

XRV9K

IOS-XR Release 25.4.2

System Upgrade Procedure

Contents

Purpose, Scope and Audience 3

Bridge SMU / Mandatory RPMs 3

Required Package Files 4

Pre-upgrade Tasks..... 6

Configuration Backup 6

Check for config inconsistency 6

Check for available disk space 6

System stability check 6

Node Isolation 7

Software Upgrade 8

Method 1: Upgrade using the Golden ISO (GISO) 8

Method 2: Upgrade using the mini ISO and optional RPMs 9

Method 3: M7 Appliance - CIMC boot 11

Method 4: M7 ESXI - Fresh Boot 14

Post-Upgrade Tasks..... 18

Health Check 18

Software Version Check..... 18

Check for config inconsistency 18

Check/fix the configuration file system 18

Downgrade/Rollback to previous IOS-XR version 19

Caveats:..... 20

Purpose, Scope and Audience

This document provides information on the two methods Classic and GISO methods available for system upgrade and downgrade for XRV9000 Series platforms from software version 24.4.1 to 25.4.2 and vice versa. The table below presents the supported compatibility matrix for this release.

Table 1. Compatibility Matrix

Platform	From	To
XRV9000	IOS-XR 24.4.1	IOS-XR 25.4.2
XRV9000	IOS-XR 24.4.2	IOS-XR 25.4.2
XRV9000	IOS-XR 25.1.1	IOS-XR 25.4.2
XRV9000	IOS-XR 25.1.2	IOS-XR 25.4.2
XRV9000	IOS-XR 25.2.1	IOS-XR 25.4.2
XRV9000	IOS-XR 25.3.1	IOS-XR 25.4.2
XRV9000	IOS-XR 25.2.2	IOS-XR 25.4.2
XRV9000	IOS-XR 25.4.1	IOS-XR 25.4.2
XRV9000	IOS-XR 26.1.1	IOS-XR 25.4.2

Note : Non-OE (below 24.4.1) to OE Migration image (24.4.1 and above) upgrade is not supported and vice versa. Fresh boot is required.

Audience: This guide is for Cisco Systems Field Engineers and Network Operators.

Bridge SMU / Mandatory RPMs

A bridge SMU is an SMU that is a prerequisite to an upgrade or downgrade to another Cisco IOS XR software release. Bridge SMUs are also referred to as mandatory upgrade or downgrade SMUs because they must be installed before an upgrade or downgrade.

Mini ISO Package is mandatory to perform the System Upgrade, and upgrade needs to be done from XR VM. Additional XR packages listed below are needed depending on the router configuration and required features

Refer to [Cisco IOS XR General Information](#) for procedures for each upgrade or downgrade and for details of any mandatory bridge SMUs.

Table 2. Bridge SMU / Mandatory RPMs

From Release	To Release	Bridge SMU / Mandatory RPMs
IOS-XR 24.4.1	IOS-XR 25.4.2	N/A

From Release	To Release	Bridge SMU / Mandatory RPMs
IOS-XR 24.4.2	IOS-XR 25.4.2	N/A
IOS-XR 25.1.1	IOS-XR 25.4.2	N/A
IOS-XR 25.1.2	IOS-XR 25.4.2	N/A
IOS-XR 25.2.1	IOS-XR 25.4.2	N/A
IOS-XR 25.3.1	IOS-XR 25.4.2	N/A
IOS-XR 25.2.2	IOS-XR 25.4.2	N/A
IOS-XR 25.4.1	IOS-XR 25.4.2	N/A
IOS-XR 26.1.1	IOS-XR 25.4.2	N/A

Note: No Bridge SMU required to upgrade/downgrade between above paths.

Required Package Files

Mini ISO Package is mandatory to perform the System Upgrade, and upgrade needs to be done from XR VM. Additional XR packages listed below are needed depending on the router configuration and required features

Table 3. Package Files

Description	Package Name	Details
M7 Appliance/EXSI VRR profile	fullk9-R-XRV9000-2542-RR.tar	Used for Fresh bake and upgrade M7 Appliance for VRR Profile. Download from Cisco Software Download portal.
M7 Appliance/EXSI VRR profile with VGA support	fullk9-R-XRV9000-2542-RRVG.tar	Used for Fresh bake and upgrade M7 ESXI for VRR Profile. Download from Cisco Software Download portal.
M7 Appliance/EXSI Non VRR profile	fullk9-R-XRV9000-2542.tar	Used for Fresh bake and upgrade M7 ESXI for Non VRR Profile. Download from Cisco Software Download portal.
M7 Appliance/EXSI Non VRR profile with VGA support	fullk9-R-XRV9000-2542-VG.tar	Used for Fresh bake and upgrade/downgrade for Non VRR Profile. Download from Cisco Software Download portal.
Golden ISO Image	Golden ISO (GISO) is a customized ISO	Refer Configuration Guide - Cisco IOS XRv 9000 Router Installation and Configuration Guide Chapter: Customize Installation using Golden ISO



Pre-upgrade Tasks

This includes tasks and health checks that can be performed outside of the standard upgrade MOP to verify abnormal hardware behavior and validate system parameters relevant to upgrade success.

