Release-specific Caveats and Workarounds

This section lists the caveats and workarounds when setting up or upgrading the software for each Cisco IOS XR release.

Caveats and Workarounds

Release 7.4.1

There are no caveats for system upgrade to Cisco IOS XR Release 7.4.1.

Release 7.4.2

CSCvp19524: When downgrading from Cisco IOS XR Release 7.4.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

Release 7.5.1

CSCvp19524: When downgrading from Cisco IOS XR Release 7.5.1 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

Release 7.5.2

CSCvp19524: When downgrading from Cisco IOS XR Release 7.5.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

Release 7.6.2

1. **CSCvp19524:** When downgrading from Cisco IOS XR Release 7.6.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. **CSCwb36344:** When downgrading from Cisco IOS XR Release 7.6.1 and later releases to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

Recommended Workaround

If you are upgrading to Cisco IOS XR Release 7.6.2, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

In scenarios where the above option is not available:

a. Perform software installation via iPXE or USB.

b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

Please contact your TAC representative for further information.

Release 7.7.2

1. **CSCvp19524:** When downgrading from Cisco IOS XR Release 7.7.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. **CSCwb36344:** When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.7.2) to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

   Recommended Workaround

   If upgrading to Cisco IOS XR Release 7.7.2, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

   In scenarios where the above option is not available:

   a. Perform software installation via iPXE or USB.

   b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

      Please contact your TAC representative for further information.

   c. When upgrading the software version of an ASR 9000 router with an mLACP/ICCP Redundancy Model setup, ensure that both the active and standby nodes are upgraded to the same IOS XR version.

Release 7.8.1

1. **CSCvp19524:** When downgrading from Cisco IOS XR Release 7.8.1 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. **CSCwb36344:** When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.8.1) to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

   Recommended Workaround

If you are upgrading to Cisco IOS XR Release 7.8.1, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

In scenarios where the above option is not available:

a. Perform software installation via iPXE or USB.

b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

Please contact your TAC representative for further information.

Release 7.8.2

1. **CSCvp19524:** When downgrading from Cisco IOS XR Release 7.8.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. CSCwb36344: When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.8.2) to versions lower than 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

   Recommended Workaround

   If you are upgrading to Cisco IOS XR Release 7.8.2, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

   In scenarios where the above option is not available:

   a. Perform software installation via iPXE or USB.

   b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

   Please contact your TAC representative for further information.

Release 7.9.1

1. **CSCvp19524:** When downgrading from Cisco IOS XR Release 7.9.1 to any release lower than Cisco IOS XR Release 7.0.1, it's necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. **CSCwb36344:** When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.9.1) to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

   Recommended Workaround

   If you are upgrading to Cisco IOS XR Release 7.9.1, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

   In scenarios where the above option is not available:

    a. Perform software installation via iPXE or USB.

    b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

    Please contact your TAC representative for further information.

3. CSCwd30936: When downgrading from Cisco IOS XR Release 7.9.1 to an older release, the "ema_server_sdr" process may crash.

Release 7.9.2

1. CSCvp19524: When downgrading from Cisco IOS XR Release 7.9.2 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. CSCwb36344: When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.9.2) to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process as it causes continuous process crashes and respawns.

Recommended Workaround

If you are upgrading to Cisco IOS XR Release 7.9.2, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

In scenarios where the above option is not available:

    a. Perform software installation via iPXE or USB.

    b. If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

    Please contact your TAC representative for further information.

3. CSCwd30936: When downgrading from Cisco IOS XR Release 7.9.2 to an older release, the "ema_server_sdr" process may crash.

Release 7.10.1

1. CSCvp19524: When downgrading from Cisco IOS XR release 7.10.1 to any release lower than Cisco IOS XR Release 7.0.1, it is necessary to remove AAA user configurations from SYSADMIN/XR VMs before proceeding with the downgrade.

2. CSCwb36344: When downgrading from Cisco IOS XR Release 7.6.1 and later releases (including Cisco IOS XR Release 7.10.1) to versions lower than Cisco IOS XR Release 7.6.1, there is a risk of loading incomplete DLLs during the downgrade process, causing continuous process crashes and respawns.

