

Install Owner and Partner RPMs using IOS XR Install Infrastructure

This chapter describes how to install and manage Owner and Partner RPMs using the IOS XR install infrastructure.

This document is intended for network operators who want to install and manage proprietary Owner and Partner RPMs on devices running the Cisco IOS XR software. It assumes that these users are familiar with the basic concepts and commands of IOS XR and docker.

This chapter includes these sections:

- Owner and partner RPMs, on page 1
- Third-party unsigned RPMs, on page 9
- Troubleshooting Installation Failures, on page 11

Owner and partner RPMs

Owner RPMs are RPMs created by Cisco customers, or by other third parties. Cisco's customer (also known as the Owner) is responsible for the content and GPG-based signing of these RPMs as needed.

Partner RPMs are RPMs created by Cisco partners. These are supplied by Cisco and are signed with Cisco-managed security keys.

The owner and partner RPMs are installed as docker container images that run on the router.

The following steps provide the high level overview of the end-to-end signed owner RPM secure onboarding:

1. Owner signed RPM (docker image) in GISO or standalone needs owner's GPG keys to validate the RPM packages.
2. Owner's GPG keys are onboarded through secure workflow using key packages (explained in later sections).
3. Validation of the said key packages needs owner's public keys installed on the device.
4. Owner's public keys are onboarded on to the device using the ownership certificate (OC) or ownership voucher (OV) workflow as part of device ownership.
5. The chain of trust resides with Cisco through Ownership Vouchers.
6. The owner and partner RPMs are managed as docker container images using Cisco App Manager that are then run on the router. For more information, see the Application Hosting Configuration Guide.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Signature verification for owner RPMs using owner public keys	Release 26.1.1	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) This feature ensures integrity of owner RPMs and validates the authenticity of these RPMs by enabling the router to securely verify the owner RPM signatures using owner public keys onboarded on to the router. With this feature, you can now control whether or not to enable signature verification for owner RPMs based on defined security postures. When the signature verification for owner RPMs is enabled, all owner RPMs must be verified prior to IOS XR package installation. This feature introduces these changes: CLI: • A new command, **show install rpmdb keys**, has been added. • A new keyword, **keys**, has been added to the **show install active** and **show install committed** commands.

Feature Name	Release Information	Feature Description
Install Owner and Partner RPMs using IOS XR Install Infrastructure	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Install Owner and Partner RPMs Using IOS XR Install Infrastructure	Release 24.2.11	You can now use the existing IOS XR install infrastructure to install your proprietary Owner and Partner RPMs. This enhancement streamlines the process of integrating third-party software seamlessly into the IOS XR environment, including bundling the owner and partner RPMs into a GISO. In previous releases, you could only install Owner and Partner applications using the Application Manager interface. This feature introduces the keyword **skip-implicit-owner-packages-checks** in the following install commands: • **install package** • **install replace** • **install source** • **install rollback** • **install replace reimage**

Signature verification for owner RPMs

Starting from Cisco IOS XR Release 26.1.1, you can choose whether to enable signature verification for owner RPMs or not. When the signature verification for owner RPMs is enabled, all owner RPMs must be signed with GPG keys and the signatures are always verified. Owner RPM signatures are verified using owner public

keys onboarded on to the router. Signature verification validates the authenticity and integrity of the RPMs, ensuring that they are correct and unmodified.

You can control whether or not owner RPM signatures are verified, by setting the security posture to Low, Medium, or High.

The supported security postures are:

- High: Owner RPMs must always be signed. The owner RPMs are installed only after the signatures are verified.
- Medium: Owner RPM signatures are not verified, but owner RPMs must be installed explicitly.

  In an explicit installation, owner RPMs can either be named (**install package add** *owner-foo*) or the **skip-implicit-owner-packages-checks** option be added (**install package add** <*iso*>**skip-implicit-owner-packages-checks**).

  This is the default security posture.
- Low: Owner RPMs signatures are not verified.

You can request the router to change from one security posture to another security posture. For more information, see Security posture transitions, on page 5 .