Configuration Backup

Copy the running-configuration to a harddisk: on the router and to a remote scp server.

```
RP/0/RP0/CPU0# copy running-config harddisk:/running_config-<mmddyyyy>
RP/0/RP0/CPU0:ios#scp harddisk:/ running_config-<mmddyyyy> user@<ip-address>:<location>
```

Check for config inconsistency

Check for any inconsistencies in the configuration before upgrade using '*show configuration failed startup*'. If there are any errors, clear them using '*clear configuration inconsistency*'

Check for available disk space

Check the space available in the install repository; free space in /harddisk: is required to perform system upgrade. Use "*show media*" to check the space availability.

TIP: Remove old or large size files to free disk space:

- delete harddisk:*core*
- delete harddisk:/showtech/*
- delete harddisk:<old iso files if any>
- remove inactive packages using "install remove inactive" from XR and Admin plane.

System stability check

The following commands should be executed at the XR prompt to verify basic system stability before the upgrade.

CLI	Description
show platform	Verify that all nodes are in "IOS XR RUN/OPERATIONAL" state
show platform vm	Verify that all nodes are in "FINAL Band" state
show ipv4 interface brief <or> show ipv6 interface brief <or> show interface summary	Verify that all necessary interfaces are "UP"
show install active	Verify that the proper set of packages are active

CLI	Description
admin show install active	Verify on sysadmin plane
show install committed	Verify that the proper set of committed packages are same as active. If not, execute 'install commit'
show alarms brief system active	Shows any outstanding active alarms in system
admin show environment all	Shows temperature, Fan, Voltage, Power status
show media (both XR and Admin mode) location all	Shows the disk usage in XR and admin state
show inventory	Shows chassis inventory information
show logging	Capture show logging to check for any errors
show watchdog memory-state location all	Monitors watchdog memory status
show health gsp	GSP health check
show health sysdb	Sysdb health check
admin show install health	Verifies the current state of the system

Node Isolation

Once the sanity check is done, it's recommended to drain/isolate the router. This can be achieved using regular routing techniques (ISIS overload bit, OSPF max metric, MPLS traffic engineering, BGP attributes, etc.).

Software Upgrade

Available Boot Methods for Install/Upgrade:

1. Install Replace with Golden ISO (Recommended)
Use a pre-built Golden ISO image to perform a fresh installation or replacement of the existing system. Recommended method if the router with a running pre-25.4.2 image is in a stable state, and the intention is to upgrade without losing the existing configuration
2. Install add/activate using mini ISO + Optional RPMs
Start with a standard mini ISO image for installation, with the option to include additional RPM packages as needed.
3. M7 Appliance – CIMC boot
Used for Fresh bake and upgrade M7 Appliance with either a standard ISO or a Golden ISO image.
4. M7 ESXI – Fresh Boot
Used for Fresh bake and upgrade M7 Appliance with either a standard ISO or a Golden ISO image.

Method 1: Upgrade using the Golden ISO (GISO)

Users have the option to create a custom Golden ISO (GISO) by utilizing the gisobuild.py script perform the upgrade with the single command 'install replace <giso>'. For detailed instructions, please refer to the "Customize Installation using Golden ISO" chapter in the [Cisco IOS XRv 9000 Router Installation and Configuration Guide](#)

Alternatively, you may contact the Cisco Technical Assistance Centre (TAC) to request a Golden ISO (GISO) that includes the specific optional RPMs you require.

GISO on External Server (Recommended)

Upgrade the system to replace the current software with the GISO image available on external server.

```
RP/0/RP0/CPU0:ios#install replace sftp://user:*****@172.24.77.24/auto/tftp-rtp-sit/asr9k/xrv9k-goldenk9-x-25.4.2.iso commit noprompt
```

Enter absolute path of GISO which is intended to be installed

Example:

```
sftp://user[:password]@server/directory/GISO
scp://user[:password]@server/directory/GISO
ftp://user[:password]@server/directory/GISO
tftp://server/directory/GISO
http://server/directory/GISO
```


GISO on Router harddisk

Download/Copy the ISO (or GISO) image to the harddisk: location on the router.

