

Cisco Secure Network Server 36x5 Firmware Upgrade Guide

Overview 2

Upgrade and activate the firmware 7

Verify the firmware version 10

Revised: August 11, 2026

Overview

This document describes how to upgrade firmware on Cisco Secure Network Server (SNS) 3600 series appliance.

Note We recommend that you gracefully shutdown the ISE services on the Cisco SNS appliance before performing this upgrade.

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.260020) from these releases:

- 4.3(2.260007)
- 4.3(2.250045)
- 4.3(2.240107)
- 4.3(2.240077)
- 4.3(2.240053)
- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

These files are required for this upgrade:

- SNS-36xx-BIOS-4-3-2h_ISE.cap: BIOS update image for Cisco SNS 36x5 appliances
- SNS-36xx-HUU-4.3.2.260020_ISE.iso: Host Upgrade Utility (HUU) ISO for Cisco SNS 36x5 appliances

For more information about the firmware release 4.3(2.260020), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.260007) from these releases:

- 4.3(2.250045)
- 4.3(2.240107)
- 4.3(2.240077)
- 4.3(2.240053)

- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

These files are required for this upgrade:

- SNS-36xx-BIOS-4-3-2g_ISE.cap: BIOS update image for Cisco SNS 36x5 appliances
- SNS-36xx-HUU-4.3.2.260007_ISE.iso: HUU ISO for Cisco SNS 36x5 appliances

For more information about the firmware release 4.3(2.260007), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.250045) from these releases:

- 4.3(2.240107)
- 4.3(2.240077)
- 4.3(2.240053)
- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

These files are required for this upgrade:

- SNS-36xx-BIOS-4-3-2f_ISE.cap: BIOS update image for Cisco SNS 36x5 appliances
- SNS-36xx-HUU-4.3.2.250045_ISE.iso: Host Upgrade Utility (HUU) ISO for Cisco SNS 36x5 appliances

For more information about the firmware release 4.3(2.250045), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.240107) from these releases:

- 4.3(2.240077)
- 4.3(2.240053)
- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

These files are required for this upgrade:

- SNS-36xx-BIOS-4-3-2c_ISE.cap file: BIOS firmware for Cisco SNS 3600 series appliance
- SNS-36xx-HUU-4.3.2.240107_ISE.iso: HUU .iso file for Cisco SNS 3600 series appliance

You must download these files from the Cisco ISE Software Download site.

For more information about the firmware release 4.3(2.240107), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.240077) from these releases:

- 4.3(2.240053)
- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

Note If you are upgrading from firmware release 4.3(2.240053), you can directly perform the HUU ISO upgrade using the SNS-36xx-HUU-4.3.2.240077_ISE.iso. For other releases, you must first upgrade the BIOS firmware using the SNS-36xx-BIOS-4-3-2b_ISE.cap file and then perform the HUU ISO upgrade using the SNS-36xx-HUU-4.3.2.240077_ISE.iso file. You must download these files from the Cisco ISE Software Download site.

For more information about the firmware release 4.3(2.240077), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.240053) from these releases:

- 4.3(2.240009)
- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

For more information about the firmware release 4.3(2.240053), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.240009) from these releases:

- 4.3(2.230207)
- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

Note If you are upgrading from firmware release 4.3(2.230207), you can directly perform the Host Upgrade Utility (HUU) ISO upgrade using the SNS-36xx-HUU-4.3.2.240009_ISE.iso file. For other releases, you must first upgrade the BIOS firmware using the SNS-36xx-BIOS-4-3-2a_ISE.cap file and then perform the HUU ISO upgrade using the SNS-36xx-HUU-4.3.2.240009_ISE.iso file. You must download these files from the Cisco ISE Software Download site.

For more information about the firmware release 4.3(2.240009), see the Release Notes for Cisco UCS Rack Server Software, Release 4.3(2).

You can upgrade to Cisco SNS 36x5 firmware release 4.3(2.230207) from these releases:

- 4.2(3d)
- 4.2(2b)
- 4.2(2)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

You can upgrade to Cisco SNS 36x5 firmware release 4.2(3d) from these releases:

- 4.2(2b)
- 4.2(1)
- 4.1(3)
- 4.1(2)
- 4.1(1)
- 4.0(4)

You can upgrade to Cisco SNS 36x5 firmware release 4.2(2b) from these releases:

- 4.1(3b)
- 4.1(3e)
- 4.0(1g)
- 4.0(4h)
- 4.0(4m)

You can upgrade to Cisco SNS 36x5 firmware release 4.1(3b) from these releases:

- 4.0(1g)
- 4.0(4h)
- 4.0(4m)



Note If you are using a version earlier than 4.0(1g), you must first upgrade to version 4.0(1g) before proceeding with the documented upgrade path.

