

Release-specific Caveats and Workarounds

Some IOS XR releases have changes to the upgrade procedure due to new features and enhancements in these releases. The information in this section summarises the key changes. To view supported upgrade paths and caveats for any release upgrade path, use the **show install upgrade-matrix** commands.

- Release 25.3.1, on page 1
- Release 25.2.1, on page 3
- Release 7.10.1, on page 5
- Release 7.9.1, on page 7
- Release 7.7.2, on page 8
- Release 7.7.1, on page 8
- Release 7.5.2, Release 7.5.3, on page 9
- Release 7.5.1, Release 7.3.2, on page 10

Release 25.3.1

The caveats in 25.3.1 release are:

- CSCwo09365: FPDs not upgraded prior to install operation for upgrade to 25.2.1+ (Cisco 8000).
- CSCwo11635: Limit on Harddisk Files preserved in 8000-x86 upgrades/downgrades to/from versions >=25.2.1.
- CSCwq98264: No automatic recovery back to start software if unexpected reload occurs during install.
- CSCwq98275: **install package replace** and **install rollback** no longer supported for release upgrade/downgrade.

Table 1: Upgrade caveats

From	To	Bridge SMUs required (CSCwm77418)	Caveats
7.10.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
7.11.2 , 7.11.21	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635

From	To	Bridge SMUs required (CSCwm77418)	Caveats
24.1.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.2.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.2.20, 24.2.20x, 24.2.21	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.1	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.20, 24.3.30	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.4.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.4.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.1.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.1.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.2.15, 25.2.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365

Table 2: Downgrade caveats

From	To	Target SMUs required (CSCwm77418)	Caveats
25.3.1	7.10.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	7.11.2 , 7.11.21	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.1.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.2.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635

From	To	Target SMUs required (CSCwm77418)	Caveats
25.3.1	24.2.20, 24.2.20x, 24.2.21	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.3.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.3.20, 24.3.30	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.4.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	24.4.2	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	25.1.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	25.1.2	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.3.1	25.2.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	25.2.15, 25.2.2	No	CSCwq98264, CSCwq98275, CSCwo09365

Release 25.2.1

The caveats in 25.2.1 release are:

- CSCwo09365: FPDs not upgraded prior to install operation for upgrade to 25.2.1+ (Cisco 8000).

  CSCwo11635: Limit on Harddisk Files preserved in 8000-x86 upgrades/downgrades to/from versions >=25.2.1.

- CSCwq98264: No automatic recovery back to start software if unexpected reload occurs during install.
- CSCwq98275: **install package replace** and **install rollback** no longer supported for release upgrade/downgrade.

For further information on these caveats, see Restrictions for disk encryption.

Table 3: Upgrade caveats

From	To	Bridge SMUs required (CSCwm77418)	Caveats
7.10.2	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
7.11.2 , 7.11.21	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.1.2	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.2.11	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.2.2	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.2.20, 24.2.21	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.1	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.2	25.2.1+	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.3.20	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.4.1	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
24.4.2	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.1.1	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.1.2	25.2.1+	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635

Table 4: Downgrade caveats

From	To	Target SMUs required (CSCwm77418)	Caveats
25.2.1+	7.10.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	7.11.2 , 7.11.21	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635

From	To	Target SMUs required (CSCwm77418)	Caveats
25.2.1+	24.1.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.2.11	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.2.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.2.20, 24.2.21	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.3.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.3.20	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.4.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	24.4.2	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	25.1.1	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635
25.2.1+	25.1.2	No	CSCwq98264, CSCwq98275, CSCwo09365, CSCwo11635

Release 7.10.1

The following upgrade caveats are applicable for Release 7.10.1 and later:

Table 5: Upgrade Caveats

From	To	Bridge SMUs Required	Caveats
7.3.3	7.10.1 and later	Yes	1*, 2*, 3*
7.3.4	7.10.1 and later	Yes	1*, 2*, 3*
7.5.3	7.10.1 and later	None	1*
7.5.4	7.10.1 and later	None	1*
7.7.1	7.10.1 and later	None	1*

From	To	Bridge SMUs Required	Caveats
7.7.2	7.10.1 and later	None	1*
7.8.1	7.10.1 and later	None	1*
7.8.2	7.10.1 and later	None	1*
7.9.1	7.10.1 and later	None	1*
7.9.2	7.10.1 and later	None	1*

1*: You can't roll back using the **install rollback** command.

2*: Ensure that a reload bridging SMU (CSCwd71524) is installed.

3*: Ensure that you install the bridge SMU (CSCwd71524) manually because even if it's available inside the GISO that's replacing the existing GISO, this SMU doesn't get installed automatically.

