

BIOS Upgrade for C8200 UCPE

Table 1: Feature History

Feature Name	Release Information	Description
BIOS Upgrade for Cisco Catalyst 8200 Series Edge uCPE	Cisco NFVIS Release 4.9.6	This feature outlines the BIOS upgrade process for the Cisco Catalyst 8200 Series Edge uCPE device to resolve the random number generation issue. This upgrade includes updates to Secure Boot FPGA and BIOS capsule.

- Information About BIOS Upgrade for C8200 UCPE, on page 1
- Prerequisites for BIOS Upgrade for C8200 UCPE, on page 2
- Supported Platforms for BIOS Upgrade, on page 2
- Perform BIOS Upgrade for C8200 UCPE, on page 2
- Verify BIOS Upgrade for C8200 UCPE, on page 2

Information About BIOS Upgrade for C8200 UCPE

In NFVIS release 4.9.6, a BIOS upgrade is needed for C8200 UCPE platforms to resolve an issue with entropy functioning, where random numbers are not being generated.

Perform the BIOS upgrade via an SSH session or a serial console using the following commands in sequence:

1. **platform-upgrade fpga secboot**
2. **platform-upgrade bios capsule**

Note The Cisco Catalyst 8200 Series Edge uCPE device reboots after the execution of each command.

Prerequisites for BIOS Upgrade for C8200 UCPE

Ensure that there are no power interruptions during the upgrade process.

Supported Platforms for BIOS Upgrade

Cisco Catalyst 8200 Series Edge uCPE.

Perform BIOS Upgrade for C8200 UCPE

To upgrade the BIOS for the C8200 UCPE, do the following:

Upgrade Secure Boot FPGA

From an SSH terminal or a serial console, execute the **platform-upgrade fpga secboot** command.

The system reboots after the execution of this command.

Update BIOS Capsule

From the SSH terminal or a serial console, execute the **platform-upgrade bios capsule** command .

The system reboots after the execution of this command.

Verify BIOS Upgrade for C8200 UCPE

Verify Secure Boot FPGA Version

The following is a sample output from the **support show aikido-version** command. This command confirms the updated Aikido version is 113.

```
Aikido version: 113
```

Verify BIOS Version

The following is a sample output from the **show platform** command. This command confirms the BIOS has been updated.

Below is a sample output from the **show platform** command, which confirms that the BIOS has been updated. The new BIOS version is highlighted in this example.

```
platform-detail hardware_info Manufacturer "Cisco Systems, Inc."
platform-detail hardware_info PID C8200-UCPE-1N8
platform-detail hardware_info SN FOC241106RR
platform-detail hardware_info hardware-version V01
platform-detail hardware_info UUID 4ce1767c-0660-0000-2903-0f0f000a0b05
platform-detail hardware_info Version 4.9.6-12
platform-detail hardware_info Compile_Time "Wednesday, September 18, 2024 [03:37:38 UTC]"
platform-detail hardware_info CPU_Information "Intel(R) Atom(TM) CPU C3758 @ 2.20GHz 8
cores"
```

```
platform-detail hardware_info Memory_Information "16294400 kB"
platform-detail hardware_info Disk_Size "75.4 GB"
platform-detail hardware_info CIMC_IP NA
platform-detail hardware_info Entity-Name "C8200 UCPE"
platform-detail hardware_info Entity-Desc "Cisco Catalyst 8200 Series Edge uCPE"
platform-detail hardware_info BIOS-Version C8200-UCPE_3.04.073120240748
platform-detail hardware_info CIMC-Version NA
platform-detail software_packages Kernel_Version 3.10.0-1062.4.1.4.el7.x86_64
platform-detail software_packages QEMU_Version 2.12.0
platform-detail software_packages LibVirt_Version 4.5.0
platform-detail software_packages OVS_Version 2.11.4
platform-detail switch_detail UUID NA
platform-detail switch_detail Type NA
platform-detail switch_detail Name NA
platform-detail switch_detail Ports 0
```

Verify Entropy Functionality

The following is a sample output from the **support show entropy** command. This command verifies whether entropy is functioning correctly.

```
Entropy sources that are available but disabled
1: TPM RNG Device (tpm)
5: NIST Network Entropy Beacon (nist)
9: Qrypt quantum entropy beacon (qrypt)

Available and enabled entropy sources:
0: Hardware RNG Device (hwrng)
2: Intel RDRAND Instruction RNG (rdrand)

Available entropy sources that failed initalization:
6: JITTER Entropy generator (jitter)
```