Upgrade the system to replace the current software with the GISO image available on the /harddisk: of the router

```
Step1: RP/0/RP0/CPU0:ios#scp <user>@<ip-address>:<directory>/xrv9k-goldenk9-x-25.4.2.iso  
harddisk:
```

```
Step2: RP/0/RP0/CPU0:ios#show md5 file /harddisk:/xrv9k-goldenk9-x-25.4.2.iso
```

```
Step3: RP/0/RP0/CPU0:ios#install replace harddisk:/xrv9k-goldenk9-x-25.4.2.iso commit  
noprompt
```

Enter local path to the GISO relative to the default path: /harddisk:/mirror/

Example:

/directory/GISO

GISO

directory/GISO (path relative to /harddisk:/mirror)

./directory/GISO (path relative to /harddisk:/mirror)

Method 2: Upgrade using the mini ISO and optional RPMs

This method requires user to perform 2 step process of install add and install activate operation to complete the upgrade.

Packages on External Server (Recommended)

Untar the RPMs and create a single tar that includes the mini.iso and all optional RPMs on external server.

Pre-requisite: Refer Appendix section for Managing External server/repo reachability.

1. Perform 'install add' of the tar file.

```
RP/0/RP0/CPU0:ios#install add source sftp://user:*****@172.24.77.24/auto/tftp-  
rtp-sit/asr9k/ xrv9k-goldenk9-x-25.4.2.tar
```

Example:

sftp://user[:password]@server:/directory/

ftp://user[:password]@server:/directory/

http://[user:password@]server/directory/

https://[user:password@]server/directory/

ftp://user[:password]@server;VRF/directory/

2. Take a note of the install operation id generated by the add operation in previous step.

Note: Install operation **id#** finished successfully

3. Prepare the packages added in the previous step:

```
RP/0/RP0/CPU0:ios#install prepare id id#
```

Or, if multiple add operations occurred:

```
RP/0/RP0/CPU0:ios#install prepare id id1 id2
```

4. Activate all the packages:

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

5. Router will reload at the end of activation to start using the new packages.

Note: This operation may take up some time to complete as the router goes for reboot with new image.

6. After performing Post Upgrade Checks and execute 'install commit' to commit the newly active software (install commit is required after any install activate operation else after router reload, nodes will go back to previously committed software)

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

Packages on Router harddisk

Download/Copy the single tar created to the harddisk: location on the router.

```
Step1: RP/0/RP0/CPU0:ios#scp <user>@<ip-address>:<directory>/ xrv9k-goldenk9-x-25.4.2.tar  
harddisk:
```

```
Step2: RP/0/RP0/CPU0:ios#show md5 file /harddisk:/xrv9k-goldenk9-x-25.4.2.tar
```

```
Step3: RP/0/RP0/CPU0:ios#install add source harddisk:/ xrv9k-goldenk9-x-25.4.2.tar
```

Example:

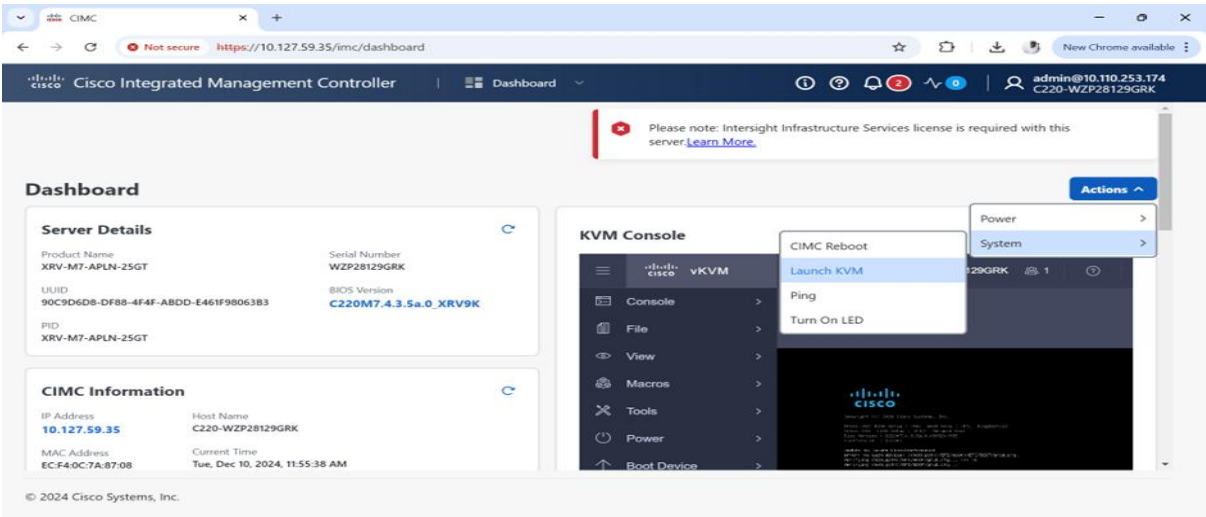
```
harddisk:/directory
```

Perform steps 2–6 as described in the "Packages on External Server (Recommended)" section.