Note CSCwd71524:

- When you upgrade from earlier than Release 7.10.1 to Release 7.10.1, system supports the installation process seemlessly.
- When you downgrade from Release 7.10.1, system preserves the present configuration and the install history from last transaction.

The following downgrade caveats are applicable for Release 7.10.1 and later:

Table 6: Downgrade Caveats

From	To	Bridge SMUs Required	Caveats
7.10.1 and later	7.3.3	Yes	C*
7.10.1 and later	7.3.4	Yes	C*
7.10.1 and later	7.5.3	Yes	***, A*, B*
7.10.1 and later	7.5.4	Yes	***, A*
7.10.1 and later	7.7.1	Yes	***, A*, B*
7.10.1 and later	7.7.2	Yes	***, A*, B*
7.10.1 and later	7.8.1	Yes	***, A*, B*
7.10.1 and later	7.8.2	Yes	***, A*, B*
7.10.1 and later	7.9.1	Yes	***
7.10.1 and later	7.9.2	Yes	***

***

- You don't need to run the **install commit** command after a downgrade operation because the operation is automatically committed.
- You can't roll back after a downgrade. To revert to the previous IOS XR previous version, replace or reimage to the relevant ISO.
- IOS XR configuration history is lost after a downgrade, but the router preserves the latest configuration.
- Install history from the last transaction is preserved after a downgrade operation.
- Downtime takes a longer time as the operation is performed through reimage.
- You can't downgrade using the **install package replace** command. Instead, use the **install replace** command to downgrade.
- Ensure that you reinstall third-party application once you complete the downgrade.
- PXE recovery is required if the image downgrading isn't bootable.
- You must re-install the *Type 6 masterkey* and reapply the configuration encrypted by it because they are lost after the downgrade.
- You must regenerate crypto keys and certificates after a downgrade.

A*: You can't downgrade to the base ISO. You can downgrade to a GISO containing the bridge SMU (CSCwd71524).

B*: You must recover the router through PXE if a power cycle occurs during the downgrade.

C*: One-step downgrade isn't supported. You must use either PXE/USB to downgrade or perform a two-step downgrade through Release 7.9.1 or Release 7.5.4. The first-hop downgrade to Release 7.9.1 or Release 7.5.4 still carries the same caveats.

Use the **show install upgrade-matrix running** command to view the caveats.

Release 7.9.1

The following caveats are applicable to Release 7.9.1 and later:

- CSCvy66646 (Hitless/Recommended SMU)—When you upgrade from releases earlier than 7.3.2 to release 7.8.2, we recommend that you install the `8000-version-CSCvy66646.tar` SMU from Cisco Software Download center and commit the install operation. Without this SMU, if you upgrade the router and if the router is reloaded due to any issue (excluding **install apply reload** command) before you commit the install operation, the system may prevent install operations in the future.
- CSCvw93597—If the **install package add** *pkg-name* command after **install package replace 8000-x64-7.9.1.iso** command fails when upgrading from release 7.3.15, rerun the **install package add** *pkg-name* command.
- CSCwc47306—The appmgr crashes continuously while downgrading from release 7.8.2 (with the healthcheck optional RPM) to releases earlier than 7.8.2. There is no impact to the upgrade operation.
- CSCwd59323—The counter-size value configured using **healthcheck metric** command is lost when the router is upgraded to release 7.8.2. This size indicates the buffer that stores the history of the counter value. Reconfigure the counter-size to a value in the range of 2 to 15 cadence snapshots.

- CSCwc47212—Configuration on breakout interface is lost after downgrading to releases earlier than 7.8.1 on 8202 router variants. Reapply the configuration.
- CSCwd30936—The `ema_server_sdr` process crashes after downgrading to releases earlier than 7.8.1. There is no workaround and no impact to the functionality.

Release 7.7.2

The following caveats are applicable for Release 7.7.2 and later:

- CSCvy66646 (Hitless/Recommended SMU)—When you upgrade from releases earlier than 7.3.2 to release 7.7.2, we recommend that you install the `8000-version-CSCvy66646.tar` SMU from Cisco Software Download center and commit the install operation. Without this SMU, if you upgrade the router and if the router is reloaded due to any issue (excluding **install apply reload** command) before you commit the install operation, the system may prevent install operations in the future.
- CSCvw93597—If the **install package add** *pkg-name* command after **install package replace 8000-x64-7.7.2.iso** command fails when upgrading from release 7.3.15, rerun the **install package add** *pkg-name* command.
- CSCwc47306—The appmgr crashes continuously while downgrading from release 7.7.2 (with the healthcheck optional RPM) to releases earlier than 7.7.2. There is no impact to the upgrade operation.
- CSCwb36889—When you upgrade from release 7.3.x to release 7.7.2, the line cards (LCs) may continue to be in the `BOOT HOLD` state, or the BIOS FPD may be in `NEED UPGD` state. This is an intermittent behavior and we recommend that you install the SMU on the 7.3.x image before upgrading to release 7.7.2.
- CSCwd37438—Upgrading from releases earlier than 7.7.2 leads to an additional silent reload due to BMC FPGA upgrade. This is specific to only 8201 and 8202 chassis. There is no impact to the upgrade operation. We recommend that you install the RPM before upgrading to release 7.7.2.

