



## CHAPTER 4

# Cisco IOS XE Software Package Compatibility for ISSU

---

This section discusses interoperability of different Cisco IOS XE software releases for the Cisco ASR1000 Series Aggregation Services Routers. It contains the following sections:

- [Overview, page 4-1](#)
- [Cisco IOS XE Release Compatibility Using the ISSU Process, page 4-2](#)

## Overview

When upgrading the Cisco IOS XE operating system software using the In Service Software Upgrade (ISSU) process, it is important to determine the compatibility of the upgraded software to your current software and hardware. The ISSU process allows software to be updated or otherwise modified while packet forwarding continues with minimal interruption. (See the [In Service Software Upgrades \(ISSU\)](#) section for a complete discussion of the ISSU upgrade process.)

This section discusses the interoperability of different Cisco IOS XE releases. [Table 4-1](#) and [Table 4-2](#) provide information about release pairs that are compatible and those that are not compatible for Cisco ASR1000 Series Routers. You can use this information to determine the impact of a Route Processor (RP) or Embedded Service Processor (ESP) switchover when the router is running a mixed combination of software as occurs during the whole-node ISSU procedures.

Table [Table 4-1](#) describes the compatibility of Cisco IOS XE software packages for the Cisco ASR1006 Series Router, a hardware-redundant chassis. The hardware-redundant chassis has two ESP linecards and two RPs which exchange state using hardware links.

Table [Table 4-2](#) describes the compatibility of Cisco IOS XE software packages for the Cisco ASR1002 and ASR1004 Series Routers which are not hardware redundant but are software redundancy capable. The non-redundant chassis has a single RP and a single ESP, but allows the operation of up to two IOS processes on the single RP to exchange states locally.

Cisco IOS XE releases not listed as compatible in [Table 4-1](#) and [Table 4-2](#) must not be run simultaneously (in a Cisco ASR1006 Series Router) or co-installed on any of the Cisco ASR1000 Series Routers since unexpected failures of one or both RPs or state loss can be experienced. Cisco IOS XE releases listed as partially compatible may incur a loss of state. Cisco IOS XE releases listed as requiring an intermediate release are not directly compatible; however, a migration path is available to preserve some or all state by upgrading to a separate intermediate version, as shown in [Table 4-1](#) and [Table 4-2](#). The tables do not cover non-redundant (software or hardware) environments as no incremental update is possible under those circumstances.

# Cisco IOS XE Release Compatibility Using the ISSU Process

Cisco IOS XE release compatibility using the ISSU process utilizes the SSO functionality to preserve state while software versions on the router differ, as during an upgrade. Most SSO-capable features in each Cisco IOS XE release are ISSU capable. ISSU is only supported if SSO is enabled in the configuration and the system is in a steady state (SSO ready state has been achieved). ISSU compatibility depends on the set of specific feature clients that are in use and whether they support ISSU. All ISSU upgrades include at least one IOS switchover operation. It is important to understand which features are in use and whether these features are ISSU compatible.

For non-hardware-redundant chassis types, the router must be running in subpackage mode to support ISSU. This is because ISSU on these chassis types requires sub-package installation and certain steps in a full ISSU upgrade will have impact equivalent to an ESP or SPA Interface Processor (SIP) online insertion and removal (OIR). SIP impact can be mitigated by installing SIPs one slot at a time if shared port adapters (SPAs) are redundant across SIPs (such as when using Gigabit Etherchannel, load balancing, and so on). Traffic loss cannot be avoided with the installation of the ESP package as a part of ISSU. For a non-hardware-redundant chassis, the chassis must be running with software redundancy active (not simply configured).

Hardware redundant chassis types support ISSU when running in sub-package mode or in consolidated package mode. As with non-hardware-redundant chassis types, SIP impact can be mitigated by installing SIPs one slot at a time if SPAs are redundant across SIPs (such as when using Gigabit Etherchannel). ESP redundancy provides similar capability for the ESP allowing hitless upgrade of a chassis from one software release to another. Consolidated package mode does not provide such a per-slot staging option and always incurs a traffic loss equivalent to simultaneous OIR of all SIPs.

Non-SSO-capable features and non-ISSU-capable features are not included in [Table 4-1](#) or [Table 4-2](#) since these features lose state on any Cisco IOS XE switchover—RP switchover in the case of hardware-redundant chassis and software switchover on software-redundant chassis.

## Discussion of Table Fields

In [Table 4-1](#) and [Table 4-2](#), the following information is provided:

- SSO
  - A Cisco IOS XE release denoted in [Table 4-1](#) or [Table 4-2](#) as supporting SSO for all supported SSO-capable features is fully compatible for upgrades using ISSU, even if some of the SSO-capable features are not ISSU capable. Two different versions of the software are denoted as supporting SSO if they are able to reach an SSO state when run simultaneously, regardless of the impact on specific features.
- SSO Tested
  - A Cisco IOS XE release denoted in [Table 4-1](#) or [Table 4-2](#) as SSO Tested indicates that the two releases are fully tested and supported as interoperable and will retain state across a switchover. ISSU upgrades between the releases are supported.
- SSO via *<release>*
  - A Cisco IOS XE release denoted in [Table 4-1](#) or [Table 4-2](#) as SSO via *<release>* indicates that the two releases are not interoperable and must not be run simultaneously (must not be run at the same time on the two RPs of a hardware redundant chassis and must not be co-installed as subpackages on any chassis). However, an SSO path exists using the intermediate release that is specified.

