

Additional Install Operations

After you upgrade your system, based on your requirement, you can perform additional install operations:

- View the Version of Installed Packages, on page 1
- Golden ISO images, on page 4
- Upgrade the System to Obtain Bug Fixes, on page 6
- Remove a bug fix from Cisco IOS XR software, on page 11
- Roll back software to a previously saved installation point , on page 12
- Telemetry Support for Install Operations, on page 15
- Caveats, on page 16
- View Features and Capabilities Supported on a Platform, on page 20
- Deprecated commands, on page 24

View the Version of Installed Packages

The router is shipped with a pre-installed operating system. You can view the version of the installed software and the active packages. If you have upgraded your system, installed additional packages or bug fixes, you can view the version of the committed packages.

Review the software version information:

- Package name and version
- User who built the package
- Time the package was built
- Build workspace
- Build host
- ISO label:
    - Label is present if GISO boots using PXE boot
    - Label is present if GISO is installed using the `install replace` method
    - Label reverts to default (only release version) if there is any change since the time the image with the label was installed.
    - Label is nullified and reverts to default if an RPM is added or removed on top of an existing GISO.

- Label is repopulated if an RPM from the GISO is added or removed and a rollback operation is performed.

- Copyright information
- Hardware information

Procedure

Step 1 View the version of the Cisco IOS XR software, and its various software components that are installed on the router.

Example:

The following example shows the version information for a non-GISO image:

NCS 5500 Series:

```
Router#show version
Cisco IOS XR Software, Version 7.5.2 LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
Built On     : Tue June 07 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5500/ws
Version      : 7.5.2
Label        : 7.5.2

cisco NCS5500L (D-1563N @ 2.00GHz)
cisco NCS-55A1-36H-S (D-1563N @ 2.00GHz) processor with 32GB of memory
ios uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS-55A1-36H-S Fixed Scale HW Flexible Consumption Need Smart Lic
```

NCS 5500 Series:

```
Router#show version
Cisco IOS XR Software, Version 7.3.1 LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
Built On     : Tue June 07 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5700/ws
Version      : 7.3.1
Label        : 7.3.1

cisco NCS5700 (D-1563N @ 2.00GHz)
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
ios uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS-57B1-5DSE-SYS Fixed Scale HW Flexible Consumption Need Smart Lic
```

The following example shows the version information for a GISO image. The customer label is appended to the `Label` field in the GISO image:

NCS 5500 Series:

```
Router#show version
Cisco IOS XR Software, Version 7.5.2 LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
```

```
Built On     : Tue June 07 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5500/ws
Version      : 7.5.2
Label        : 7.5.2-Customer_Label

cisco NCS5500L (D-1563N @ 2.00GHz)
cisco NCS-55A1-36H-S (D-1563N @ 2.00GHz) processor with 32GB of memory
ios uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS-55A1-36H-S Fixed Scale HW Flexible Consumption Need Smart Lic
```

NCS 5500 Series:

```
Router#show version
Cisco IOS XR Software, Version 7.3.1 LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
Built On     : Tue June 07 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5700/ws
Version      : 7.3.1
Label        : 7.3.1-Customer_Label

cisco NCS5700 (D-1563N @ 2.00GHz)
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
ios uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS-57B1-5DSE-SYS Fixed Scale HW Flexible Consumption Need Smart Lic
```

You can also use the `get` RPC on the `install.version` data model.

Step 2 View the active packages.

Example:

NCS 5500 Series:

```
Router#show install active summary
Mon Jun  6 04:18:26.684 UTC
Active Packages:    XR: 145    All: 1157
Label:              7.5.2
Software Hash:      28dd70ef227aeca3d3fd3ecf8d1792a4f51fabb299ec7d38725869575fd9cfaf

Optional Packages                                                  Version
-------------------------------------------------- --------------------------
xr-bgp                                                        7.5.2v1.0.0-1
xr-ipsla                                                      7.5.2v1.0.0-1
xr-is-is                                                      7.5.2v1.0.0-1
xr-lldp                                                       7.5.2v1.0.0-1
xr-mcast                                                      7.5.2v1.0.0-1
xr-mpls-oam                                                   7.5.2v1.0.0-1
xr-ncs5500l-mcast                                             7.5.2v1.0.0-1
xr-ncs5500l-netflow                                           7.5.2v1.0.0-1
xr-netflow                                                    7.5.2v1.0.0-1
xr-ospf                                                       7.5.2v1.0.0-1
xr-perf-meas                                                  7.5.2v1.0.0-1
xr-perfmgmt                                                   7.5.2v1.0.0-1
xr-track                                                      7.5.2v1.0.0-1
```

NCS 5700 Series:

```
Router#show install active summary
Fri Mar  5 17:37:23.205 UTC
Active Packages:    XR: 156    All: 1214
Label:              7.4.1-LABEL
Software Hash:      28dd70ef227aeca3d3fd3ecf8d1792a4f51fabb299ec7d38725869575fd9cfaf
```

```
Optional Packages                                                               Version
--------------------------------------------------------------------------------------
xr-bgp                                                                  7.3.1v1.0.0-1
xr-cdp                                                                  7.3.1v1.0.0-1
xr-eigrp                                                                7.3.1v1.0.0-1
xr-ipsla                                                                7.3.1v1.0.0-1
xr-is-is                                                                7.3.1v1.0.0-1
xr-lldp                                                                 7.3.1v1.0.0-1
xr-mcast                                                                7.3.1v1.0.0-1
xr-mpls-oam                                                             7.3.1v1.0.0-1
xr-ncs5700-mcast                                                        7.3.1v1.0.0-1
xr-ncs5700-netflow                                                      7.3.1v1.0.0-1
xr-netflow                                                              7.3.1v1.0.0-1
xr-ospf                                                                 7.3.1v1.0.0-1
xr-perf-meas                                                            7.3.1v1.0.0-1
xr-perfmgmt                                                             7.3.1v1.0.0-1
xr-telnet                                                               7.3.1v1.0.0-1
xr-track                                                                7.3.1v1.0.0-1
xr-xcare                                                                7.3.1v1.0.0-1
```

You can also use the `get` RPC on the `install.packages.active.node` and the `install.packages.active.node.summary` data models.

