

Perform System Upgrade and Install Feature Packages

You can execute the system upgrade and package installation processes using the **install** commands on NCS 1014. The processes involve adding and activating the ISO images (*.iso*) and feature packages (*.rpm*) on NCS 1014. You can accesss these files from a network server and then activate on NCS 1014. If the installed package or SMU causes any issue, you can uninstall it.

Note The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

Note We recommend that you collect the output of **show tech-support ncs1014** command before performing operations such as a reload or CPU OIR on NCS 1014. The command provides information about the state of the system before reload or before the CPU OIR operation is performed. This information is useful in debugging.

- Software and firmware compatibility matrix, on page 1
- Upgrade Software, on page 3
- View Supported Software Upgrade or Downgrade Versions, on page 5
- Software Upgrade and Downgrade Matrix , on page 8
- Install Packages and RPMs, on page 9
- Upgrade FPD, on page 14
- Verify if an FPD Upgrade is Required, on page 17
- Manual FPD Upgrade, on page 19
- Automatic FPD upgrade, on page 20

Software and firmware compatibility matrix

These tables provide the compatibility of FPGA firmware versions for each hardware type and supported software release.

Table 1: FPGA firmware compatibility

Hardware Type	FPGA	R7.11.1	R24.1.1	R24.2.11	R24.3.1	R24.4.1	R25.1.1	R25.2.1	R25.3.1	R25.4.1	R26.1.1
NCS1K14-2.4T-K9	CpuModFw	234.10	241.10	242.10	243.10	244.100	252.100	252.100	253.100	254.100	261.100
NCS1K14-24T-X-K9	CpuModFw	NA	241.10	242.10	243.10	244.10	251.100	252.100	253.100	254.100	261.100
NCS1K4-QXP-K9	CpuModFw	NA	241.10	242.10	243.10	244.10	251.100	252.100	253.100	254.100	261.100
NCS1K14-CCMD-16-C	CpuModFw	234.10	241.10	242.10	243.10	244.10	251.100	252.100	253.100	254.100	261.100
	OptModFw	18.03	20.02	20.02	20.02	20.02	20.02	20.02	20.02	254.100	20.02
NCS1K14-EDFA2	CpuModFw	NA	NA	NA	NA	NA	251.100	252.100	253.100	254.100	261.100
	OptModFw	NA	NA	NA	NA	NA	2.04	2.04	2.08	2.08	2.10
NCS1014	ADM-CHASSIS	0.21	0.21	0.21	0.21	0.21	0.21	0.21	0.21	0.21	0.21
	IoFpga	1.10	1.10	1.10	1.19	1.19	1.19	2.26	2.26	1.19	2.26
	IoFpgaGolden	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05
	SsdIntelSC2KB	1.20	1.20	1.20	1.20	1.20	1.30	1.30	1.30	1.30	1.30

Table 2: FPGA firmware compatibility for NCS1K4-AC-PSU-2 power supply unit

FPGA	R7.11.1	R24.1.1	R24.2.11	R24.3.1	R24.4.1	R25.1.1	R25.2.1	R25.3.1	R25.4.1	R26.1.1
PO-PriMCU	1.03	1.03	1.01	1.03	1.03	1.03	1.03	1.03	1.03	1.03
PO-SecMCU	1.05	1.05	1.01	1.05	1.05	1.05	1.05	1.05	1.05	1.05

Table 3: FPGA firmware compatibility for NCS1K14-CNTLR-K9 controller card

FPGA	R7.11.1	R24.1.1	R24.2.11	R24.3.1	R24.4.1	R25.1.1	R25.2.1	R25.3.1	R25.4.1	R26.1.1
ADM-DB	2.10	2.10	2.10	2.10	2.10	2.10	2.10	2.10	2.10	2.10
ADM-MB	2.30	2.30	2.30	2.30	2.30	2.30	2.30	2.10	2.30	2.30
BIOS	4.70	4.80	4.80	4.80	4.80	5.00	5.00	5.00	5.80	6.10
BIOS-Golden	4.50	4.50	1.72	4.50	4.70	4.70	4.70	4.70	4.70	4.70
CpuFpga	1.09	1.09	1.09	1.17	1.17	1.17	1.17	1.17	1.17	1.17
CpuFpgaGolden	1.03	1.09	1.09	1.09	1.09	1.09	1.09	1.09	1.09	1.09
SsdMicron5300	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
TamFw	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04
TamFwGolden	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04	9.04

Upgrade Software

Upgrading the software is the process of installing a new version of the Cisco IOS XR operating system on NCS 1014. NCS 1014 is preinstalled with the Cisco IOS XR image. However, you can install a new version to keep features up to date. You can perform the software upgrade operation using an ISO image from the XR mode.

Note NCS1014 and NCS1014 platform uses the same IOS-XR packaging image. Nomenclature of ISO image of IOS-XR base image example: "ncs1010-x64-[sw-rel-ver].iso'.