From Cisco IOS XR Release 26.1.1, a new command, **show install rpmdb keys**, has been introduced and a new keyword **keys**,has been added to the **show install active** and **show install committed** commands.

Limitations and Guidelines

General Limitations and Guidelines

- Owner and partner RPMs can be installed only on route processors, and not on the line cards.
- Owner and partner RPMs are managed by App Manager, which is responsible for running the docker containers and handling notifications from Install.
- Owner and partner RPMs must install files only to the designated filesystem locations. These locations are `/opt/owner/` and `/opt/partner/` respectively.
- When installing Owner and partner RPMs, the maximum size of a GISO that can be used for bootstrap or when using the **install replace** command is 4GB.
- If you are upgrading from an IOS XR release that does not support installing the Owner or Partner RPMs (for example, upgrading from IOS XR Release 24.1.1 to IOS XR Release 24.2.11), owner and partner RPMs will not be installed automatically during the upgrade process. See the *Two-Step Upgrade Process for Installing Owner or Partner RPMs* section for more information.

Limitations and Guidelines for Owner RPMs

- Names of all Owner RPMs must begin with the string “owner-”.
- Owner RPMs can either be unsigned or signed with a non-Cisco key. Owner RPM signatures can either be verified or not verified during the installation of these RPMs.
- Owner RPMs must not include any RPM scriptlets, including pre-install and post-install scripts.
- You must request the installation of an Owner RPMs either by listing them explicitly or by including an additional parameter *skip-implicit-owner-packages-checks* in the install commands.

- During the network boot process using PXE or when booting from a USB drive, Owner RPMs are not automatically installed. This limitation arises because in these scenarios, there is no mechanism for the owner (Cisco customer) to convey consent for the installation of Owner RPMs. That is, there is no way for the owner to provide the *skip-implicit-owner-packages-checks* parameter.

  If you want to include Owner RPMs after booting from an ISO via PXE or USB, execute the **install replace** command with the ISO that contains the desired Owner RPM packages. This action incorporates the Owner RPM packages into your installation without affecting any other aspects of the system.

- To onboard owner RPMs on a new RP, the router either requires a separate OV in the tar file or a separate MASA service to create an ownership voucher (OV), which can added to the router using XR interfaces.

Limitations and Guidelines for Partner RPMs

- All Partner RPMs must be signed with a Cisco key; otherwise, they are treated as owner RPMs.
- Names of all Partner RPMs must begin with the string “partner-”.

Security posture transitions

A security posture transition is the process of changing a system’s operational security mode for a feature from one predefined level to another. Security posture transitions ensure integrity and protection of the system throughout the change.

The router blocks the change from a Low or Medium security posture to a High security posture, if there are any unverifiable packages.

Security posture transitions are performed using ownership vouchers (OVs). For more informtion, see Security profiles for Cisco IOS XR software.

Installing owner and partner RPMs

This process provides the workflow to install the owner and partner RPMs.

Summary

Owner RPMs created by Cisco customers or by other third parties, and partner RPMs created by Cisco partners are installed as docker container images that run on the router.

Workflow

These are the stages of the owner and partner RPMs installation:

1. Create an RPM containing the application (in the form of a docker container image), according to the requirements for owner and partner RPMs.



Note Starting from Cisco IOS XR 26.1.1, prior to installing owner RPMs, owner RPMs must be signed and the owner RPM signatures must be verified if the security posture is set to High.

You can also include the RPMs in the GISO using the appropriate Cisco tools.

2. Install the RPMs using the XR Install infrastructure, that is, by using any of the install commands, similar to installing IOS XR RPMs.

Note When installing an owner RPM and when the security posture is set to Medium, you must do one of the following:

- Option 1: Specify the name of the owner RPM explicitly.

  ```
  install package add owner-foo
  ```

- Option 2: Specify the **skip-implicit-owner-packages-checks** option.

  ```
  install replace [iso] skip-implicit-owner-packages-checks
  ```

3. Activate the RPMs (or let the system do this automatically if requested in the install operation).
4. Commit the transaction (or let the system do this automatically).

Install unsigned owner RPMs

This task helps you to install unsigned owner RPMs using different command options.