To understand the data model structure and its arguments, see the Obtain Data Models for Install Operation topic.

Golden ISO images

The Golden ISO (GISO) image is a custom-built IOS XR software image that

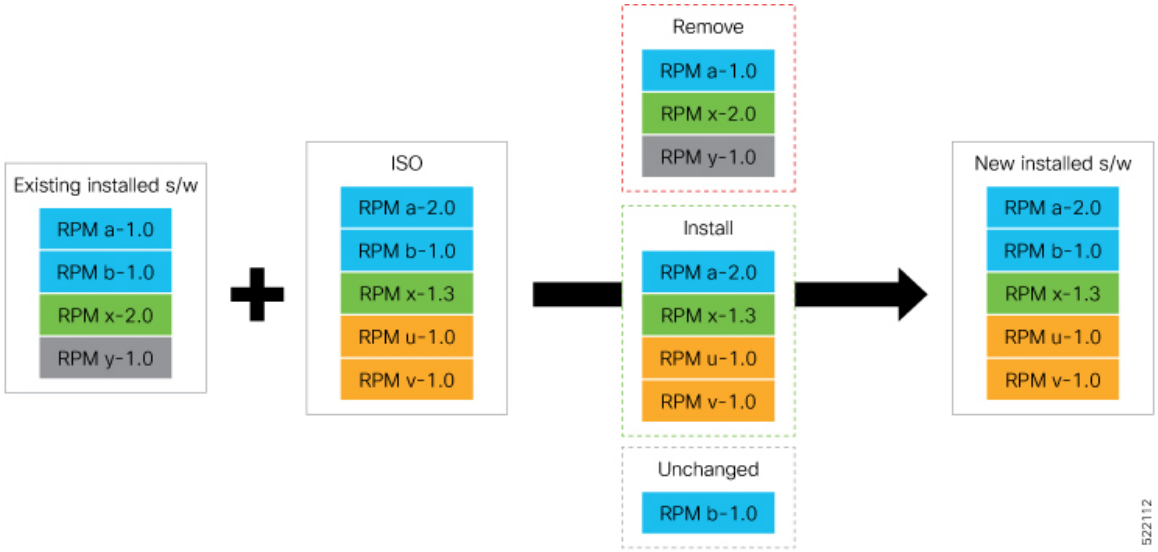
- is based on a given IOS XR version
- contains all mandatory packages
- includes optional packages and SMUs requested by the GISO image owner, and
- enables automated router boot using iPXE or system upgrade to a specified software version in a single operation.

Note When switching between Golden ISOs (GISOs) built on the same base version of IOS-XR, the **install replace** command automatically apples only the minimum required changes such as package additions, removals, and upgrades required for the transition.

Table 1: Feature History Table

Feature Name	Release Information	Description
Build a Golden ISO image using `gisobuild.py` tool	Release 7.6.1	This feature facilitates faster deployment by allowing you to build your GISO image without the need to contact Cisco support. You can now select the install files, add your RPMs, repackage them as a custom image, and install the image. In previous releases, you were required to contact Cisco to have your GISO built.

Figure 1: Golden ISO build process



Build a Golden ISO image

This section provides the options that help you build a GISO image.

Procedure

Step 1 Build a GISO image using one of the following options:

- **Option 1:** Contact Cisco Support to build the GISO image with the set of packages based on your requirement
- **Option 2:** Use the `gisobuild.py` tool to build the GISO. For information about the tool and how to use it, see https://github.com/ios-xr/gisobuild.

Step 2 Execute this command to install the GISO image built from previous step similar to installing any other ISO image.