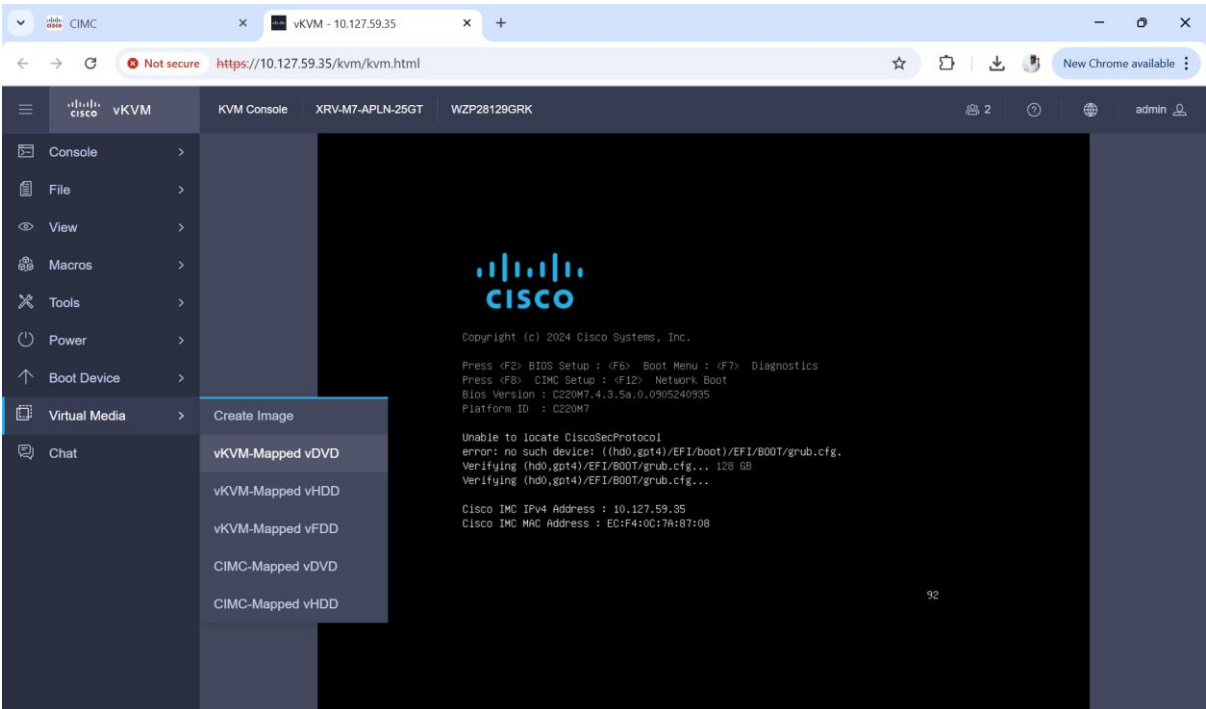
Method 3: M7 Appliance – CIMC boot

All System Upgrade related install operations should be done in the XR VM plane.

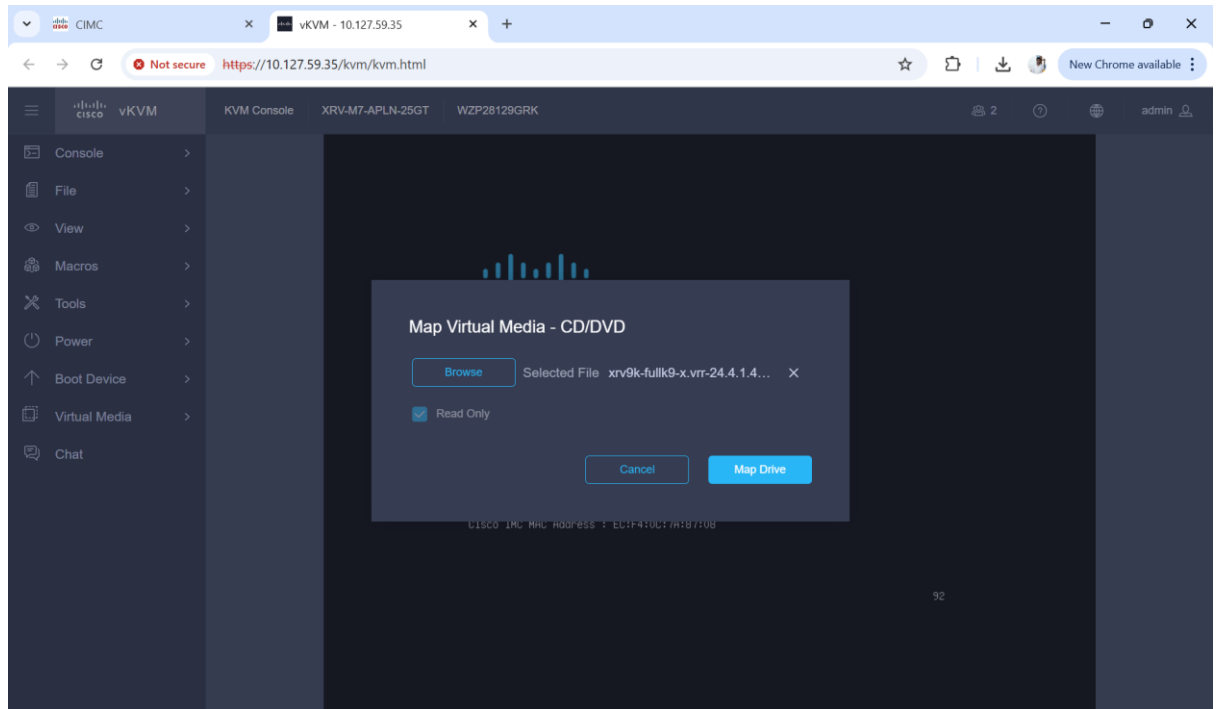
- Download the xrv9k-fullk9-x.vrr-25.4.2.iso image (version 25.4.2) from Cisco CCO portal
- Copy OS installation ISO disk image files to your computer.
- Verify the md5 checksum of the tar/individual rpms with the original MD5 values on CCO
- If CIMC is not open, then log in
- In the Navigation pane, click the Launch KVM