Note Upgrading from R7.11.1 to either R24.2.1 or R24.3.1 will raise the *DISASTER_RECOVERY_UNAVAILABLE_ALARM*. Postupgrade, this alarm clears automatically. For more information on the alarm, see *Troubleshooting Guide for Cisco NCS 1014*.

Before you begin

- Configure Management Interface
- Copy the ISO image to be installed either on the NCS 1014 hard disk or on a network server to which NCS 1014 has access.

Procedure

Step 1 Execute one of these commands:

Installs the new ISO image from the harddisk or from the network server. The install operation takes 20–40 minutes to complete.

- **install replace /harddisk:/***iso-image-name*
- **install package replace** *<ftp or http or https protocol>/package_path/ filename1 filename2 ...*

Note
The **install package replace** command upgrades the ISO image but doesn't reload the RP automatically. But the **install replace** command upgrades the ISO image and reloads the RP.

Example:

```
RP/0/RP0/CPU0:ios#install replace /harddisk:/ncs1010-x64-7.11.1.iso
Wed Nov 15 09:44:44.491 UTC
Once the packaging dependencies have been determined, the install operation may have to reload the
system.
If you want to control the timing of system reload, you must not continue, but use the 'install
package replace' command instead, followed by 'install apply'.
Continue? [yes/no]:[yes]
Install replace operation 1.1 has started
Install operation will continue in the background
```

```
.....................
.....................
ios con0/RP0/CPU0 is now available
```

Note
Boot time FPD upgrade happens before XR boot. All the FPDs belonging to the RP location are upgraded during the boot time FPD upgrade.

Note
Automatic Field Programmable Device(FPD) upgrade is enabled by default.. When the automatic FPD upgrade is enabled, the install operation also upgrades the FPDs (except the Golden FPDs and Power modules) that need to be upgraded.

Step 2 **show install request**

Displays the status of the install operation.

Example:

```
RP/0/RP0/CPU0:ios#show install request
Wed Nov 15 10:00:35.713 UTC
User request: install replace /harddisk://1010-x64-release.iso
Operation ID: 1.1
State:In progress since 2023-11-15 09:50:23 UTC
Current activity:    Package add or other package operation
Next activity:       Apply
Time started:        2023-11-15 09:55:24 UTC
Timeout in:          84m 43s
Locations responded: 0/1
Location          Packaging operation stage Notification Phase Clients responded
----------------- ------------------------- ------------------ -----------------
0/RP0/CPU0        Package operations        None in progress                N/A
```

When the install operation completes successfully, the device automatically reloads.

Note
In case of the **install package replace** command, you'll be prompted to enter the next command (**install apply reload** command).

Step 3 **install commit**

Commits the new ISO image.

Example:

```
RP/0/RP0/CPU0:ios#install commit
Wed Nov 15 10:38:00.592 UTC
Install commit operation 1 has started
Install operation will continue in the background
```

Note
It is the mandatory to commit the install successfully to upgrade the software, missing this step followed by any controller reload/restart/power cycle will result in rollback to previously installed committed software/RPM package version.

The *DISASTER_RECOVERY_UNAVAILABLE_ALARM* clears upon completion of the upgrade from R7.11.1 to R24.2.1 or R24.3.1.

Step 4 **show install committed**

Displays the committed package information.

Example:

```
RP/0/RP0/CPU0:ios#show install committed
Wed Nov 15 10:41:20.454 UTC
Software Hash: ec69dcceb81c0da69b297aa7de1d00f56b8aef52403c5e0ffe6e5db098bd83b8
Package                                                                      Version
-------------------------------------------------------------------------------------
xr-aaa                                                                 7.11.1.48Iv1.0.0-1
xr-acl                                                                 7.11.1.48Iv1.0.0-1
xr-apphosting                                                          7.11.1.48Iv1.0.0-1
xr-appmgr                                                              7.11.1.48Iv1.0.0-1
xr-bcdl                                                                7.11.1.48Iv1.0.0-1
xr-bfd                                                                 7.11.1.48Iv1.0.0-1
xr-bgp                                                                 7.11.1.48Iv1.0.0-1
xr-bgputil                                                             7.11.1.48Iv1.0.0-1
xr-bng-stubs                                                           7.11.1.48Iv1.0.0-1
xr-bundles                                                             7.11.1.48Iv1.0.0-1
```

View Supported Software Upgrade or Downgrade Versions

Your Cisco chassis comes preinstalled with IOS XR software. You either upgrade the software release to use new features and software fixes, or you downgrade the software. To leverage new features that are added or software fixes that are provided, it is important that you upgrade your software to a current version.

To help you select a Cisco IOS XR software release that aligns with Cisco-certified upgrade and downgrade paths, this feature provides answers to the following questions:

- What upgrade or downgrade releases are supported for the current release?
- I plan to upgrade from Release X to Release Y. Does my chassis support upgrade to Release Y?
- Are there any bridging SMUs that must be installed before I upgrade the software?