- Limited

A Cisco IOS XE release denoted in [Table 4-2](#) as Limited indicates that the two releases have interoperability limitations. On the Cisco ASR1002 and Cisco ASR1004 routers, an ISSU upgrade is supported but a downgrade requires a stateless reload. This means booting the appropriate pre-upgraded sub-package provisioning file and package set.

## Restrictions

- Cisco IOS XE software compatibility is between “like” images, for example, *advipservicesk9* to *advipservicesk9*, *adventerprisek9* to *adventerprisek9*, and so on. Cross-image-type upgrades or installations are not supported in the ISSU process. For example, you cannot upgrade *ipbase* to *advipservicesk9* or *advipservices* to *advipservicesk9*.
- Different image types must not be run simultaneously.

## Compatibility Support Policy

Rebuilds of a specific Cisco IOS XE release are intended to be fully ISSU and SSO capable for supported features between any two image pairings, however compatibility is not guaranteed for all releases. It is expected that rebuilds between release versions are compatible within a reasonable time frame.

### Support for Cisco IOS XE Rebuilds

The support policy for version rebuilds is as follows:

- The immediate prior rebuild for the version is expected to be SSO and ISSU compatible with a new released rebuild of that version.
- A newly released rebuild is expected to be SSO and ISSU compatible with the current rebuild for the previous two versions.

As an example, a rebuild Y of version X is version XY. For rebuilds on the two previous versions of X, X-1 and X-2, it is expected that XY will be compatible with those versions.

### Support for Special Cisco IOS XE Releases

Certain special Cisco IOS XE software releases may be made from time to time. These releases are not specified in this document and any supported SSO or ISSU interoperability must be determined on a case by case basis.

## Cisco IOS XE Release Compatibility Matrices

[Table 4-1](#) and [Table 4-2](#) list the compatibility of Cisco IOS XE releases.



#### Note

In [Table 4-1](#) and [Table 4-2](#):

- The software version numbers are given first as the Cisco IOS XE release version number followed by the bundled Cisco IOS release number.
- The Cisco IOS XE releases are populated according to the release post date.

**Note**

For descriptions of the table fields, see the “Discussion of Table Fields” section on page 4-2.

**Table 4-1 Cisco IOS XE Compatibility for Cisco ASR1006 Series Routers: Consolidated Package or Sub-package Mode**

Deployed Cisco IOS XE Release	Upgrading to: IOS XE 2.1.0 12.2(33)XNA	Upgrading to: IOS XE 2.1.1 12.2(33)XNA1	Upgrading to: IOS XE 2.1.2 12.2(33)XNA2	Upgrading to: IOS XE 2.2.1 12.2(33)XNB1	Upgrading to: IOS XE 2.2.2 12.2(33)XNB2	Upgrading to: IOS XE 2.2.3 12.2(33)XNB3	Upgrading to: IOS XE 2.3.0 12.2(33)XNC	Upgrading to: IOS XE 2.3.1 12.2(33)XNC1	Upgrading to: IOS XE 2.4 12.2(33)XND
IOS XE 2.1.0 12.2(33)XNA	—	SSO Tested <sup>1</sup>	SSO <sup>1</sup>	SSO via 2.1.2 <sup>1</sup>	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	—	—
IOS XE 2.1.1 12.2(33)XNA	SSO Tested <sup>1</sup>	—	SSO Tested	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	—	—
IOS XE 2.1.2 12.2(33)XNA 2	SSO <sup>1</sup>	SSO Tested	—	SSO Tested	SSO Tested	SSO <sup>2</sup>	SSO <sup>2</sup>	—	—
IOS XE 2.2.1 12.2(33)XNB1	SSO via 2.1.2 <sup>1</sup>	SSO via 2.1.2	SSO Tested	—	SSO Tested	SSO	SSO <sup>2</sup>	SSO via 2.2.3	SSO via 2.2.3
IOS XE 2.2.2 12.2(33)XNB2	SSO via 2.1.2 <sup>1</sup>	SSO via 2.1.2	Limited Tested	SSO Tested	—	SSO Tested	SSO Tested <sup>2</sup>	SSO via 2.2.3	SSO via 2.2.3
IOS XE 2.2.3 12.2(33)XNB3	SSO via 2.1.2	SSO via 2.1.2	Limited <sup>3</sup>	SSO	SSO Tested	—	SSO Tested <sup>2</sup>	SSO Tested	SSO Tested
IOS XE 2.3.0 12.2(33)XNC	SSO via 2.1.2	SSO via 2.1.2	Limited <sup>3</sup>	Limited <sup>3</sup>	SSO Tested	SSO Tested	—	SSO Tested	SSO
IOS XE 2.3.1 12.2(33)XNC1	—	—	—	SSO via 2.2.3	SSO via 2.2.3	SSO Tested	SSO Tested	—	SSO Tested
IOS XE 2.4 12.2(33)XND	—	—	—	SSO via 2.2.3	SSO via 2.2.3	SSO Tested	SSO	SSO Tested	—