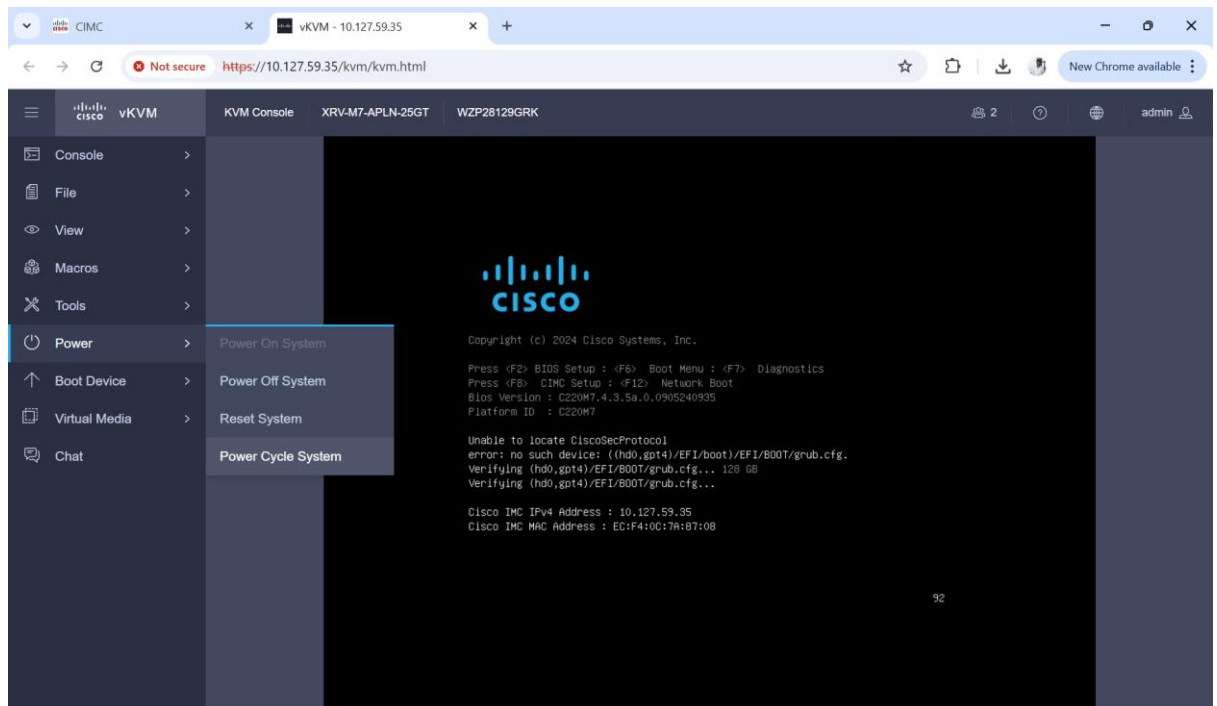
- Select Virtual Media>Activate Virtual Device in the KVM console.