This feature provides a mechanism to determine whether the current release supports an upgrade to a target release. This task is run at the start of a software upgrade or downgrade through the **install replace** command. If the validation fails, the software upgrade is blocked, and the system notifies the reason for the failure. This feature allows you to proactively examine whether you can upgrade or downgrade to a certain release, saving time and effort involved in planning and upgrading the software.

The feature provides the following information to help you understand the prerequisites or limitations related to the specific software upgrade or downgrade:

- Required bridging SMU RPMs
- Blocking SMU RPMs
- Unsupported hardware
- Caveats or restrictions

You can overwrite the automatic validation using the **force** keyword in the **install replace** command. With this option, the system displays warning messages when the upgrade fails but does not block the software upgrade. Use the **force ?** keyword to understand any other impact to system functionalities apart from the disabling of this process that determines the supported releases for software upgrade or downgrade.

You can view the support information using the following **show** commands or through the operational data.

Command	Description
show install upgrade-matrix running	Displays all supported software upgrades from the current version according to the support data installed on the running system
show install upgrade-matrix iso *path-to-ISO*	Displays details about the software upgrade from the current version to the version of the target ISO according to the support data in both the running system and the ISO image
show install upgrade-matrix iso *path-to-ISO* **all**	Displays all supported software upgrades from any version according to the support data in the target ISO image
show install upgrade-matrix iso *path-to-ISO* **from-running**	Displays details about the software upgrade from the current version to the version of ISO according to the support matrices in both the running system and the target ISO image

View All Supported Software Upgrade from Running Version

The following example shows all supported releases for upgrade from the current version 24.1.1 on the chassis:

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix running
Fri Mar 15 12:53:23.715 IST
Matrix: XR version: 24.1.1, File version: 1.0, Version: N/A

The upgrade matrix indicates that the following system upgrades are supported from the
current XR version:

From       To         Restrictions
---------- ---------- ------------
24.1.1     7.11.1     -

Add the from and to versions to the end of the CLI command, for data on versions with
additional restrictions

For example, to display restrictions for the 24.1.1->7.11.1 upgrade, use
        'show install upgrade-matrix running 24.1.1 7.11.1'
```

Pre and Post-Upgrade Installation Health Checks

This section describes about of the pre and postupgrade Installation health check for routers.

Existing client-server framework notifies the subscribed clients to perform the precheck functionality.

The System health check infrastructure that is plugged to the install pre and postchecks phase of the system upgrade. This includes other existing install pre or postchecks.

Upgrade precheck:

- If single command upgrade is triggered either with a force option or is configured to skip checks, then health check is bypassed and a syslog entry added.

- When single command upgrade is triggered, install infra performs install specific prechecks. If the install prechecks pass, the system health check infra plug-in is invoked to check the overall system health.
- The health check infrastructure returns the health status during the installation.
- Single command upgrade continues on if the prechecks completes with no errors.
- If any errors are detected, then single command upgrade continues or terminates depending on the option that is selected for abort-on-precheck-failure.
- Single command upgrade postchecks before autocommit triggers based on the user selected level information.

Upgrade post check:

- Post checks are bypassed if force or config option is selected for single command upgrade.
- If install specific postchecks are completed sucessfully, then the system health check infra plug-in is invoked. If no errors are reported then the autocommit triggers.
- If any errors are detected, the abort-on option that is saved before the upgrade reload is used to either abort the single command upgrade or continue. This depends on the severity of the errors that are detected during post check.
- Summary of the pre and posthealth check is appended to the single command upgrade operation log.

Installation Profile Creation

Installation Profile is created to choose and alternate installation behavior. One default profile is created involving pre and postchecks. You can edit the install behavior to choose cases like terminate installation if precheck fails or revert after post installation check. You can also choose to continue installation despite failure in pre checks.

You can configure “enable or disable” options to run pre or post installation checks or “abort-on-failure” for pre checks, or "warn-on-failure" and “restore-to-v1” on post checks. To configure the Install profile, use the following commands:

config

install profile *profile_name* **pre-check***metric-name* **[enable | disable] [abort-on-failure | continue-on-failure | revert-on-failure]**

end

Following is a sample to display metric settings in the install profile.

```
RP/0/RP0/CPU0:ios#show install profile default
Fri Mar 15 11:29:35.381 IST
Profile Name : default
State : Enabled

Prechecks : Enabled
        communication-timeout   : Enabled       [ warn-on-failure ]
        config-inconsistency    : Enabled       [ error-on-failure ]
        process-resource        : Enabled       [ warn-on-failure ]
        process-status          : Enabled       [ warn-on-failure ]
        system-clock            : Enabled       [ warn-on-failure ]
        hw-monitoring           : Enabled       [ warn-on-failure ]
        lc-monitoring           : Enabled       [ warn-on-failure ]
        pci-monitoring          : Enabled       [ warn-on-failure ]
```