Example:

```
Router# install replace /harddisk:/ncs540l-giso-x64.iso
```

Upgrade the System to Obtain Bug Fixes

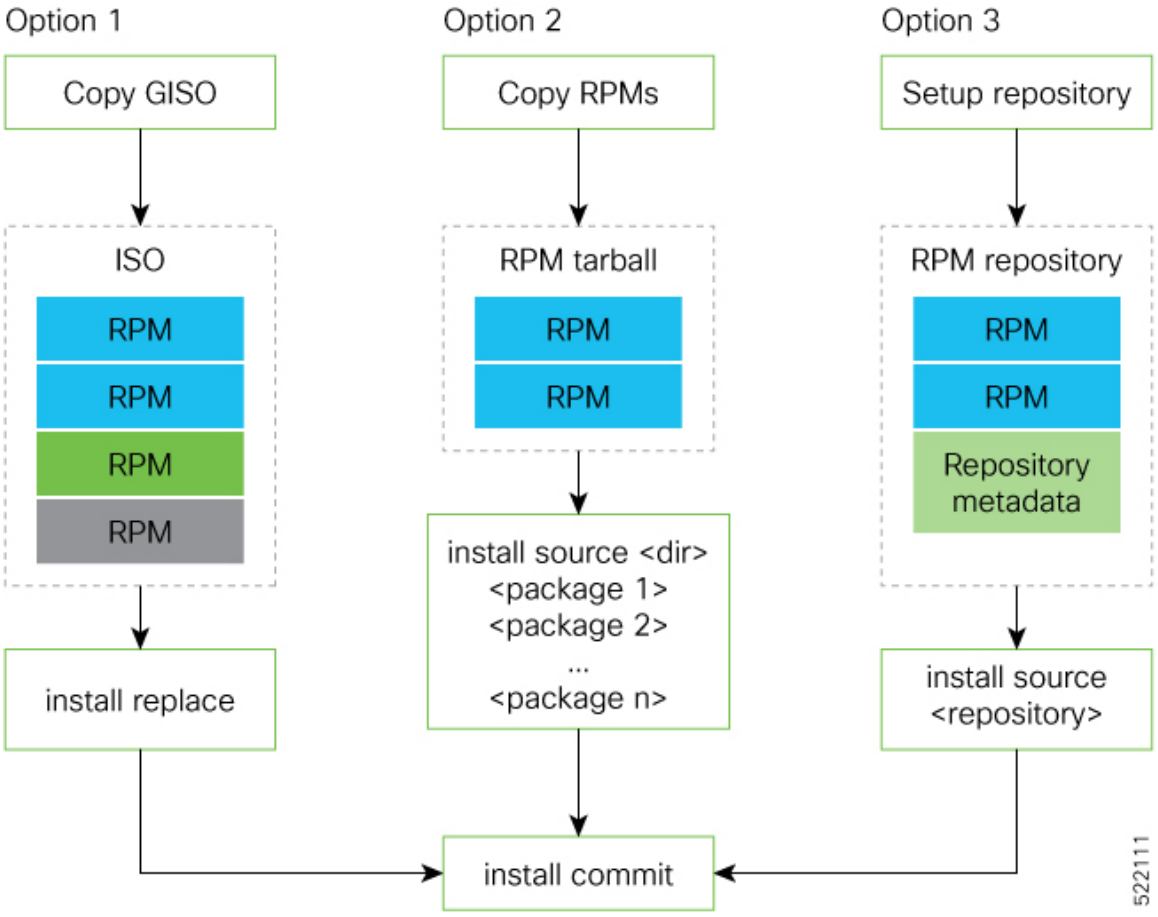
You can upgrade the system to obtain all available bug fixes or choose specific bug fix using bug ID.

Bug fixes are available as optional RPMs. The bug fixes replace packages in the base ISO without adding up to the image size. For example, even if you add 20 RPMs to the GISO, the GISO file size will remain the same as the initial ISO.

You can download the bug fix RPMs from the Cisco Software Download portal .

The `README` file provides the relevant information about the bug fix and also identifies the dependencies, if any, where other bug fix RPMs may be required for a complete fix.

The following image shows the options to install the bug fix RPMs.



The software is split into modular blocks and the package manager infrastructure computes the dependencies between the blocks. Each block of software has a top-level package and various partition-level packages. Bug

fixes that span multiple blocks may lead to creating multiple dependent packages that are built as part of earlier bug fixes.

Note We recommend that you leverage the GISO workflow. Contact Cisco Support to build a new GISO with the required bug fixes. The RPMs are present in the initrd, which is the initial RAM disk for the boot loader, and this requires that the package is signed by Cisco. You can install GISO using a single `install replace` operation. For more information about GISO, see the *Build a Golden GISO* section.

However, if you do not prefer using the GISO, here are a few alternative ways to install bug fixes:

- Create tarballs to install one or more bug fixes. For example, if you are installing bug fixes CSCxx11111, CSCyy22222 and CSCzz33333, you can use the individual tarball files and create a single tarball file.
- Use a Dandified Yum- or DNF repository to install, update, or remove relevant bug fixes. See, Create a repository to install IOS XR SMUs or optional packages.

Note The RPMs can be installed from the TAR file using CLI or Yang data model.

- CLI—
  - Packaging operation: `install package add source /harddisk:/ncs5700-<version>.tgz synchronous`
  - Packaging operation and atomic change: `install source /harddisk:/ncs5700-<version>.tgz synchronous`
- Yang Data Model—

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:
base:1.0" message-id="101">
<install-package-add xmlns=
"http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-act">
<source-type>tar</source-type>
<source>/misc/disk1/<platform>-<version>.tgz</source>
</install-package-add>
</rpc>
```

Note Use the RPM repository to harvest the benefits of package manager. The package manager queries the available packages, and downloads only those packages and their dependencies that are needed for installation.

Procedure

Step 1 View the list of available bug fixes.

Example:

NCS 5700 Series:

```
Router#show install fixes available
Bug Id            Packages                      Repository
-----------    ----------------------------  ----------------
CSCxx12345     xr-5700-core-7.3.1v1.0.1-1      <repository-name>

               xr-core-7.3.1v1.0.1-1           <repository-name>
```

Step 2 Install the bug fix or package using one of the following options:

- Install the package where the bug fix is applied.

  NCS 5700 Series:

  ```
  Router#install package upgrade xr-5700-core-7.3.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
  Packaging operation 1.1.1 started - xr-5700-core-7.3.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
  ```

  This task can also be accomplished using Cisco-IOS-XR-install-augmented-oper data model.

  Apply the changes.