Release 7.7.1

The following upgrade caveats are applicable for Release 7.7.1 and later:

- CSCvy66646 (Hitless/Recommended SMU)—When you upgrade from releases earlier than 7.3.2 to releases 7.7.1, we recommend that you install the `8000-version-CSCvy66646.tar` SMU from Cisco Software Download center and commit the install operation. Without this SMU, if you upgrade the router and if the router is reloaded due to any issue (excluding **install apply reload** command) before you commit the install operation; the system may prevent install operations in the future.
- CSCvw93597—If the **install package add** *pkg-name* command after **install package replace** *iso-image* command fails when upgrading from release 7.3.15, rerun the **install package add** *pkg-name* command.
- CSCvz88814—The upgrade operation fails only in the following scenario:
  1. Upgrade from release 7.3.1 to release 7.7.1
  2. Downgrade from release 7.7.1 to release 7.3.1
  3. Upgrade again to release 7.7.1. The operation fails.

To avoid the failure when you upgrade after you downgrade the router, run the following commands in order:

1. **install package remove** *any optional package*
2. **install package abort all-since-apply**
3. **install replace** *iso-image*

Release 7.5.2, Release 7.5.3

The following caveats are applicable for Release 7.5.2 and Release 7.5.3:

- CSCvy66646 (Hitless/Recommended SMU)—When you upgrade from releases earlier than 7.3.2 to releases 7.5.2 or 7.5.3, we recommend that you install the `8000-version-CSCvy66646.tar` SMU from Cisco Software Download center and commit the install operation. Without this SMU, if you upgrade the router and if the router is reloaded due to any issue (excluding **install apply reload** command) before you commit the install operation; the system may prevent install operations in the future.
- CSCvw93597—If the **install package add** *pkg-name* command after **install package replace** *iso-image* command fails when upgrading from release 7.3.15. To solve the issue, rerun the **install package add** *pkg-name* command.
- CSCvz44123—An error message `ACCESS failure 'fail to get BiosGolden fpd info` displayed on the BIOS does not have a functional impact on the router. After the router is upgraded, the FPD shows the `CURRENT` state.

```
RP/0/RP0/CPU0:Feb 14 21:05:55.720 UTC: fpd_client[251]:
%PLATFORM-CPA_INTF_FPD-3-ACCESS_ERROR : Node
0/RP0/CPU0 FPD BiosGolden ACCESS failure 'fail to get BiosGolden fpd info'
RP/0/RP0/CPU0:Feb 14 21:05:55.738 UTC: fpd_client[251]:
%PLATFORM-CPA_INTF_FPD-3-ACCESS_ERROR : Node
0/RP0/CPU0 FPD Bios ACCESS failure 'fail to get Bios fpd info'
```

- CSCvz88814—The upgrade operation fails only in the following scenario:
  1. Upgrade from release 7.0.14, 7.2.1 or 7.3.1 to release 7.5.2 or 7.5.3
  2. Downgrade from release 7.5.2 or 7.5.3 to release 7.0.14, 7.2.1 or 7.3.1
  3. Upgrade again to release 7.5.2 or 7.5.3. The operation fails.

  To avoid the failure when you upgrade after you downgrade the router, run the following commands in order:

  1. **install package remove** *any optional package*
  2. **install package abort all-since-apply**
  3. **install replace** *iso-image*

Release 7.5.1, Release 7.3.2

The following caveats are applicable for Release 7.5.1 and Release 7.3.2:

- CSCvv17670—The issue with FPDs not upgraded on the line cards in release 7.0.14 with default auto FPD enabled. This issue is resolved in release 7.3.2.
- When auto FPD is enabled, the FPDs are automatically updated when a SMU or image changes, including an updated firmware revision. Although the FPD auto upgrade is enabled by default, when upgrading to release 7.5.1 or 7.3.2, we recommend that you run the **fpd auto-upgrade enable** command to avoid FPD upgrade failures.