Recommended Workaround

If you are upgrading to Cisco IOS XR Release 7.10.1, do not perform the install commit after the upgrade. If you need to revert to the previous image, perform the **hw-module reload** operation.

In scenarios where the above option is not available:

      a.   Perform software installation via iPXE or USB.

      b.   If the system is currently running Cisco IOS XR Software 7.6.1 or later, a specific SMU (CSCwb36344) for the older release can be provided. When downgrading, use the release default ISO and packages along with the CSCwb36344 SMU. After the downgrade, perform the install commit, deactivate the CSCwb36344 packages, and add any other required or recommended SMUs for the release.

         Please contact your TAC representative for further information.

3. **CSCwd30936:** When downgrading from Cisco IOS XR Release 7.10.1 to an older release, the "ema_server_sdr" process may crash.

4. **SR695094155:** When upgrading the software version of an ASR 9000 router with an mLACP/ICCP Redundancy Model setup, ensure that both the active and standby nodes are upgraded to the same IOS XR version.

Release 24.1.1

Table 1: Upgrade Caveats for Cisco IOS XR Release 24.1.1 and Later

To Upgrade From Cisco IOS XR Release...	To Cisco IOS XR Release...	Bridge SMU Required	Caveats
Release 7.11.1	Release 24.1.1	CSCwi95358, CSCwh61644	A*
Release 7.10.2	Release 24.1.1		
Release 7.10.1	Release 24.1.1		
Release 7.9.2.1	Release 24.1.1		
Release 7.9.2	Release 24.1.1		
Release 7.8.2	Release 24.1.1		
Release 7.7.2	Release 24.1.1		
Release 7.6.2	Release 24.1.1		
Release 7.5.2	Release 24.1.1		
Release 7.4.2	Release 24.1.1		
Release 7.3.2	Release 24.1.1		

A*: Ensure that bridge SMUs (CSCwi95358, CSCwh61644) are installed before system upgrade.

> **Note** **CSCwi95358:**
>
> • This is a hitless SMU in Cisco IOS XR Release 7.4.1. Installing the SMU does not impact traffic and services. Do not reload the system when this SMU is installed.
>
> • This is a reload SMU in Cisco IOS XR Release 7.3.2, which reloads the system when installed.
>
> **CSCwh61644**—When installed following a software upgrade, both the Line Card (LC) and the Route Processor (RP) become active and function properly.

Table 2: Downgrade Caveats for Cisco IOS XR Release 24.1.1 and Earlier

From	To	Revisions to Include	Caveats
Release 24.1.1	Release 7.11.1	CSCwi95358	A*
Release 24.1.1	Release 7.10.2		
Release 24.1.1	Release 7.10.1	CSCwi95358, CSCwh61644	A*, B*
Release 24.1.1	Release 7.9.2.1		
Release 24.1.1	Release 7.9.2		
Release 24.1.1	Release 7.8.2		
Release 24.1.1	Release 7.7.2		
Release 24.1.1	Release 7.6.2		
Release 24.1.1	Release 7.5.2		
Release 24.1.1	Release 7.4.2	CSCwi95358, CSCwh61644,CSCwb36344	A*, B*, C*
Release 24.1.1	Release 7.3.2		

A*: Ensure that the additional enhancement (CSCwi95358) is included.

B*: Ensure that the additional enhancement (CSCwh61644) is included.

C*: Ensure that the additional enhancement (CSCwb36344) is included.

> **Note** **CSCwi95358:**
>
> • This is a hitless SMU in Cisco IOS XR Release 7.4.1. Installing the SMU does not impact traffic and services. Do not reload the system when this SMU is installed.
>
> • This is a reload SMU in Cisco IOS XR Release 7.3.4, which reloads the system when installed.
>
> **CSCwh61644**—When installed following a software upgrade, both the Line Card (LC) and the Route Processor (RP) become active and function properly.
>
> **CSCwb36344**—Prevents recurring crashes and process restarts due to the undefined symbols on the Route Processor (RP) and Line Cards (LCs).