Procedure

Use one of the following options to install owner and partner RPMs:

- Execute the **install package add** command to add one or more packages to the active software without replacing the entire software.

  Example 1: This example shows how to install, activate, and commit an owner RPM individually.

  ```
  Router# install package add disk0:owner-app-24.2.11.x86_64.rpm activate commit
  ```

  Example 2: This example includes the `skip-implicit-owner-packages-checks` option, which is required only if the owner RPM name is not specified explicitly. This example is applicable to owner RPMs for which the security posture is set to Medium.

  ```
  Router# install package add skip-implicit-owner-packages-checks activate commit
  ```

- Execute the **install replace** command to replace the currently installed software with a new GISO that includes new owner RPMs.

  ```
  Router# install replace /harddisk:/8000-64-24.2.11-owner.iso activate commit
  Router# install replace skip-implicit-owner-packages-checks activate commit
  ```

- Execute the **install rollback** command to roll back to roll back the installation of owner and partner RPMs in the software associated with the specific transaction ID.

  This example includes the `skip-implicit-owner-packages-checks` option, which is required only if the owner RPM name is not specified explicitly.

  ```
  Router# install rollback skip-implicit-owner-packages-checks
  ```

The owner RPMs are installed successfully.

In addition to the commands used in this section, the install infrastructure also supports the following install operations to install owner RPMs – **install package remove**,**install package deactivate**,and **install source**.

For information about using the XR application manager to control the life cycle of installed owner or partner RPMs, see the *Customize Docker Run Options Using Application Manager* section in the *Application Hosting Configuration Guide for Cisco 8000 Series Routers*.

Install signed owner RPMs with or without signature verification

Before you begin

- The signing keys must be installed. For more information, see Install key packages on the router. The owner keys or signing keys can also be included in a GISO.
- Security posture is set to High, Medium, or Low.

This task provides the steps to install signed owner RPMs with or without verifying their signatures.

Procedure

Step 1 Create owner RPMs as per the owner RPM requirements.

Step 2 Create a GPG key or owner key anchored to the ownership certificate (OC) and install the owner keys on the router.

Step 3 Sign the owner RPMs with the GPG keys created in the previous step and install these keys on the router using the key package. For installing key packages on the router, see Install key packages on the router.

Step 4 Install the owner RPMs using one of the installation commands used in Install unsigned owner RPMs. The router installs the signed owner RPMs based on the security postures:

- If the security posture is High, the router verifies the owner RPMs signatures using the signing keys installed on the router and installs the owner RPMs upon successful signature verification.
- If the security posture is Medium, the router installs the signed owner RPMs explicitly without verifying the owner RPM signatures.

  An explicit installation requires the owner RPM name specified in the installation command. The **skip-implicit-owner-packages-checks** option is required in an explicit installation, if the owner RPM name is not specified in the installation command.
- If the security posture is Low, the router installs the signed owner RPMs implicitly without verifying the owner RPM signatures.

  An implicit installation operation installs the owner RPMs in the GISO using the **install replace**<*iso*> command, where the packages to be installed are not listed explicitly.

Install signed owner RPMs using GISO

This task helps you to install signed owner RPMs using GISO.

Procedure

Step 1 Create a key package with GPG keys used to sign the owner RPM and sign it with a key anchored in the OC.

For more information about key packages, OC, and OV, see *Provision Third-party Key Packages* and *Device Ownership* chapters in the *System Security Configuration Guide*

Step 2 Create an owner RPM and sign it with the GPG key obtained using the key package.

Step 3 Include both the owner RPM and the signed key package in a GISO.

Step 4 Execute the **install replace** command to install the GISO image.

Example:

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

Step 5 Starting from Cisco IOS XR Release 26.1.1, the router verifies the signature on the key package. On successful verification, the router temporarily installs the GPG keys on the router.

Step 6 Starting from Cisco IOS XR Release 26.1.1, if the security posture is High, the router installs the RPMs from the GISO and verifies the signature for owner RPMs using the key installed earlier.
The router aborts the install operation if the signature verification for key packages or owner RPMs fails.