```
        wd-monitoring           : Enabled       [ warn-on-failure ]
        disk-space              : Enabled       [ error-on-failure ]
        upgrade_matrix          : Enabled       [ error-on-failure ]
        core-cleanup            : Disabled      [ NA ]
        file-cleanup            : Disabled      [ NA ]

Postchecks : Enabled
        communication-timeout   : Enabled       [ error-on-failure ]
        config-inconsistency    : Enabled       [ error-on-failure ]
        process-resource        : Enabled       [ error-on-failure ]
        process-status          : Enabled       [ error-on-failure ]
        system-clock            : Enabled       [ error-on-failure ]
        hw-monitoring           : Enabled       [ error-on-failure ]
        lc-monitoring           : Enabled       [ error-on-failure ]
        pci-monitoring          : Enabled       [ error-on-failure ]
        wd-monitoring           : Enabled       [ error-on-failure ]
```

Use the following configuration to report health check:

config

grpc local-connection

Netconf-yang agent

commit

The following is a sample to display health check states:

```
RP/0/RP0/CPU0:ios#show healthcheck internal states
Fri Mar 15 12:55:54.739 IST

 Internal Structure INFO

 Current state: Disabled

 Reason: Success

 Netconf Config State: Enabled

 Grpc Config State: Disabled

 Nosi state: Not ready

 Appmgr conn state: Invalid

 Nosi lib state: Not ready

 Nosi client: Valid client
```

Software Upgrade and Downgrade Matrix

This table lists the upgrade and downgrade paths supported for Cisco NCS 1014.

Upgrade Path			Downgrade Path		
Source Release	Destination Release	Bridge SMU	Source Release	Destination Release	Bridge SMU
• R7.11.1 • R24.1.1 • R24.2.11 • R24.3.1 • • R25.1.1		No		• R25.1.1 • • R24.3.1 • R24.2.11 • R24.1.1 • R7.11.1	No

Install Packages and RPMs

Complete this task to install additional packages or rpm files. The rpm files that need to be installed must be placed in a folder.

Note This task can be used to install SMUs as well.

Before you begin

- Configure and connect to the management interface. You can access the installable file through the management interface. For details about configuring the management interface, see Workflow for Install Process.
- Copy the package or rpm to be installed either on the NCS 1014 hard disk or on a network server to which NCS 1014 has access.

Procedure

Step 1 **install package add source /harddisk:/** *iso-image-name or rpm-folder-name*

Example:

```
RP/0/RP0/CPU0:ios#install package add source harddisk:/rpm
Wed Nov 15 18:10:14.784 UTC

Install add operation 2.1.2 has started
Install operation will continue in the background
```

```
RP/0/RP0/CPU0:ios#install package add source harddisk:/rpm/
Thu Apr 20 18:09:49.582 UTC
Install add operation 7.1.1 has started
Install operation will continue in the background
```

Ensure to add the respective packages or rpm files as appropriate. This operation may take time depending on the size of the files that are added. The operation takes place in an asynchronous mode. The **install package add source** command runs in the background, and the EXEC prompt is returned.

Step 2 **show install request**

Example:

```
RP/0/RP0/CPU0:ios#show install request

Thu Apr 20 18:13:00.720 UTC

User request: install package add source file:///harddisk:/rpm
Operation ID: 7.1.1
State:        Success since 2023-04-20 18:13:04 UTC

Current activity:    Await user input
Time started:        2023-04-20 18:13:04 UTC

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 replace reimage

Least impactful apply method: install apply restart
```

Displays the current status of the install operation.

Step 3 **install apply reload**

Example:

```
RP/0/RP0/CPU0:ios#install apply

Thu Apr 20 18:13:18.514 UTC
Once the packaging dependencies have been determined, the install operation may have to reload the
system.
If you want more control of the operation, then explicitly use 'install apply restart' or 'install
apply reload' as reported by 'show install request'.
Continue? [yes/no]:[yes] yes
Install apply operation 7.1 has started
Install operation will continue in the background
```

Enables NCS 1014 to reload.

Step 4 **show install request**

Example:

```
RP/0/RP0/CPU0:ios#show install request
Thu Apr 20 18:15:06.876 UTC

User request: install apply restart
Operation ID: 7.1
State:        Success since 2023-04-20 18:14:41 UTC

Current activity:    Await user input
Time started:        2023-04-20 18:14:41 UTC
```

```
The following actions are available:
install package add
install package remove
install package upgrade
install package downgrade
install package replace
install package rollback
install replace
install rollback
install source
install commit
install replace reimage
```

Displays the current status of the install operation.

Step 5 **install commit**

Example:

```
RP/0/RP0/CPU0:ios#install commit
Thu Apr 20 18:15:17.620 UTC
Install commit operation 7 has started
Install operation will continue in the background
```

Commits the package or rpm files.

Step 6 **show install request**

Example:

```
RP/0/RP0/CPU0:ios#show install request

User request: install commit
Operation ID: 2
State:        In progress since 2022-07-04 11:48:48 UTC