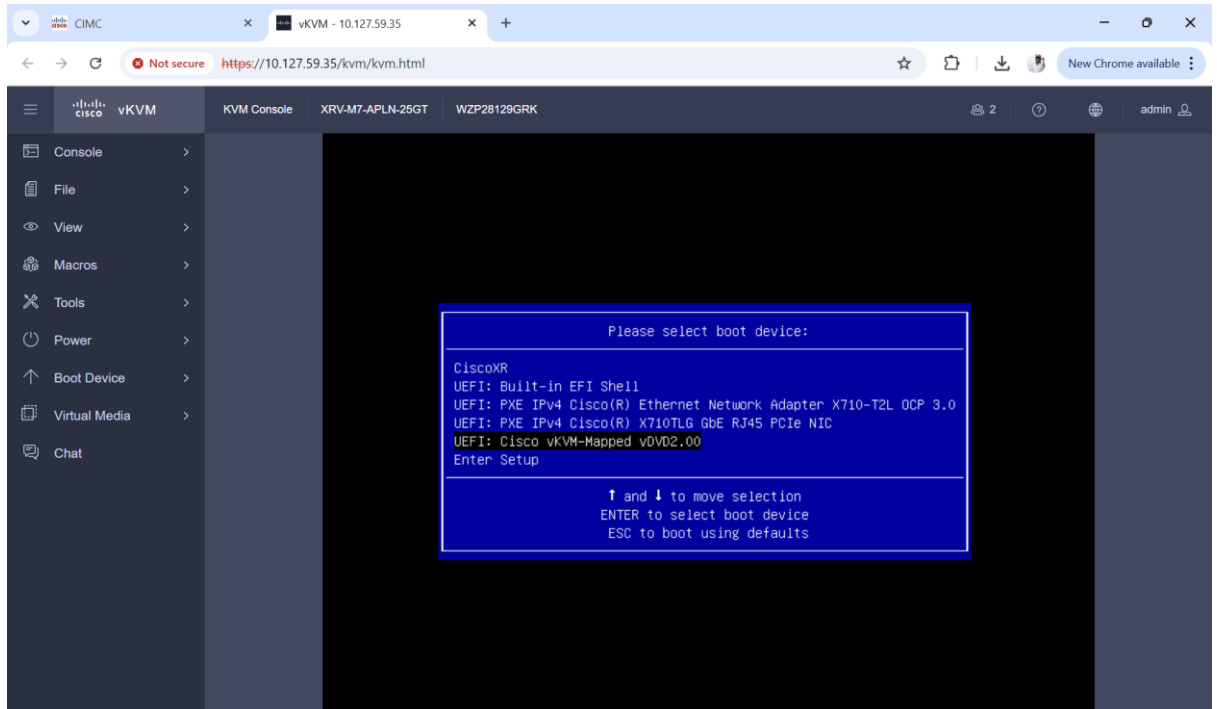
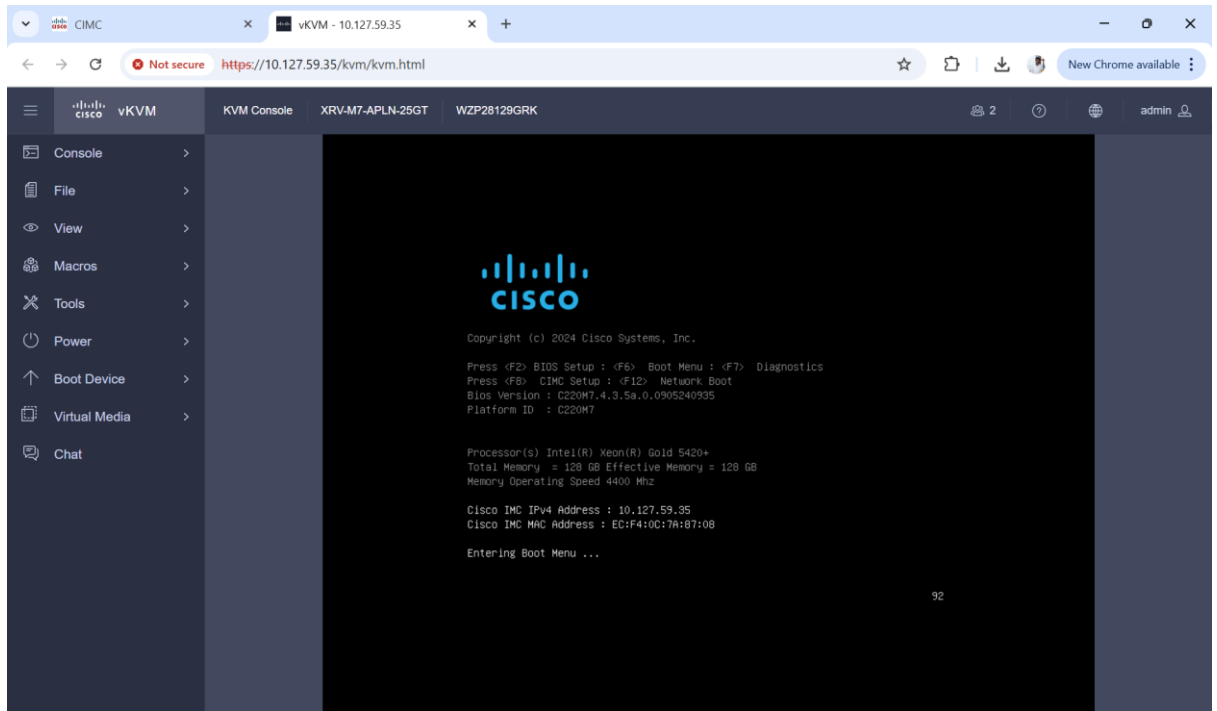
- Select Virtual Media>vKVM Mapped DVD. Then browse the ISO installation disk image stored locally and click Map Device.