  ```
  Router#install apply [reload | restart]
  ```

  Note
  To identify if you must reload or restart the system while applying the changes, use one of these two methods:

  - History of last transaction

    ```
    Router#show install history last transaction verbose
    2019-09-11 17:01:46 UTC    Transaction 3 started
    2019-09-11 17:01:46 UTC      Atomic change 3.1 started
    2019-09-11 17:01:46 UTC      Packaging operation 3.1.1 started
    2019-09-11 17:16:46 UTC    Transaction 3 complete

    Least impactful apply method: process restart
    ```

    The command also displays the information about the changes to files and processes because of the install operation, and the package operations carried out on each node.

  - Show install request

    ```
    Router:#show install request
    Wed Sep 14 02:53:21.525 PDT

    User request: install package abort latest
    Operation ID: 2.1.2
    State:        Failure since 2022-09-14 02:48:15 UTC-07:00
    Disk space check failed on nodes: 0/0/CPU0. Query 'show install history id 2.1.2 errors' for
     more details and next steps

    Current activity:    Await user input
    Time started:        2022-09-14 02:48:20 UTC-07:00

    The following actions are available:
        install package add
        install package remove
        install package upgrade
        install package downgrade
        install package abort latest
        install package abort all-since-apply
        install apply restart
        install apply reload
        install reimage
    ```

    NCS 5700 Series:

```
Router#show install request
User request: install package upgrade xr-5700-core-7.3.1v1.0.1-1
Operation ID: 2.1.1
State: Success

Current activity: Await user input
Time started:

The following actions are available:
install package add
install package remove
install package upgrade
install package downgrade
install package replace
install package rollback
install package abort latest
install package abort all-since-apply
install apply restart
install apply reload
```

Here, both `install apply restart` and `install apply reload` options are available. In this case, use `install apply restart` command because the impact on the system is the least. But when only an `install apply reload` option is available, then reload is the only option to apply the change.

- Install the optional package. Changes are applied automatically.

  Attention
  Automatic change may trigger a reload of the router depending on the package that is installed.

  ```
  Router#install source /harddisk:/files xr-<platform>-core-7.3.1v1.0.1-1
  ```

  Note
  Packages can also be installed using the package name.

  ```
  Router#install source /harddisk:/files  xr-<platform>-core
  ```

- This task can also be performed using YANG data models. Use `install` RPC on the Cisco-IOS-XR-install-act data model. Here is an example usage with an HTTP repository:

  ```
  <install>
     <packages>
       <packagename>pkg1</packagename>
     </packages>
     <source-type>http</source-type>
     <source><path-to-source></source>
  </install>
  ```

Step 3 View the state of the packaging operation.

Example:

```
Router#show install request
User request: install package upgrade xr-<platform>-core-<version> xr-core-<version>
Operation ID: 2.1.2
State:        In progress since

Current activity:    Initiate operation
Next activity:       Begin transaction
Time started:        2019-06-25 07:41:06

No per-location information.
```

Step 4 View the log to ensure that the installation is successful.

Example:

```
Router#show install log
2019-06-25 07:41:06 UTC    Transaction 1 started
2019-06-25 07:45:08 UTC    Upgrade (Success)
2019-06-25 07:45:08 UTC    xr-<platform>-core-<version>
2019-06-25 07:45:08 UTC    xr-core-<version>
2019-06-25 07:57:02 UTC    Atomic change 1.1 successfully applied by reload
```

Step 5 View the history of the install operation.

Example:

```
Router#show install history table
  Transaction             Atomic Change          Packaging Operations
--------------------  --------------------------  ----------------------------------
Id   Status          Id  Method   Status      Id  Operation   Inputs Status
--------------------  --------------------------  ----------------------------------
 1   In progress     1   Reload   Success      1   Upgrade        1  Success
```

The command can also be used to view more details if there is a failed operation.

Use **show install history id <operation-id>** command to filter the history of install information by ID. IDs are of the form `<transaction id>.<atomic id>.<packaging id>`.

```
Router#show install history id ?
  WORD Specify an operation ID (e.g. 1, 1.2, 1.2.3)
```

Use **show install history last** command to view the last packaging operation, atomic change, or transaction.

```
Router#show install history last ?
     atomic-change  Show the last atomic change
     package        Show the last packaging operation
     transaction    Show the last transaction
```

Step 6 After the operation is complete, verify that the packages `xr-5700-core-7.3.1v1.0.1-1` and `xr-core-7.3.1v1.0.1-1and xr-core-7.5.2v1.0.1-1` are installed and active.

Example:

Example:

NCS 5700 Series:

```
Router#show install active summary
Fri Mar  5 17:37:23.205 UTC
Active Packages:    XR: 156    All: 1214
Label:              7.4.1-LABEL
Software Hash:      28dd70ef227aeca3d3fd3ecf8d1792a4f51fabb299ec7d38725869575fd9cfaf
Optional Packages                                                              Version
-------------------------------------------------------------------------------------
xr-bgp                                                                    7.3.1v1.0.0-1
xr-cdp                                                                    7.3.1v1.0.0-1
xr-eigrp                                                                  7.3.1v1.0.0-1
xr-ipsla                                                                  7.3.1v1.0.0-1
xr-is-is                                                                  7.3.1v1.0.0-1
xr-lldp                                                                   7.3.1v1.0.0-1
xr-mcast                                                                  7.3.1v1.0.0-1
xr-mpls-oam                                                               7.3.1v1.0.0-1
xr-ncs5700-mcast                                                          7.3.1v1.0.0-1
xr-ncs5700-netflow                                                        7.3.1v1.0.0-1
xr-netflow                                                                7.3.1v1.0.0-1
xr-ospf                                                                   7.3.1v1.0.0-1
xr-perf-meas                                                              7.3.1v1.0.0-1
xr-perfmgmt                                                               7.3.1v1.0.0-1
```