These files are required for the upgrade:

- SNS-36xx-BIOS-4-x-xx-x_ISE.cap file (BIOS firmware for Cisco SNS 3600 series appliance)
- SNS-36xx-HUU-4.x.xx_ISE.iso (HUU .iso file for Cisco SNS 3600 series appliance)

You must download these files from the Cisco ISE Software Download site.

For more information, see the Release Notes for Cisco UCS Rack Server Software, Release 4.1(3).

Note The screenshots given in this document were taken while upgrading the firmware from 4.0(4m) to 4.1(3b). These screenshots are given for reference purpose only.

Upgrade and activate the firmware

Important You must perform these steps in the same sequence to upgrade and activate the firmware. If the BIOS firmware is not upgraded before the HUU ISO upgrade, then the BIOS will not be loaded properly and the boot options will not be displayed.

Procedure

Step 1 Update BIOS firmware , on page 7.

Step 2 Activate BIOS , on page 8.

Step 3 Update and activate other firmwares using HUU ISO, on page 8.

Attention It is highly recommended to gracefully shutdown the ISE services on the Cisco SNS appliance before performing this upgrade.

Update BIOS firmware

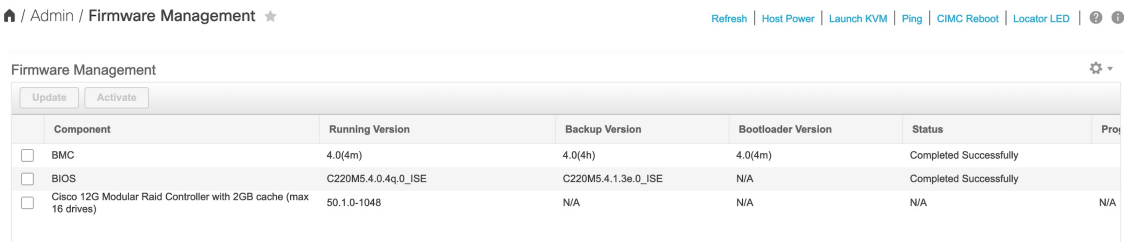
Procedure

Step 1 Check the **BIOS** check box and click **Update**.

Step 2 Click **Install BIOS Firmware Through Browser Client** and select the BIOS image.

Step 3 Click **Install Firmware**.

BIOS is successfully uploaded as the backup version.



Activate BIOS

Before you begin

You must Update BIOS firmware , on page 7 before performing this task.

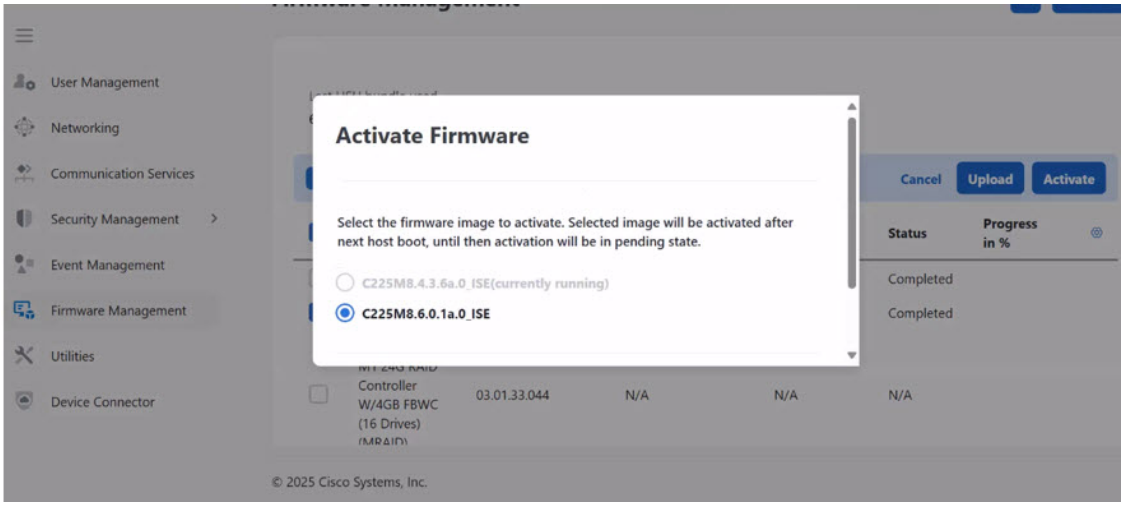
Procedure

Step 1 Choose **Host Power** > **Power Off** to power off the server manually.