Step 7 Activate the installed software.

Step 8 Commit the changes.

Note
If the router is reloaded or the install operation is aborted before committing the changes, the current active key is discarded.

The router stores the installed key after committing the changes.

The signed key packages and owner RPMs are installed and verified successfully. The router updates the file system with the new software.

For information about using the XR application manager to control the life cycle of installed owner or partner RPMs, see the *Customize Docker Run Options Using Application Manager* section in the *Application Hosting Configuration Guide for Cisco 8000 Series Routers*.

Install signed owner RPMs using USB or iPXE boot

This task helps you to install owner RPMs using USB or iPXE boot.

Procedure

Step 1 Create a key package with GPG keys used to sign the owner RPM and sign it with a key anchored in the OC.

For more information about key packages, OC, and OV, see *Provision Third-party Key Packages* and *Device Ownership* chapters in the *System Security Configuration Guide*.

Step 2 Create an owner RPM and sign it with the GPG key obtained using the key package.

Step 3 Include the partner RPM, owner RPM, and the signed key package in a GISO.

Step 4 Boot the router using USB or iPXE.

Step 5 Starting from Cisco IOS XR Release 26.1.1, the bootstrap software from GISO verifies the signature on the key package. On successful verification, the bootstrap software temporarily installs the GPG keys on the router.

Step 6 Starting from Cisco IOS XR Release 26.1.1, if the security posture is High, the bootstrap software from GISO installs the RPMs from GISO and verifies the signature for owner RPMs using the key installed earlier.
Failure to onboard keys or install owner or partner RPMs does not block the system boot; the system continues to come up.

Step 7 The router reloads and boots from the disk.

The signed key packages and owner RPMs are installed and verified successfully. The router updates the file system with the new software.

For information about using the XR application manager to control the life cycle of installed owner or partner RPMs, see the *Customize Docker Run Options Using Application Manager* section in the *Application Hosting Configuration Guide for Cisco 8000 Series Routers*.

Two-step upgrade process for installing owner or partner RPMs

If you are upgrading from an IOS XR release that does not support installing the owner or partner RPMs (any release prior to IOS XR Release 24.2.11), these RPMs will not be installed automatically during the upgrade process.

This is because the installation process governed by the previous releases does not have the functionality to handle the new RPMs.

To install Owner or partner RPMs, you must perform the upgrade in two distinct steps:

1. Upgrade from the previous release to IOS XR Release 24.2.11 without the owner or partner RPMs.
2. Perform an additional upgrade using the same newer version, that is, IOS XR Release 24.2.11 to IOS XR Release 24.2.11. This time explicitly by including the owner or partner RPMs.

These upgrade steps can be accomplished using the same ISO that contains the new version (for example, IOS XR Release 24.2.11) and the additional Owner or Partner RPMs. This two-step process ensures that the new features are properly implemented and that the Owner or Partner RPMs are correctly installed on your system.

Starting from Cisco IOS XR Release 26.1.1, the initial upgrade is done without owner RPMs, partner RPMs, and their respective keys. In the subsequent upgrade to Cisco IOS XR Release 26.1.1 includes the signed owner RPMs, signed partner RPMs, and their respective keys. After the initial upgrade, the security posture defaults to Medium so that the unsigned owner RPMs are installed upon request. However, during the second upgrade where if the security posture is set to High, the router installs and verifies the owner RPMs implicitly. If the security posture is set to Low during the second upgrade, the router installs unsigned owner RPMs implicitly.

Third-party unsigned RPMs

An unsigned third-party RPM is a software package that

- originates from a source other than the official operating system vendor
- lacks a digital signature, and

- prevents verification of its authenticity and integrity.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Third-party unsigned RPMs	Release 25.3.1	You can now install unsigned third-party RPMs on Cisco IOS XR systems, leveraging the existing install infrastructure and Golden ISO (GISO). This simplifies the deployment of custom or third-party containerized applications via the command-line interface, provided these unsigned RPMs adhere to Owner RPM conventions.

Guidelines for installing unsigned third-party RPMs

Use these guidelines when installing unsigned third-party RPMs.

