12.x (where local switching IPv6 AVC is not supported). In such instances, it is recommended that you delete the existing WLAN policy profile and create a new one.

17.3.3

- If you downgrade from this release to a lower one, the WLC can end up in a boot loop if telemetry was configured due to Cisco bug ID CSCvt69990/Cisco bug ID CSCvv87417.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with a higher range disappear.
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you can face the day-0 wizard again if you had the 'wireless country' command configured as it did not exist before 17.3.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.
- It is not possible to shut down the WLAN policy profile when you downgrade from Cisco IOS XE Amsterdam 17.3.x (supporting local switching IPv6 AVC) to Cisco IOS XE Gibraltar 16.12.x (where local switching IPv6 AVC is not supported). In such instances, it is recommended that you delete the existing WLAN policy profile and create a new one.

17.4.1

- If you downgrade from Cisco IOS XE Amsterdam 17.4.1 to a release before 17.3, you can face the day-0 wizard again if you had the 'wireless country' command configured as it did not exist before 17.3.
- If you downgrade from Cisco IOS XE Amsterdam 17.4.1 to an earlier release, you lose the telemetry connection as 17.4 uses named telemetry destinations which were not supported commands in earlier versions. You must re-create the telemetry connection.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

17.5.1

- If you downgrade from Cisco IOS XE Amsterdam 17.4.1 to a release before 17.3, you can face the day-0 wizard again if you had the 'wireless country' command configured as it did not exist before 17.3.
- If you downgrade from Cisco IOS XE Amsterdam 17.4.1 to an earlier release, you lose the telemetry connection as 17.4 uses named telemetry destinations which were not supported commands in earlier versions. You must re-create the telemetry connection.
- Continuous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. It is recommended that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

17.9.x

- You cannot see 802.1x passwords in cleartext from this release because they are encrypted. If you downgrade to an earlier image that does not support an encrypted password, the APs get stuck and repeatedly fail the dot1x authentication due to wrong credentials. You must disable 802.1x on the AP switch port in order to allow the AP to join the controller before setting the cleartext password.

17.10.1

- You can not see 802.1x passwords in cleartext from this release because they are encrypted. If you downgrade to an earlier image that does not support an encrypted password, the APs get stuck and repeatedly fail the dot1x authentication due to wrong credentials. You must disable 802.1x on the AP switch port in order to allow the AP to join the controller before setting the cleartext password.

17.11.1

- You can not see 802.1x passwords in cleartext from this release because they are encrypted. If you downgrade to an earlier image that does not support an encrypted password, the APs get stuck and repeatedly fail the dot1x authentication due to wrong credentials. You must disable 802.1x on the AP switch port in order to allow the AP to join the controller before setting the cleartext password.

17.12.x

- You can not see 802.1x passwords in cleartext from this release because they are encrypted. If you downgrade to an earlier image that does not support an encrypted password, the APs get stuck and repeatedly fail the dot1x authentication due to wrong credentials. You must disable 802.1x on the AP switch port in order to allow the AP to join the controller before setting the cleartext password.

Related Information

- 17.1 hot patching and rolling AP upgrade guide
- 17.3 hot patching and ISSU upgrade guide.
- Cisco Technical Support & Downloads