Current activity:    Commit transaction
Next activity:       Transaction complete
Time started:        2022-07-04 11:48:48 UTC

No per-location information.
```

Displays the current status of the install operation. The above output indicates that the install operation is in progress.

Example:

```
RP/0/RP0/CPU0:ios#show install request

User request: install commit
Operation ID: 2
State:        Success since 2022-07-04 11:50:32 UTC

Current activity:    No install operation in progress

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package replace
    install package rollback
    install replace
    install rollback
    install source
```

Displays the current status of the install operation. The above output indicates that the install operation is complete.

Step 7 **show install request**

Example:

```
RP/0/RP0/CPU0:ios#show install request

User request: install commit
Operation ID: 2
State:        Success since 2022-07-04 11:50:32 UTC

Current activity:    No install operation in progress

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package replace
    install package rollback
    install replace
    install rollback
    install source
```

Displays the current status of the install operation. The above output indicates that the install operation is complete.

Step 8 **show install active summary**

Example:

```
RP/0/RP0/CPU0:ios#show install active summary
Wed Nov 15 18:20:38.783 UTC
Active Packages: XR: 160 All: 1318
Label: 7.11.1.48I-Weekly
Software Hash: ec69dcceb81c0da69b297aa7de1d00f56b8aef52403c5e0ffe6e5db098bd83b8

Optional Packages                                  Version
-------------------------------------------------- ----------------------------
xr-bgp 7.11.1.48I                                  v1.0.0-1
xr-cdp 7.11.1.48I                                  v1.0.0-1
xr-cosm 7.11.1.48I                                 v1.0.0-1
xr-dt-sit 7.11.1.48I                               v1.0.0-1
xr-eigrp 7.11.1.48I                                v1.0.0-1
xr-healthcheck 7.11.1.48I                          v1.0.0-1
xr-ipsla 7.11.1.48I                                v1.0.0-1
xr-is-is 7.11.1.48I                                v1.0.0-1
xr-k9sec 7.11.1.48I                                v1.0.0-1
xr-license-util 7.11.1.48I                         v1.0.0-1
xr-lldp 7.11.1.48I                                 v1.0.0-1
xr-mpls-oam 7.11.1.48I                             v1.0.0-1
xr-netsim 7.11.1.48I                               v1.0.0-1
xr-olc 7.11.1.48I                                  v1.0.0-1
xr-ospf 7.11.1.48I                                 v1.0.0-1
xr-perfmgmt 7.11.1.48I                             v1.0.0-1
xr-rip 7.11.1.48I                                  v1.0.0-1
xr-telnet 7.11.1.48I                               v1.0.0-1
xr-tftp 7.11.1.48I                                 v1.0.0-1
xr-track 7.11.1.48I                                v1.0.0-1
```

Displays the list of active packages and rpm files.

Step 9 **show install committed summary**

Example:

```
RP/0/RP0/CPU0:ios#show install committed summary
```

```
Wed Nov 15 18:21:35.919 UTC
Committed Packages: XR: 160 All: 1318
Label: 7.11.1.48I-Weekly
Software Hash: ec69dcceb81c0da69b297aa7de1d00f56b8aef52403c5e0ffe6e5db098bd83b8

Optional Packages                    Version
---------------------------------------------------- ----------------------------
xr-bgp 7.11.1.48I                    v1.0.0-1
xr-cdp 7.11.1.48I                    v1.0.0-1
xr-cosm 7.11.1.48I                   v1.0.0-1
xr-dt-sit 7.11.1.48I                 v1.0.0-1
xr-eigrp 7.11.1.48I                  v1.0.0-1
xr-healthcheck 7.11.1.48I            v1.0.0-1
xr-ipsla 7.11.1.48I                  v1.0.0-1
xr-is-is 7.11.1.48I                  v1.0.0-1
xr-k9sec 7.11.1.48I                  v1.0.0-1
xr-license-util 7.11.1.48I           v1.0.0-1
xr-lldp 7.11.1.48I                   v1.0.0-1
xr-mpls-oam 7.11.1.48I               v1.0.0-1
xr-netsim 7.11.1.48I                 v1.0.0-1
xr-olc 7.11.1.48I                    v1.0.0-1
xr-ospf 7.11.1.48I                   v1.0.0-1
xr-perfmgmt 7.11.1.48I               v1.0.0-1
xr-rip 7.11.1.48I                    v1.0.0-1
xr-telnet 7.11.1.48I                 v1.0.0-1
xr-tftp 7.11.1.48I                   v1.0.0-1
xr-track 7.11.1.48I                  v1.0.0-1