- Select Power>Power cycle System (warm boot) in the KVM console.

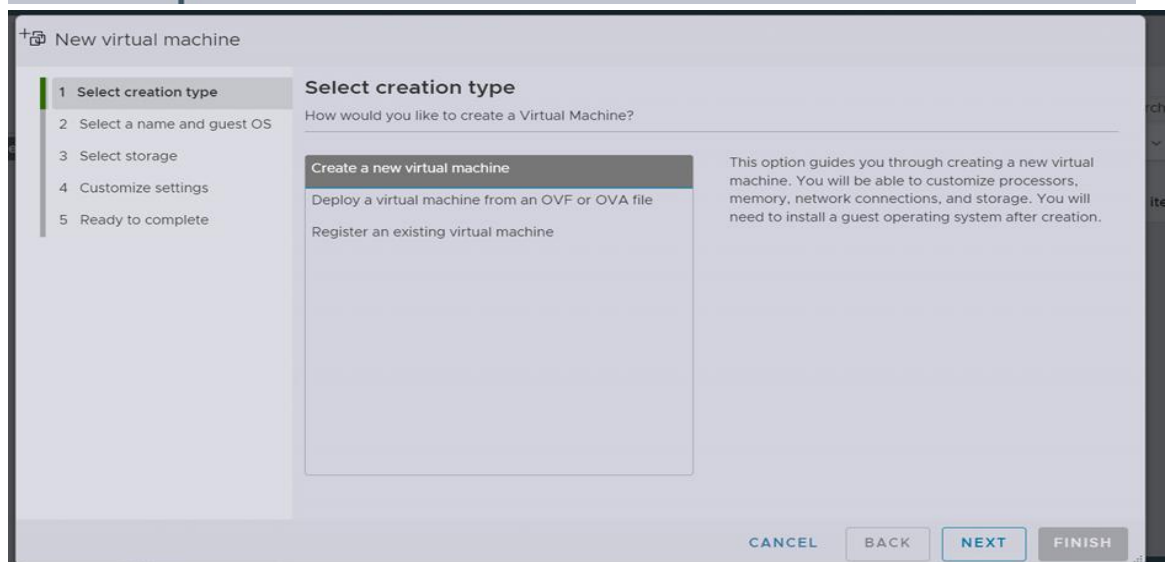
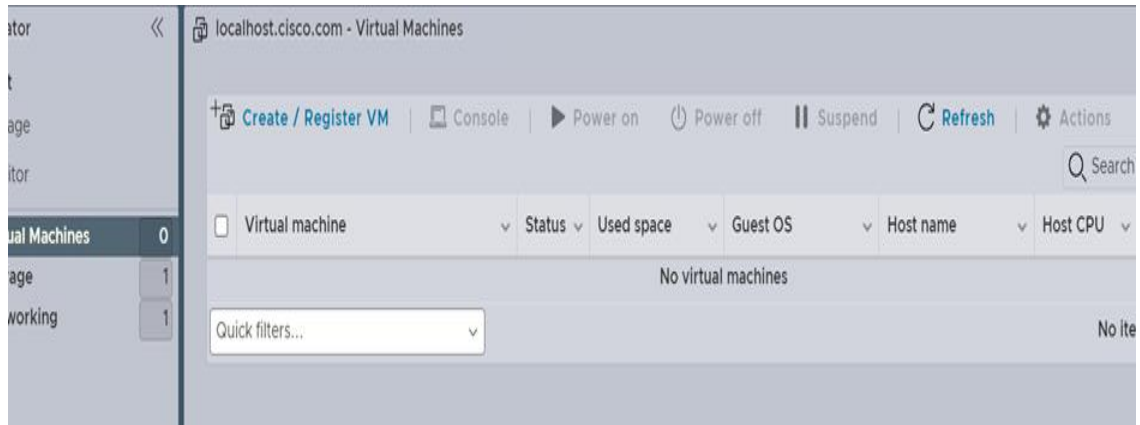


- Press F6 to enter the boot menu. Once you are in the boot menu, select the first DVD which is nothing but the same iso you selected earlier, mounted as a virtual disk. (Eg: Cisco vKVM Mapped vDVD1).
- When the server reboots, it begins the installation process. After the installation process completes, system is upgraded and committed with your desired version/25.4.2 as mentioned in page 7.



