Upgrade and downgrade of Catalyst 9800 Controllers : tips and tricks

Contents

Introduction
Before you proceed
The special case of engineering special versions
Upgrade
Gibraltar
16.12.2
16.12.3
16.12.4
16.12.5
Amsterdam
17.1.1
17.2.1
17.3.1
17.3.2
17.3.3
Bengaluru
17.4.1
17.5.1
Downgrade
Gibraltar
16.12.2
16.12.3
16.12.4
Amsterdam
17.1.1
17.2.1
17.3.1
17.3.2
17.3.3
17.4.1
References

Introduction

This document aims at highlighting things to watch out for when upgrading or downgrading a Catalyst 9800 Wireless LAN Controller (WLC) through several IOS-XE releases. This document does not aim at replacing the release notes which should always be the go-to document when upgrading. The aim is to facilitate the upgrade through several releases by highlthing the most impactful changes between releases.

Before you proceed

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

By default, the http server of the 9800 is not staitically mapped to aspecific certificate/trustpoint which can lead to changes after upgrade. Please 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 config before upgrading.

The special case of engineering special versions

Engineering special builds do not support ISSU upgrade 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 3 releases at once. For example, upgrading from 16.12.1 to 17.3.2 is covered by this document, however not upgrades from 16.12 to 17.4. In such a scenario, please go through 17.3 and check the notes under the 17.3 section, perform the upgrade and then look at the 17.4 section and prepare the second upgrade. As conclusion, tips listed are not repeated anymore after 3 major releases, even if still valid as the document assumes you go 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 default policy tag, it will go down due to the default mapping change. To restore the network operation, add the required WLAN to policy mappings under the default policy tag.

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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. To restore the network operation, add the required WLAN to policy mappings under the default policy tag.

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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. To restore the network operation, add the required WLAN to policy mappings under the default policy tag.

16.12.5

- Same as 16.12.4

Amsterdam

17.1.1

- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. 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 to check for connectivity. You need to ensure traffic filtering between the APs and the default gateway (like ACLs) 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 will reload at 4 hours interval.

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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports

being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. 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 need to ensure traffic filtering between the APs and the default gateway (like ACLs) 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 will reload at 4 hours interval.

17.3.1

- 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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. 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 need to ensure traffic filtering between the APs and the default gateway (like ACLs) 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 will reload at 4 hours interval.
- If you have configured FIPS mode, ensure that you remove **security wpa wpa1 cipher tkip** configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to do so will set the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you may have to reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, 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 will fail if you add MAC address with separators in the web UI or CLI.
- From this release onwards, APs will reload after 4 hours if they cannot join a WLC, cannot

ping their gateway AND ARP their gateway (All 3 need to fail for the AP to reboot). This is an enhancement (CSCvt89970) to the previous icmp-only gateway verification from previous releases
- From 17.3.1 onwards, the new way to configure country code 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 the maximum amount of country code way above 20. The commands "ap country" are still present and will still work, however, please consider changing them to the "Wireless country" commands as the ap country commands will be 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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. 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 need to ensure traffic filtering between the APs and the default gateway (like ACLs) 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 will reload at 4 hours interval.
- If you have configured FIPS mode, ensure that you remove **security wpa wpa1 cipher tkip** configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to do so will set the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you may have to reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, 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 will fail if you add MAC address with separators in the web UI or CLI.
- From 17.3.1 onwards, APs will reload after 4 hours if they cannot join a WLC, cannot ping their gateway AND ARP their gateway (All 3 need to fail for the AP to reboot). This is an enhancement (CSCvt89970) to the previous icmp-only gateway verification from previous releases
- From 17.3.1 onwards, the new way to configure country code 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 the maximum amount of country code way above 20. The commands "ap country" are still present and will still work, however, please consider changing them to the "Wireless country" commands as the ap country commands will be 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. Please verify the list of supported SFP and make sure your SFPs are compatible to avoid the data ports being down after the upgrade
- Upgrade file for this release may be too big for HTTP upload (when doing web UI upgrade) if you are in 16.12.1 release. Use another transfer method or go 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 default policy tag, it will go down due to the default mapping change. 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 need to ensure traffic filtering between the APs and the default gateway (like ACLs) 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 will reload at 4 hours interval.
- If you have configured FIPS mode, ensure that you remove **security wpa wpa1 cipher tkip** configuration from any WLAN before upgrading Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to do so will set the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, you may have to reconfigure WLAN with AES.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, 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 will fail if you add MAC address with separators in the web UI or CLI.
- From 17.3.1 onwards, APs will reload after 4 hours if they cannot join a WLC, cannot ping their gateway AND ARP their gateway (All 3 need to fail for the AP to reboot). This is an enhancement (CSCvt89970) to the previous icmp-only gateway verification from previous releases
- From 17.3.1 onwards, the new way to configure country code 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 the maximum amount of country code way above 20. The commands "ap country" are still present and will still work, however, please consider changing them to the "Wireless country" commands as the ap country commands will be deprecated in a future version.
- WLC might crash if your APs have hostnames longer than 32 characters (CSCvy11981)