---------------------------------------------------- ----------------------------
```

Displays the list of committed packages and rpm files.

Related Commands

The following commands can be used to track the status of the install operation.

Related Commands	Purpose
show install active	Displays the list of active packages.
show install committed	Displays the list of committed packages.
show install log	Displays the log information for the install operation. This information is used for troubleshooting in case of installation failure.
show install package	Displays the details of the packages that are added to the repository. Use this command to identify individual components of a package.
show install request	Displays the current status of the install operation.
show install which	Displays the package information on an installed file.

Upgrade FPD

A Field Programmable Device (FPD) refers to any programmable hardware device on a system which includes a Field Programmable Gate Array (FPGA). You can use the following tasks to verify and upgrade the FPDs of line cards, which are critical for chassis operation.



Note During the software upgrade, when the SSD is upgraded, the FPD goes into the RELOAD_REQ state, as displayed by the **show hw-module fpd** command. This behavior is expected because the updated SSD firmware can only be activated after reloading the specific SSD location mentioned in the **show hw-module fpd** output.

The following table lists the NCS 1014 FPDs that are distributed across Route Processor (RP), Power Modules (PM), Line Cards (LC), and Rack.

Table 4: NCS 1014 FPDs

Location	FPDs
RP	• ADM-DB • ADM-MB • BIOS • BIOS-Golden • CpuFpga • CpuFpgaGolden • SsdIntelS4510 • SsdIntelSC2KB • SsdMicron5300 • TamFw • TamFwGolden
PM0 and PM1	• PO-PriMCU • PO-SecMCU
LC	• CpuModFw • OptModFw

Location	FPDs
Rack	• ADM-CHASSIS • IoFpga • IoFpgaGolden • SsdIntelSC2KB

Golden FPDs serve as backup FPDs for the primary FPDs. For example, **BIOS-Golden** is the backup Golden FPD for the **BIOS** primary FPD. If a primary FPD is corrupted, NCS 1014 boots with the corresponding Golden FPD. The Golden FPDs cannot be upgraded.

Retrieve FPD Information

There are multiple types of FPDs for each type of module. The **show hw-module fpd** command provides information about each FPD.