Method 4: M7 ESXI – Fresh Boot

- Download the xrv9k-fullk9-x.vrr-25.4.2.iso image (version 25.4.2) from Cisco CCO portal [Cisco Software Download](#).
- Copy OS installation ISO disk image files to your computer
- Create XRv9k VM
- Click Virtual Machines on the left navigation panel and click Create/Register VM menu



- Select Name and Guest OS family and Guest OS version

New virtual machine - xrv9k_M7_3 (ESXi 7.0 U2 virtual machine)

1 Select creation type

2 Select a name and guest OS

3 Select storage

4 Customize settings

5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name
xrv9k_M7_3

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility ESXi 7.0 U2 virtual machine

Guest OS family Other

Guest OS version Other (64-bit)

CANCEL BACK NEXT FINISH

- Configure CPU, Memory and Hard disk1 memory settings on the virtual machine.

Note: for performance testing allocate 12 CPU cores for the VM

New virtual machine - xrv9k_M7_3 (ESXi 7.0 U2 virtual machine)

1 Select creation type

2 Select a name and guest OS

3 Select storage

4 Customize settings

5 Ready to complete

Add hard disk

Add network adapter

Add other device

> CPU 4

> Memory 20 GB

> Hard disk 1 64 GB

- Select IDE controller 0 and Slave under Hard disk1 and Select IDE controller 0 and Master under CD/DVD Drive 1

	BROWSE...	
Disk Provisioning	<input type="radio"/> Thin provisioned <input checked="" type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Controller location	IDE controller 0	Slave
Disk mode	Dependent	
Sharing	None	

✓ CD/DVD Drive 1	Host device	<input checked="" type="checkbox"/> Connect
Status	<input checked="" type="checkbox"/> Connect at power on	
CD/DVD Media	None	
Controller location	IDE controller 0	Master
> Video Card	Default settings	

- VM option>Boot Option >Firmware – Change BIOS TO EFI

Configure the virtual machine hardware and virtual machine additional options

The screenshot shows the 'VM Options' tab with the 'Boot Options' section expanded. Under 'Boot Options', the 'Firmware' dropdown is set to 'EFI'. Below it, the 'Enable UEFI secure boot' checkbox is present. Other sections like 'VMware Remote Console Options', 'VMware Tools', and 'Power management' are also visible.

- Select Datastore ISO file under CD/DVD Drive 1 and select the xrv9k-fullk9-x.vrr-25.4.2.iso from Datastore

The screenshot shows the 'VM Hardware' configuration window. The 'CD/DVD Drive 1' section is selected, and the 'Host device' dropdown is open, showing 'Datastore ISO file' as the selected option. Other hardware components like 'USB controller 1' and 'Network Adapter 1' are also visible.

- To add serial port, click 'Add other device' and Click on Serial port.
- Add Telnet details for console login in Port URL
- Power on the VM and wait for 15 mins and Connect to the VM using serial console port

Example Telnet 10.105.247.193 3003

- More Details Please refer

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M7/install/b-c220-m7-installation-guide.pdf

Post-Upgrade Tasks

Health Check

Execute and verify the health check commands mentioned in “System stability check” section of **Pre-upgrade Tasks**

Software Version Check

Verify show version to check router is upgraded to desired image.

```
RP/0/RP0/CPU0:RR3-XRv-M7-ESXI#sh ver
Sun Mar 29 19:31:30.327 UTC
Cisco IOS XR Software, Version 25.4.2
Copyright (c) 2013-2026 by Cisco Systems, Inc.

Build Information:
  Built By       : swtools
  Built On       : Sat Mar 28 20:07:12 PDT 2026
  Built Host     : iox-ucs-1017
  Workspace      : /auto/srcarchive12/prod/25.4.2/xrv9k/ws
  Version        : 25.4.2
  Location       : /opt/cisco/XR/packages/
  Label          : 25.4.2

cisco IOS-XRv 9000 () processor
System uptime is 4 minutes
```

Check for config inconsistency

Check for any inconsistencies in the configuration before upgrade using *'show configuration failed startup'*.
If there are any errors, clear them using *'clear configuration inconsistency'*

Check/fix the configuration file system

```
RP/0/RP0/CPU0:ios#cfs check
```

Downgrade/Rollback to previous IOS-XR version

There are few options to choose from to downgrade IOS XR version.

Option 1: If install commit was not done after upgrade to 25.4.2, a router reload will bring it back to previous install committed image.

Option 2: Install remove the inactive packages and re-add the previous IOS-XR version iso image+rpm via install add, prepare, activate to downgrade/rollback

Option 3: For Fresh bake please refer Method 3 and 4 in **Software Upgrade** section

Note: Fresh bake will wipe out all the data/config from the router. Please backup any required configuration or files before proceeding with the upgrade. Refer to section 'Pre-Upgrade Task à Configuration backup' for steps to perform this.

Caveats:

The caveats listed below may be summaries only. Please review release note enclosure (RNE) for each DDTS for complete details (Including known workarounds and/or actions to take).

DDTS	Description

Note: No caveats for downgrade from Release IOS-XR 25.4.2 to prior supported versions