Bengaluru

17.4.1

- From 17.4.1 onwards, Wave 1 IOS-based APs are not supported anymore (1700,2700,3700,1570) with the exception of IW3700.
- Your WLANs may be shut down after upgrade if they are non-WPA (e.g. guest, open or CWA SSIDs) and have adaptive FT configured. The solution is to remove adaptive FT configuration before upgrade (CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID, so there is no loss of anything by removing it.
- WLC might crash if your APs have hostnames longer than 32 characters (CSCvy11981)

17.5.1

- From 17.4.1 onwards, Wave 1 IOS-based APs are not supported anymore (1700,2700,3700,1570) with the exception of IW3700.
- From Cisco IOS XE Bengaluru Release 17.4.1 onwards, the telemetry solution provides a name for 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-the upgrade version 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 Cisco DNA Centre.
- Your WLANs may be shut down after upgrade if they are non-WPA (e.g. guest, open or CWA SSIDs) and have adaptive FT configured. The solution is to remove adaptive FT configuration before upgrade (CSCvx34349). Adaptive FT configuration makes no sense on non-WPA SSID, so there is no loss of anything by removing it.
- WLC might crash if your APs have hostnames longer than 32 characters (CSCvy11981)
- When you upgrade the GUI from one release to another, we recommend that you clear 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 will not be able to access the GUI using HTTPS. To access the GUI using HTTPS, run the following commands:ip http session-module-list pkilist OPENRESTY_PKIip 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, we recommend that you regenerate the trustpoint certificate.The procedure to generate a new self-signed trustpoint is as follows:
  `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.`

Downgrade

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

Gibraltar

16.12.2

- Nothing to point out here.

16.12.3

- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend 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 may end up in a boot loop if telemetry was configured due to CSCvt69990 /CSCvv87417

Amsterdam

17.1.1

- If you downgrade from this release to a lower one, the WLC may end up in a boot loop if telemetry was configured due to CSCvt69990 / CSCvv8741
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend 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 may end up in a boot loop if telemetry was configured due to CSCvt69990 / CSCvv87417
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with higher range than 4 will disappear
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend 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 may end up in a boot loop if telemetry was configured due to CSCvt69990 / CSCvv8741
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with higher range will disappear
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you may face the day-0 wizard again if you had the "wireless country" command configured as it did not exist before 17.3
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is

downgraded from 17.x to 16.12.4a. We recommend 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, we recommend 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 may end up in a boot loop if telemetry was configured due to CSCvt69990 / CSCvv87417
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with higher range will disappear
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you may face the day-0 wizard again if you had the "wireless country" command configured as it did not exist before 17.3
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend 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, we recommend 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 may end up in a boot loop if telemetry was configured due to CSCvt69990 / CSCvv87417
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with higher range will disappear
- If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, you may face the day-0 wizard again if you had the "wireless country" command configured as it did not exist before 17.3
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend 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, we recommend 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 an earlier release before 17.3, you may 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 will lose the

telemetry connection as 17.4 uses named telemetry destination which were not supported commands in previous versions. You will need to re-create the telemetry connection.
- Continous reload is observed when the Cisco Catalyst 9800 Wireless Controller is downgraded from 17.x to 16.12.4a. We recommend that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

References

17.1 hot patching and rolling AP upgrade guide

17.3 hot patching and ISSU upgrade guide.