```
xr-telnet                                                    7.3.1v1.0.0-1
xr-track                                                     7.3.1v1.0.0-1
xr-xcare                                                     7.3.1v1.0.0-1
```

Example:

```
Router#show install active summary
```

The version has changed. The version `1.0.1-1` indicates that the bug fix is installed.

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.active` operation using Cisco-IOS-XR-install-augmented-oper data model.

Step 7 Commit the changes for the changes to persist after a reload operation.

Example:

```
Router#install commit
```

Step 8 View the list of bug IDs for which fixes are committed.

Example:

```
Router#show install fixes committed
```

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.committed` operation using Cisco-IOS-XR-install-augmented-oper data model.

Step 9 View the list of active bug fix RPMs.

Example:

```
Router#show install fixes active
```

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.active` operation using Cisco-IOS-XR-install-augmented-oper data model.

Remove a bug fix from Cisco IOS XR software

You can remove a bug fix that is causing issues or is no longer needed.

Before you begin

Warning Bug fixes that are prerequisites for other fixes can only be removed if the dependent bug fixes are removed.

Procedure

Use one of the following options to remove a bug fix from your IOS XR software version:

- If the bug fix to be removed was the most recently installed, and the device supports the **install rollback** feature, roll back using rollback ID
  - **a.** Identify the rollback ID for the bug fix you want to remove.

b. Use the rollback process to return your software to a previous stable version using the rollback ID.

- Build a custom Golden ISO (GISO) image

a. Use the `gisobuild.py` tool to create a custom GISO image that excludes the unwanted bug fix and includes any required fixes.

b. Install the custom GISO image to update your system.

The bug fix is removed from your system using the selected method.

Roll back software to a previously saved installation point

You can roll your system software back to a previous version. This could be used to discard an ongoing install operation, or to undo an install operation that has already been committed. After each commit operation, the system saves a record of the committed software packages. Each record is a restoration point, and is assigned a unique ID. This ID is known as a rollback ID. You can use the rollback ID to roll back the software to a restoration point associated with this ID. Up to 900MB of space is allowed for rollback points, instead of a specific number of rollback points.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Rollback changes with simplified install process	Release 25.3.1	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Compatibility; Native] With the simplified install process that enhances upgrade robustness and scalability between IOS XR versions, rollback packages are no longer available after a release upgrade. You can continue to use the **install rollback** command to reverse operations within the same XR release, and existing rollback commands remain available for reverting operations involving multiple SMUs or optional packages.

Feature Name	Release Information	Feature Description
Roll back to a previously saved installation point	Release 7.4.1	A maximum of 900MB of disk space is used to store all rollback points. You can delete older rollback points to make space for newer or smaller rollback points such as, SMUs. This feature introduces the following commands: • **install commit description**—sets the description for a rollback ID • **install label id** *id* **description** *description*—adds a new description or overwrites the description of the specified rollback ID. The following command is updated to include the keyword, **oldest** *n*: • **clear install rollback oldest** *n*—deletes the specified number of rollback points

Note

- Use rollback ID 0 to roll back to the software that was present after the system booted for the first time.
- If you commit an install transaction using the **install commit** command, the GISO ZTP configuration is saved along with the rest of the software changes. This means that if you use the **install rollback** or **install package rollback** command to revert the software to the state of a previous transaction, the GISO ZTP configuration is also reverted to its previous state. To undo this install operation, as well as the change in GISO ZTP configuration, use the **install package abort** command. If there is no GISO ZTP configuration saved at the end of the install transaction, the existing GISO ZTP configuration is reverted to the previous state when the rollback operation of that transaction is applied.

Roll back Cisco IOS XR software using a rollback ID

This procedure helps you rollback your software using a rollback ID.

Procedure

Step 1 View the list of available rollback IDs.

Example:

```
Router# show install rollback list-ids
```

Step 2 Explore the main packages that can be installed if you roll the software back to the specific rollback ID.

Example:

```
Router# show install rollback id <id>
```

Step 3 View the relative changes that are made to the currently installed software if it is rolled back to a rollback ID.

Example:

```
Router# show install rollback id <id> changes
```

To perform these tasks using data models, use the `get` RPC on the Cisco-IOS-XR-install-augmented-oper data model.

```
<rpc>
  <get>
   <filter type="subtree">
      <install xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-oper">
      <rollback/>
     </install>
   </filter>
  </get>
</rpc>
```

Step 4 Roll back to the software associated with the specific rollback ID.

Example:

```
Router# install rollback <id> [commit]
```

If you want to apply the change and roll back to the associated rollback ID, commit the change. You can also include the keyword `noprompt` in the command to enable the system to bypass your permission to reload the router.

Attention
This roll back operation installs the previous software and also applies the change automatically. This may reload the router depending on the package that is rolled back.

Alternatively, use the **install package rollback** command to only roll back the package but not apply the changes. You can check whether the router will reload or restart if you apply the change using the **show install history last transaction verbose** command or **show install request** command. Based on the command output, you can take the appropriate action using the **install apply reload | restart** command to either reload or restart the system. Use the **install commi**t command to commit the transaction.

To perform this task using data models, use the `install-rollback` RPC on the Cisco-IOS-XR-install-augmented-oper data model.