1. Some ESP-maintained session state may be lost when ESPs of different versions interoperate. This affects primarily stateful firewall and network address translation functions implemented by the ESPs.
2. Use of new features in the uprev release may be limited after ISSU. To correct this issue, perform an additional redundancy force-switchover after completing all steps of the ISSU procedure and after the device has reached SSO. Alternatively, a chassis reload also addresses the issue.
3. Downgrade may fail depending on the features that are configured.

**Caution**

For upgrading deployed releases prior to Cisco IOS XE 2.1.2, refer to the appropriate configuration guide. Some adjustments to the configuration procedure may be necessary due to changes in the installation command syntax. See *Cisco IOS XE Software Configuration Guides*.

**Note**

For descriptions of the table fields, see the “Discussion of Table Fields” section on page 4-2.

**Table 4-2 Cisco IOS XE Compatibility for Cisco ASR1002 and ASR1004 Series Routers: Sub-package Mode**

Deployed Cisco IOS XE Release	Upgrading to: IOS XE 2.1.0 12.2(33)XNA	Upgrading to: IOS XE 2.1.1 12.2(33)XNA1	Upgrading to: IOS XE 2.1.2 12.2(33)XNA2	Upgrading to: IOS XE 2.2.1 12.2(33)XNB1	Upgrading to: IOS XE 2.2.2 12.2(33)XNB2	Upgrading to: IOS XE 2.2.3 12.2(33)XNB3	Upgrading to: IOS XE 2.3.0 12.2(33)XNC	Upgrading to: IOS XE 2.3.1 12.2(33)XNC1	Upgrading to: IOS XE 2.4 12.2(33)XND
IOS XE 2.1.0 12.2(33)XNA	—	SSO Tested	SSO	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	—	—
IOS XE 2.1.1 12.2(33)XNA1	SSO Tested	—	SSO Tested	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	SSO via 2.1.2	—	—
IOS XE 2.1.2 12.2(33)XNA2	SSO	SSO	—	SSO Tested	SSO Tested	SSO <sup>1</sup>	SSO via 2.2.2	—	—
IOS XE 2.2.1 12.2(33)XNB1	Limited	Limited	Limited	—	SSO Tested	SSO	SSO via 2.2.2	SSO via 2.2.3	SSO via 2.2.3
IOS XE 2.2.2 12.2(33)XNB2	SSO via 2.1.2	SSO via 2.1.2	Limited Tested	SSO Tested	—	SSO Tested	SSO Tested	SSO via 2.2.3	SSO via 2.2.3
IOS XE 2.2.3 12.2(33)XNB3	SSO via 2.1.2	SSO via 2.1.2	Limited <sup>2</sup>	Limited <sup>2</sup>	SSO Tested	—	SSO Tested	SSO Tested	SSO Tested
IOS XE 2.3.0 12.2(33)XNC	SSO via 2.1.2	SSO via 2.1.2	Limited <sup>2</sup>	Limited <sup>2</sup>	SSO Tested	SSO Tested	—	SSO Tested	SSO
IOS XE 2.3.1 12.2(33)XNC1	—	—	—	Limited SSO via 2.2.3	Limited SSO via 2.2.3	SSO Tested	SSO Tested	—	SSO Tested
IOS XE 2.4 12.2(33)XND	—	—	—	Limited SSO via 2.2.3	Limited SSO via 2.2.3	SSO Tested	SSO	SSO Tested	—

- When ISSU is used to upgrade router software, new features available in the new version are configurable as soon as the RP software portion of the update has been completed for both active and standby IOS. New features will be fully reflected in the operation of the router once the linecard images are also updated. Under some circumstances, the new features may not be available until after the final step of the ASR1002 and ASR1004 ISSU procedure is performed (chassis reload).
- The Cisco IOS software on the standby RP may spontaneously restart creating a core dump file when **issu loadversion** (issu command set) or **request platform software package install** (request platform command set) is used to simultaneously install the RP packages other than the base package (as specified by the {**rpcontrol,rpaccess,rpiois**} portion of the filename specification). The Cisco IOS software on the standby RP will recover after this event.

**Caution**

For upgrading deployed releases prior to Cisco IOS XE 2.1.2, refer to the appropriate configuration guide. Some adjustments to the configuration procedure may be necessary due to changes in the installation command syntax. See *Cisco IOS XE Software Configuration Guides*.