Step 2 Check the **BIOS** check box.

Step 3 Click **Activate**.

Step 4 Choose the BIOS version and click **Activate Firmware**.



Step 5 Choose **Host Power** > **Power On** after activating the BIOS.

Update and activate other firmwares using HUU ISO

Before you begin

You must complete these steps before performing this task:

1. Update the BIOS firware.
2. Activate BIOS firmware.

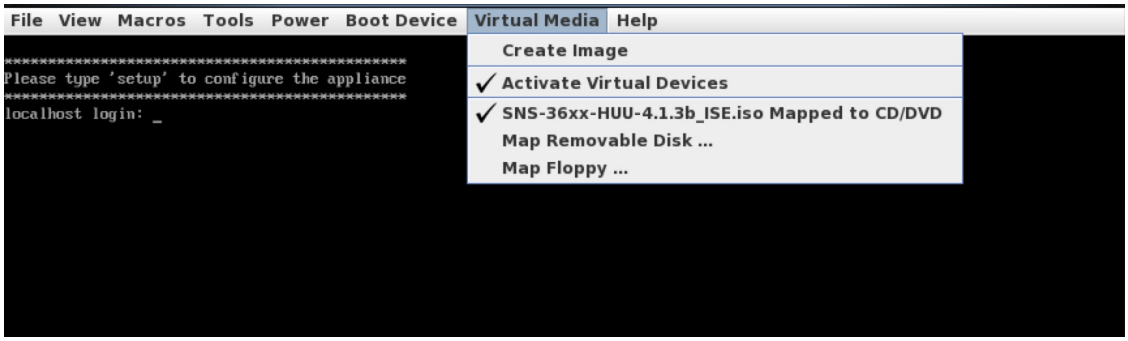
Important If the BIOS firmware is not upgraded before the HUU ISO upgrade, then the BIOS will not be loaded properly and the boot options will not be displayed.

Procedure

Step 1 Click **Launch KVM Console** on the toolbar to launch the KVM console.

Step 2 In the KVM console, click **Virtual Media**.

Step 3 Click **Activate Virtual Devices** and then click **Accept this Session**.



Step 4 Click **Map CD/DVD** and browse for the .iso file.

Step 5 Click **Map Device**.

Step 6 Choose **Power > Reset System (Warm Boot)** and press F6 when prompted to open the **Boot Menu** window.

Step 7 Choose **Cisco vKVM-Mapped vDVD1.22** and press Enter.

The server boots from the selected device.

Step 8 Read the Cisco End User License Agreement (EULA) and click **Agree** to proceed with the update.

The **Cisco Host Upgrade Utility** window appears with a list of components that are available for update.

Note
If you choose the **Disagree** option, the upgrade process is canceled and the host is rebooted.

Step 9 Click **Update & Activate**.

Step 10 In the **Update & Activate All** window, check the **Power Cycle to Activate** check box and click **Update & Activate**.

Note
BIOS upgrade is skipped during this step because BIOS is already upgraded to the latest version (see Update BIOS firmware , on page 7 and Activate BIOS , on page 8).

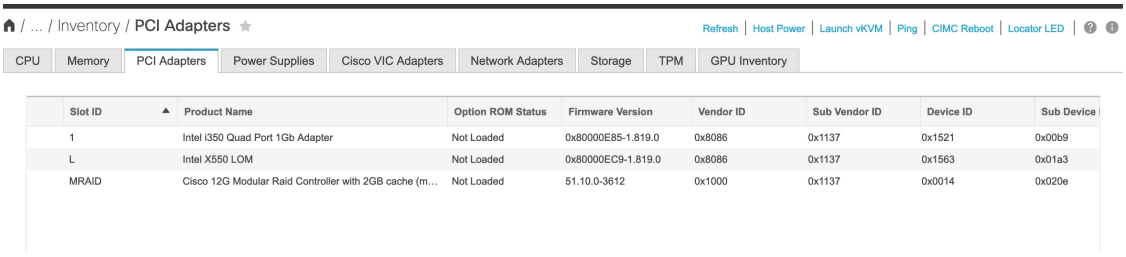
Step 11 The system is restarted after the firmware upgrade. Log in back to verify the upgraded firmware versions.

Verify the firmware version

Choose **Admin > Firmware Management** and verify the firmware version.



Choose **Chassis > Inventory > PCI Adapters** and verify the firmware versions.



Note Rollback of BMC and BIOS is not recommended while upgrading using the HUU ISO because it might cause compatibility issues.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.