```
<rpc>
 <install-rollback xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-act">
  <commit>true</commit>
   <transaction-id>0</transaction-id>
```

```
 </install-rollback>
</rpc>
```

To understand the data model structure and its arguments, see the Access the Install-Related Data Model.

Step 5 Commit the operation.

Example:

```
Router#install commit
```

Telemetry Support for Install Operations

Table 3: Feature History Table

Feature Name	Release Information	Description
Stream Telemetry Data about Install Operations	Release 7.5.2	You can stream telemetry data for install-related details such as active and committed packages, view the progress of install operations, retrieve the image version, and view the error messages with recovery information when an operation fails.

To stream telemetry data that is related to software installation, you must create subscriptions to the sensor paths in the YANG data models. See *Obtain Data Models for Install Operation* for the list of supported data models. For information about establishing a telemetry session and creating subscriptions, see the *Telemetry Configuration Guide for Cisco NCS 5500 Series Routers*.

Stream Telemetry Data About	Description	YANG Path
Summary of active packages	Data is streamed after a successful **apply** operation. An active package is the software currently running on the system.	`Cisco-IOS-XR-install-oper: install/packages/active/summary`
Summary of committed packages	Data is streamed after a successful **commit** operation. A package that is committed remains active following a system reload.	`Cisco-IOS-XR-install-oper: install/packages/committed/summary`
Status of the last request operation	Data is streamed when starting a new request and also when entering an `idle` state. If the operation has failed, this includes error messages along with recovery state.	`Cisco-IOS-XR-install-oper: install/request`
Image version and GISO label	Data is streamed after a successful **apply** operation.	`Cisco-IOS-XR-install-oper: install/version`

Stream Telemetry Data About	Description	YANG Path
Packaging information	Data is streamed at the start and end of a packaging operation.	`Cisco-IOS-XR-install-augmented-oper: install/history/latest-packaging-operation`
Atomic information	Data is streamed at the start and end of **apply** operation.	`Cisco-IOS-XR-install-augmented-oper: install/history/latest-atomic-change`
Transaction information	Data is streamed at the start, in progress, and end of a **commit** operation. **Note** After a transactional rollback, some of the data such as summary of active packages, image version can change. However, telemetry events are not sent after the reload operation.	`Cisco-IOS-XR-install-augmented-oper: install/history/latest-transaction`

Caveats

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

The caveats in 25.3.1 release are:

- CSCwo09365: FPDs not upgraded prior to install operation for upgrade to 25.3.1+ (NCS 5700).
- 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 4: Upgrade caveats

From	To	Bridge SMUs required (CSCwm77418)	Caveats
7.10.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
7.11.2 , 7.11.21	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
24.1.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
24.2.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
24.2.21	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365

From	To	Bridge SMUs required (CSCwm77418)	Caveats
24.3.1	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
24.3.2	25.3.1	Yes	CSCwq98264, CSCwq98275, CSCwo09365
24.3.20	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
24.4.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
24.4.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.1.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.1.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.2.1	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.2.2	25.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365

Table 5: Downgrade caveats

From	To	Target SMUs required (CSCwm77418)	Caveats
25.3.1	7.10.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	7.11.2 , 7.11.21	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.1.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.2.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.2.21	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.3.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.3.2	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.3.20	Yes	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.4.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	24.4.2	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	25.1.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	25.1.2	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	25.2.1	No	CSCwq98264, CSCwq98275, CSCwo09365
25.3.1	25.2.2	No	CSCwq98264, CSCwq98275, CSCwo09365

Release 7.10.1

Table 6: Upgrade caveats

From	To	Bridge SMUs required	caveats
7.5.2	7.10.1 and later	Yes	1*, 2*
7.6.1	7.10.1 and later	Yes	1*, 2*
7.6.2	7.10.1 and later	None	1*
7.7.1	7.10.1 and later	None	1*
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.

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.

These downgrade caveats are applicable for Release 7.10.1 and later.

Table 7: Downgrade caveats

From	To	Target SMUs required	Caveats
7.10.1 and later	7.5.2	Yes	***, A*, B*

From	To	Target SMUs required	Caveats
7.10.1 and later	7.6.1	Yes	***, A*, B*
7.10.1 and later	7.6.2	Yes	***, A*, B*
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.
- 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.
- PXE recovery is required if the image downgrading isn’t bootable.

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.

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

View Features and Capabilities Supported on a Platform

Table 8: Feature History Table

Feature Name	Release Information	Description
View Features and Capabilities Supported on a Platform	Release 7.5.2	This functionality displays a list of supported and unsupported features and their capabilities in a release for your router. With this feature, you are better equipped to plan your network configuration with features annotated for their support information. This feature introduces the **show features** command.

This feature provides an answer to the question `Is feature X supported on my router?`

You can determine whether a feature and their capabilities are supported on your router for the release. The support information is based on the release and platform-specific data such as platform variants, RP, or LC present on the router.

Note In Cisco IOS XR Software Release 7.5.2, only the capabilities for Access Control List (ACL) feature is supported.

The functionality to determine the capabilities information is enabled by default when the supported release is installed on the router.

Use the **show features** command to view the list of supported features and their capabilities. The feature capabilities are displayed in a tree structure with notations for the support information. For example, in ACL, the capability to use compression to accommodate a large number of Access Control Elements (ACEs) is supported, whereas IPv6 ACL BNG does not have support data in Cisco IOS XR Software Release 7.5.2. This support information about the feature is represented with the following key in the tree structure:

Key	Capability Support Information	Description
X	Unsupported	The feature capability is not supported on the platform for the release
-	Supported	The feature capability is supported on the platform for the release
?	Support unknown	The support for the feature capability is unknown on the platform for the release. This data could be because the optional package for the feature is not installed on the router.
*	Support data not available	The support for the feature capability is not available on the platform for the release. This data could be because the feature may be specific to a line card that is not present on the router.

View the List of Supported Features

In this example, the supported features on the router are displayed.



Note In Cisco IOS XR Software Release 7.5.2, only the feature capabilities for Access Control List (ACL) are supported.