- Third-party RPMs can be unsigned, and no signature verification is performed during installation for these RPMs.
- Do not include any RPM scriptlets, such as pre-install or post-install scripts.
- Third-party RPMs must install files only to `/opt/owner/` as per system conventions.
- Third-party unsigned RPMs are not installed implicitly during boot. To install third-party unsigned RPMs, use the **install replace** command with the **skip-implicit-owner-packages-checks** keyword.
- During PXE or USB boot, third-party owner RPMs are not installed automatically. Install them after initial boot using an explicit install command.
- The maximum supported GISO size, including third-party owner RPMs, is 4 GB.

Install third-party unsigned RPMs

Before you begin

- Ensure the RPM follows the owner RPM requirements:
  - The name starts with `owner-`.
  - It installs only to allowed locations.
  - It contains no scriptlets.
- The RPM file must be available in a GISO, which can reside in `disk0` or harddisk or an external repository.

Procedure

Step 1 Install all third-party unsigned RPMs included in the GISO using the **skip-implicit-owner-packages-checks** command.

Example:

```
Router# install replace /harddisk:/ncs5500-custom-25.3.1.iso skip-implicit-owner-packages-checks
commit
```

Step 2 Verify installation of third-party unsigned RPMs.

Example:

```
Router# show install active summary
Label : 25.3.1.06I-V1_TPA

    Active Packages: 15
        ncs5500-xr-25.3.1.06I version=25.3.1.06I [Boot image]
        ncs5500-isis-1.0.0.0-r253106I
        ncs5500-eigrp-1.0.0.0-r253106I
        ncs5500-li-1.0.0.0-r253106I
        ncs5500-xcare-1.0.0.0-r253106I
        ncs5500-mpls-te-rsvp-1.0.0.0-r253106I
        ncs5500-ospf-1.0.0.0-r253106I
        ncs5500-healthcheck-1.0.0.0-r253106I
        ncs5500-mgbl-1.0.0.0-r253106I
        ncs5500-mcast-1.0.0.0-r253106I
        ncs5500-lictrl-1.0.0.0-r253106I
        ncs5500-k9sec-1.0.0.0-r253106I
        ncs5500-mpls-1.0.0.0-r253106I
        owner-swan-0.1.3-25.3.1.x86_64 [TPA]
        owner-bonnet-0.1.2-25.3.1.x86_64 [TPA]
```

Troubleshooting Installation Failures

Normal Installation Failures (While IOS XR is Running)

If you encounter a failure while installing Owner or Partner RPMs during routine operations, such as **install replace** or **install package add**, the system treats this failure exactly like the failure to install any IOS XR RPMs.

The installation is aborted, and you must resolve the issue to continue. Standard recovery procedures for failed RPM installations should be followed in this case. For more information, see the *Troubleshoot Router Setup and Upgrade* chapter.

Bootstrap Installation Failures (During System Reimage)

If an Owner or Partner RPM fails to install during the bootstrap process, such as during a reimage from a disk, the system continues to boot, assuming all IOS XR software have been installed successfully.

After the system restarts, you will be alerted if any Owner or Partner RPMs were not installed. Use the **show install boot packages-not-installed** command for a list of uninstalled packages and the reasons they were not applied.

This distinction exists because the IOS XR system can fully boot and operate without the Owner or Partner RPMs, allowing you to troubleshoot the issue in a fully operational environment.

Inconsistencies in Owner/Partner RPMs Across Route Processors

If the system detects inconsistent versions of the IOS XR software on the active and standby RPs, the standby RP is repeatedly reimaged until the versions match.

However, if the system detects different versions of Owner or Partner applications on the active and standby route processors (RPs), you are required to address the discrepancy.

These are some of the use cases:

1. Use case 1:If the standby RP has Owner or Partner RPM versions different from that of an active RP, the standby RP is reimaged.
2. Use case 2: If both the standby RP and active RP have same Owner or Partner RPM versions, no further action is required.
3. Use case 3: If both the standy RP and active RP have different Owner or Partner RPM versions, syslogs are generated to notify users about different RPM versions.