```
RP/0/RP0/CPU0:ios#show hw-module fpd
Wed Nov 15 19:29:37.061 UTC

Auto-upgrade:Enabled
Attribute codes: B golden, P protect, S secure, A Anti Theft aware
                                                                 FPD Versions
                                                                 ==============
Location    Card type       HWver   FPD device     ATR Status   Running Programd Reload Loc
-------------------------------------------------------------------------------------------
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   ADM-DB             CURRENT    2.10  2.10    NOT REQ
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   ADM-MB             CURRENT    2.30  2.30    NOT REQ
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   BIOS S             CURRENT    4.70  4.70    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   BIOS-Golden      BS CURRENT          4.70    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   CpuFpga           S CURRENT    1.09  1.09    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   CpuFpgaGolden    BS CURRENT          1.09    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   SsdMicron5300     S CURRENT    0.01  0.01    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   TamFw             S CURRENT    9.04  9.04    0/RP0
0/RP0/CPU0 NCS1K14-CNTLR-K9  0.2   TamFwGolden      BS CURRENT          9.04    0/RP0
0/PM0      NCS1K4-AC-PSU     0.1   PO-PriMCU          CURRENT    2.04  2.04    NOT REQ
0/PM0      NCS1K4-AC-PSU     0.1   PO-SecMCU          CURRENT    2.06  2.06    NOT REQ
0/PM1      NCS1K4-AC-PSU     0.1   PO-PriMCU          CURRENT    2.04  2.04    NOT REQ
0/PM1      NCS1K4-AC-PSU     0.1   PO-SecMCU          CURRENT    2.06  2.06    NOT REQ
0/0/NXR0   NCS1K4-1.2T-K9    0.1   CpuModFw          S CURRENT   234.10 234.10  NOT REQ
0/0/NXR0   NCS1K4-1.2T-K9    0.1   OptModFw          S CURRENT    1.38  1.38    NOT REQ
0/1/NXR0   NCS1K14-2.4T-K9   0.1   CpuModFw          S CURRENT   234.10 234.10  NOT REQ
0/2/NXR0   NCS1K14-CCMD-16-C 0.1   CpuModFw          S CURRENT   234.10 234.10  NOT REQ
0/2/NXR0   NCS1K14-CCMD-16-C 0.1   OptModFw          S CURRENT     1.38 1.38    NOT REQ
0/3/NXR0   NCS1K4-1.2T-K9    0.1   CpuModFw          S CURRENT   234.10 234.10  NOT REQ
0/3/NXR0   NCS1K4-1.2T-K9    0.1   OptModFw          S CURRENT     1.38 1.38    NOT REQ
0/Rack     NCS1014           0.1   ADM-CHASSIS        CURRENT     0.21 0.21    NOT REQ
0/Rack     NCS1014           0.1   IoFpga            S CURRENT     1.10 1.10    NOT REQ
0/Rack     NCS1014           0.1   IoFpgaGolden     BS CURRENT          1.05    NOT REQ
0/Rack     NCS1014           0.1   SsdIntelSC2KB     S CURRENT     1.20 1.20    0/Rack
```

The following table describes the significant fields in the output of the **show hw-module fpd** command.

Table 5: Description of Fields in show hw-module fpd Command

Field	Description
Location	Location of the FPD.

Field	Description
Card type	PID of the modules such as chassis, card, CPU, and PSU.
HWver	Hardware version where the FPD resides.
FPD device	Name of the FPD.
ATR	Attribute codes. The possible values are: • B - Golden Image • S - Secure Image • P - Protect Image The attribute code of the primary FPDs is S and the Golden FPDs is BS.
Status	Status of the FPD. See Table 6: Description of FPD Status Values in show hw-module fpd Command Output, on page 16.
Running	FPD image version that has been activated and currently running in the FPD device.
Programd	FPD image version that has been programmed into the FPD device, but might not be activated.
Reload Loc	Indicates whether reload of the location is required or not.

The following table describes the possible values of the **Status** field in the output of the **show hw-module fpd** command.

Table 6: Description of FPD Status Values in show hw-module fpd Command Output

FPD Status	Description
NOT READY	The driver that owns the FPD device has not initialized the FPD client to handle this device.
CURRENT	FPD version is up-to-date and upgrade is not required.
NEED UPGD	Upgrade is required for this FPD. Check the output of the **show fpd package** command to determine the recommended FPD version.
UPGD PREP	FPD is preparing for upgrade.
IN QUEUE	Upgrade of this FPD is in queue.

FPD Status	Description
UPGD SKIP	FPD upgrade is not required. For example, • FPD version is up-to-date and compatible. • FPD image is protected.
UPGRADING	FPD upgrade has started and the driver has not reported the upgrade progress information yet.
%UPGD	Percentage of FPD upgrade completion.
RLOAD REQ	FPD upgrade is successful and the FPD must be reloaded for the new version to take effect.
UPGD FAIL	FPD upgrade has failed.Check the syslog for any timeout messages or any failure reported by the driver.
UPGD DONE	FPD upgrade is successfull.



Restriction The NCS 1014 does not support trunk FPD upgrade on the QXP card.

Verify if an FPD Upgrade is Required

Table 7: Feature History

Feature Name	Release Information	Feature Description
Automatic FPD Upgrade Support for Coherent Interconnect Module 8	Cisco IOS XR Release 24.3.1	The Coherent Interconnect Module 8 (CIM8) FPD is automatically upgraded to the latest qualified version when the line card FPD is upgraded. This ensures that both the line card and CIM8 operate with optimized performance and improved interoperability. Supported line cards are: • NCS1K14-2.4T-X-K9 • NCS1K4-2.4T-K9

Procedure

Step 1 Use the **show hw-module fpd** command to check whether all the FPDs are in the Current state.

If the status of any FPD is **NEED UPGD**, then the upgrade is required for that FPD.

Step 2 Use the **show fpd package** command to determine the FPDs that are supported with the current software release and the minimum hardware requirements for each FPD.

The Coherent Interconnect Module 8 (CIM8) FPD is automatically upgraded to the latest qualified version while the line card FPD is being upgraded. If the CIM 8 has a higher version than the line card's CIM 8 FPD version, the CIM 8 remains at the higher version and does not downgrade.

- NCS1K14-2.4T-X-K9
- NCS1K4-2.4T-K9

You can see the CIM 8 FPD version in the **show fpd package** command output.

```
RP/0/RP0/CPU0:ios#show fpd package
Wed Jul 17 11:44:07.258 IST

================================ ================================================
                                        Field Programmable Device Package
                                 ================================================
                                           Req      SW       Min Req   Min Req
Card Type            FPD Description       Reload   Ver      SW Ver    Board Ver
================== ========================= ====== ======= ======== =========
--------------------------------------------------------------------------------
NCS1014              ADM-CHASSIS             NO      0.21      0.21      0.0
                     IoFpga                  NO      1.19      1.19      0.0
                     IoFpgaGolden            NO      1.05      1.05      0.0
                     SsdIntelSC2KB           YES     1.20      1.20      0.0
                     SsdMicron5400           YES     0.02      0.02      0.0
--------------------------------------------------------------------------------
NCS1K-MD-32E-C       MD-32-ACC               NO      2.18      2.18      0.0
                     MD-32-NEO               NO      2.02      2.02      0.0
.
.
.
--------------------------------------------------------------------------------
NCS1K14-2.4T-K9      CIMFw                   NO    180.13019 180.13019   0.0
                     CpuModFw                NO     43.27     43.27      0.0
--------------------------------------------------------------------------------
NCS1K14-2.4T-L-K9    CIMFw                   NO    180.13019 180.13019   0.0
                     CpuModFw                NO     43.27     43.27      0.0
--------------------------------------------------------------------------------
NCS1K14-2.4T-X-K9    CIMFw                   NO    180.13019 180.13019   0.0
                     CpuModFw                NO     43.27     43.27      0.0
--------------------------------------------------------------------------------
NCS1K14-2.4TXL-K9    CIMFw                   NO    180.13019 180.13019   0.0
                     CpuModFw                NO     43.27     43.27      0.0
--------------------------------------------------------------------------------
.
.
NCS1K14-CNTLR-K9     ADM-DB                  NO      2.10      2.10      0.2
                     ADM-MB                  NO      2.30      2.30      0.2
                     BIOS                    YES     4.80      4.80      0.0
                     BIOS-Golden             YES     4.70      0.01      0.0
```

This table describes the fields in the output of the **show fpd package** command.

Table 8: Description of Fields in show fpd package Command

Field	Description
Card Type	PID of the modules such as chassis, card, CPU, and PSU.
FPD Description	Description of the FPD.
Req Reload	Determines whether reload is required to activate the FPD image.
SW Ver	Recommended FPD software version for the associated module running the current Cisco IOS XR Software.
Min Req SW Ver	Minimum required FPD software version to operate the module.
Min Req Board Ver	Minimum required hardware version for the associated FPD. A minimum hardware requirement of version 0.0 indicates that all the hardware can support this FPD version.

FPD can be upgraded using two methods:

- Manual upgrade
- Automatic upgrade

Manual FPD Upgrade

Use the following procedure to upgrade the FPDs manually.

Procedure

Step 1 Use the **upgrade hw-module location** *[location-id]* **fpd** *[fpd name]* command to upgrade a specific FPD.

Note
FPD upgrades are non-traffic affecting.

Example:

```
RP/0/RP0/CPU0:ios#upgrade hw-module location 0/0/NXR0 fpd CPUModFw
```

Step 2 Use the **show hw-module fpd** command to display information about the completed FPD upgrade.

Step 3 (Optional) Use the **upgrade hw-module location** *[location-id]* **fpd** *[fpd name]* **force** command to forcibly upgrade a specific FPD irrespective of whether the upgrade is required or not.

Example:

```
RP/0/RP0/CPU0:ios#upgrade hw-module location 0/0/NXR0 fpd CPUModFw force
```

Step 4 Use the **reload location** *location-id* to reload the FPDs belonging to a specific location with the new version.

The **Reload Loc** field in the output of **show hw-module fpd** command indicates whether the reload is required or not.

Example:

```
RP/0/RP0/CPU0:ios#reload location 0/RP0/CPU0
```

Step 5 (Optional) Use the **upgrade hw-module location all fpd all** command to upgrade all the FPDs concurrently.

Example:

```
RP/0/RP0/CPU0:ios#upgrade hw-module location all fpd all
```

Note
You cannot upgrade PSU FPD using **location all fpd all** command. You can excecute **Step 6** command to upgrade PSU FPD.

Step 6 (Optional) Use the **upgrade hw-module [location** [*location-id* | **all**]] **fpd** [*fpd name*] | **all**] command to upgrade a specific FPD, all the FPDs, or the FPDs belonging to a specific location.

Note
Until Release 24.2.1, you cannot forcefully upgrade FPDs of power modules and SSDs.

From Release 24.3.1, you can upgrade power module FPDs by using the command:

upgrade hw-module [location [*location-id* | **all**]] **[pm** [*pm-id* | **all**]] **fpd** [*fpd name*] | **all**].

Automatic FPD upgrade

Table 9: Feature History

Feature Name	Release Information	Feature Description
Automatic FPD Upgrade Support for Power Module	Cisco IOS XR Release 24.3.1	The FPD upgrade for power modules is now integrated with the NCS 1014 automatic FPD upgrade. You have the flexibility to include or exclude the power module FPD in the automatic upgrade according to your operational requirements. This option is disabled by default. Command added: • **fpd auto-upgrade {include | exclude} pm** You can also enable the automatic FPD upgrade for power modules using the OpenConfig data model Cisco-IOS-XR-openconfig-system-fpd-ext.

The automatic FPD upgrade process the firmware upgraded with the **NEED UPGD** status to **CURRENT** status automatically. Use the **show hw-module fpd** command to view the latest status after the automatic upgrade is completed.

In NCS 1014, automatic FPD upgrade is enabled by default.

Procedure

Step 1 Use the following commands to disable automatic FPD upgrade.

Example:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#fpd auto-upgrade disable
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#end
```

Note

- CpuModFw is upgraded during the automated FPD upgrade for cards NCS1K14-2.4T-K9 and NCS1K14-2.4T-L-K9.
- OptModFw is upgraded first followed by CpuModFw during automated FPD upgrade for the cards NCS1K14-CCMD-16-C, NCS1K14-CCMD-16-L, and NCS1K4-1.2T-K9 .
- Untill R24.2.1, you cannot do an automatic upgrade for the FPD power module.

Step 2 (From R24.3.1), to include or exclude automatic upgrade of power modules, use the following commands:

Example:

```
RP/0/RP0/CPU0:ios#fpd auto-upgrade include pm
RP/0/RP0/CPU0:ios#commit
```

Example:

```
RP/0/RP0/CPU0:ios#fpd auto-upgrade exclude pm
RP/0/RP0/CPU0:ios#commit
```