```
Router#show features
Fri June 3 19:16:58.298 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Cisco IOS XR
|--[-] XR Protocols
|  |--[-] XR Base Protocols
|  |  |--[-] Services
|  |  |  |--[-] Access Control List (ACL)
|  |  |  |  |--[-]  IPv6 ACL Support
|  |  |  |  |  |--[*] IPv6 ACL ABF Track
|  |  |  |  |  |--[*] IPv6 ACL BNG
|  |  |  |  |  |--[*] IPv6 ACL Chaining (Meta ACL)
|  |  |  |  |  |--[-] IPv6 ACL Common ACL
|  |  |  |  |  |--[-] IPv6 ACL Compression
|  |  |  |  |  |--[*] IPv6 ACL Default ABF
|  |  |  |  |  |--[*] IPv6 ACL Fragment
|  |  |  |  |  |--[-] IPv6 ACL ICMP Off
|  |  |  |  |  |--[-] IPv6 ACL ICMP Protocol
|  |  |  |  |  |--[-] IPv6 ACL Interface Statistics
|  |  |  |  |  |--[-] IPv6 ACL Log Rate
|  |  |  |  |  |--[-] IPv6 ACL Log Threshold
|  |  |  |  |  |--[-] IPv6 ACL Logging
|  |  |  |  |  |--[-] IPv6 ACL MIB
|  |  |  |  |  |--[-] IPv6 ACL Object Groups (Scale)
|  |  |  |  |  |--[-] IPv6 ACL Police
|  |  |  |  |  |--[-] IPv6 ACL Priority
|  |  |  |  |  |--[*] IPv6 ACL Protocol Range
|  |  |  |  |  |--[-] IPv6 ACL Set Qos-Group
|  |  |  |  |  |--[-] IPv6 ACL Set TTL
|  |  |  |  |  |--[-] IPv6 ACL TCP Flags
|  |  |  |  |  |--[-] IPv6 ACL TTL Match
|  |  |  |  |  |--[-] IPv6 ACL UDF
|  |  |  |  |--[-] ES-ACL Support (L2 ACL)
|  |  |  |  |--[-] IPv4 ACL Support
|  |  |  |  |  |--[-] IPv4 ACL  Set Qos-group
|  |  |  |  |  |--[*] IPv4 ACL ABF Track
|  |  |  |  |  |--[*] IPv4 ACL BNG
|  |  |  |  |  |--[*] IPv4 ACL Chaining (Meta ACL)
|  |  |  |  |  |--[-] IPv4 ACL Common ACL
|  |  |  |  |  |--[-] IPv4 ACL Compression
|  |  |  |  |  |--[*] IPv4 ACL Default ABF
|  |  |  |  |  |--[*] IPv4 ACL Fragment
|  |  |  |  |  |--[-] IPv4 ACL Fragment Flags
|  |  |  |  |  |--[-] IPv4 ACL ICMP Off
|  |  |  |  |  |--[-] IPv4 ACL ICMP Protocol
|  |  |  |  |  |--[-] IPv4 ACL Interface Statistics
|  |  |  |  |  |--[-] IPv4 ACL Log Rate
```

```
|  |  |  |  |  |--[-] IPv4 ACL Log Threshold
|  |  |  |  |  |--[-] IPv4 ACL Logging
|  |  |  |  |  |--[-] IPv4 ACL MIB
|  |  |  |  |  |--[-] IPv4 ACL Object Groups (Scale)
|  |  |  |  |  |--[-] IPv4 ACL Police
|  |  |  |  |  |--[-] IPv4 ACL Priority
|  |  |  |  |  |--[*] IPv4 ACL Protocol Range
|  |  |  |  |  |--[-] IPv4 ACL Set TTL
|  |  |  |  |  |--[-] IPv4 ACL TCP Flags
|  |  |  |  |  |--[-] IPv4 ACL TTL
|  |  |  |  |  |--[-] IPv4 ACL UDF
|  |  |  |  |--[-] IPv4 Prefix-List
|  |  |  |  |--[-] IPv6 Prefix-List
```

View the List of Supported ACL Features

In this example, the capabilities for ACL features on the router are displayed.

```
Router#show features acl
Fri June 3 19:17:31.635 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
|--[-]  IPv6 ACL Support
|  |--[*] IPv6 ACL ABF Track
|  |--[*] IPv6 ACL BNG
|  |--[*] IPv6 ACL Chaining (Meta ACL)
|  |--[-] IPv6 ACL Common ACL
|  |--[-] IPv6 ACL Compression
|  |--[*] IPv6 ACL Default ABF
|  |--[*] IPv6 ACL Fragment
|  |--[-] IPv6 ACL ICMP Off
|  |--[-] IPv6 ACL ICMP Protocol
|  |--[-] IPv6 ACL Interface Statistics
|  |--[-] IPv6 ACL Log Rate
|  |--[-] IPv6 ACL Log Threshold
|  |--[-] IPv6 ACL Logging
|  |--[-] IPv6 ACL MIB
|  |--[-] IPv6 ACL Object Groups (Scale)
|  |--[-] IPv6 ACL Police
|  |--[-] IPv6 ACL Priority
|  |--[*] IPv6 ACL Protocol Range
|  |--[-] IPv6 ACL Set Qos-Group
|  |--[-] IPv6 ACL Set TTL
|  |--[-] IPv6 ACL TCP Flags
|  |--[-] IPv6 ACL TTL Match
|  |--[-] IPv6 ACL UDF
|--[-] ES-ACL Support (L2 ACL)
|--[-] IPv4 ACL Support
|  |--[-] IPv4 ACL  Set Qos-group
|  |--[*] IPv4 ACL ABF Track
|  |--[*] IPv4 ACL BNG
|  |--[*] IPv4 ACL Chaining (Meta ACL)
|  |--[-] IPv4 ACL Common ACL
|  |--[-] IPv4 ACL Compression
|  |--[*] IPv4 ACL Default ABF
|  |--[*] IPv4 ACL Fragment
|  |--[-] IPv4 ACL Fragment Flags
```

```
|  |--[-] IPv4 ACL ICMP Off
|  |--[-] IPv4 ACL ICMP Protocol
|  |--[-] IPv4 ACL Interface Statistics
|  |--[-] IPv4 ACL Log Rate
|  |--[-] IPv4 ACL Log Threshold
|  |--[-] IPv4 ACL Logging
|  |--[-] IPv4 ACL MIB
|  |--[-] IPv4 ACL Object Groups (Scale)
|  |--[-] IPv4 ACL Police
|  |--[-] IPv4 ACL Priority
|  |--[*] IPv4 ACL Protocol Range
|  |--[-] IPv4 ACL Set TTL
|  |--[-] IPv4 ACL TCP Flags
|  |--[-] IPv4 ACL TTL
|  |--[-] IPv4 ACL UDF
|--[-] IPv4 Prefix-List
|--[-] IPv6 Prefix-List
```

View the List of Supported ACL Features for Specific RP

In this example, the capabilities for ACL features on the RP location `0/RP0/CPU0` are displayed.

```
Router#show features acl detail location 0/RP0/CPU0
Fri June 3 19:15:49.889 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
    Cisco provides basic traffic filtering capabilities with access control
    lists (also referred to as access lists). User can configure access
    control lists (ACLs) for all routed network protocols to filter protocol
    packets when these packets pass through a device. User can configure
    access lists on your device to control access to a network, access lists
    can prevent certain traffic from entering or exiting a network.
|--[-]  IPv6 ACL Support
|       IPv6 based ACL is a list of source IPv6 addresses that use Layer 3 or
|       Layer 4 information to permit or deny access to traffic. IPv6 router
|       ACLs apply only to IPv6 packets that are routed.. A filter contains the
|       rules to match the packet matches, the rule also stipulates if the
|       packet should be permitted or denied.
|  |--[*] IPv6 ACL ABF Track
|  |      IPv6 ACL ABF Track allows the user to configure a rule with track as
|  |      nexthop inside the ACL rule . ACL Based Forwarding (ABF) denotes the
|  |      ability to forward packets to another next hop router based on the
|  |      criteria defined in the rule. Track takes precedence over VRF and
|  |      IP, if present in the nexthop
|  |--[*] IPv6 ACL BNG
|  |      IPv6 ACL BNG is an ACL subscriber BNG feature. It allows the use of
|  |      ACL on dynamic template.
|  |--[*] IPv6 ACL Chaining (Meta ACL)
|  |      IPv6 ACL Chaining (Meta ACL) allows the user to apply more than one
|  |      ACL on the interface.  is known as Meta ACL or ACL chaining.
|  |--[-] IPv6 ACL Common ACL
|  |      IPv6 ACL Common allows the user to apply the ACL on the interface
|  |      using the common keyword. Using this feature the ACL won't be
|  |      applied to the specific interface but it will be common to th entire
|  |      NPU to which the interface belongs.
|  |--[-] IPv6 ACL Compression
|  |      IPv6 ACL Compression allows the user to apply the ACL on the
```

```
|   |      interface using a compression level. This helps in reducing the
|   |      hardware resources needed to program the ACL.
|   |--[*] IPv6 ACL Default ABF
|   |      IPv6 ACL Default ABF allows the user to configure a rule with
|   |      default nexthop inside the ACL rule . ACL Based Forwarding (ABF)
|   |      denotes the ability to forward packets to another next hop router
|   |      based on the criteria defined in the rule
|   |--[*] IPv6 ACL Fragment
|   |      IPv6 ACL Fragment allows the user to configure a rule with fragment
|   |      inside the ACL rule and use it as a match criteria to filter traffic.
|   |--[-] IPv6 ACL ICMP Off
|   |      IPv6 ACL ICMP Off allows the user to not genearte the ICMP error
|   |      message on a deny action. When configured it will not send the
|   |      packet to FIB to generate ICMP error message.
-------------------------- Truncated for Brevity --------------------------
```

Deprecated commands

The following table lists deprecated commands along with their respective releases.

Table 9: Deprecated commands

Deprecated command	Release deprecated	Description
show install packages	Release 26.3.1	The **show install packages** family of commands including **show install packages info**, **show install packages search**, and **show install packages provides** are deprecated.
show install fixes deactivate	Release 26.3.1	To remove or deactivate a bug fix, see Deactivation of bug fixes.

Deactivation of bug fixes

To deactivate or remove a bug fix, use one of the following workflows:

- If there was a previous point where the same version of XR was loaded without the bug fix, revert to that point using the **install rollback** command. Use **show install rollback ?** to list the commands you can use to identify a suitable rollback point.
- If a suitable previous gISO is available without the bug fix, install it using the **install replace** command.
- If there is no previous point with the desired set of bug fixes, build a new gISO.

Note If the gISO build fails or the "bad bugfix" is still included, the set of desired fixes is not feasible. In this case, contact Cisco support to obtain a new version of the bad bug fix.