



Extreme OS ONE Switching and Routing v22.2.3.0 Deployment Guide

Installation, Configuration, and Firmware Upgrades

9041123-00 Rev AA
August 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks® and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: <https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks>

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>

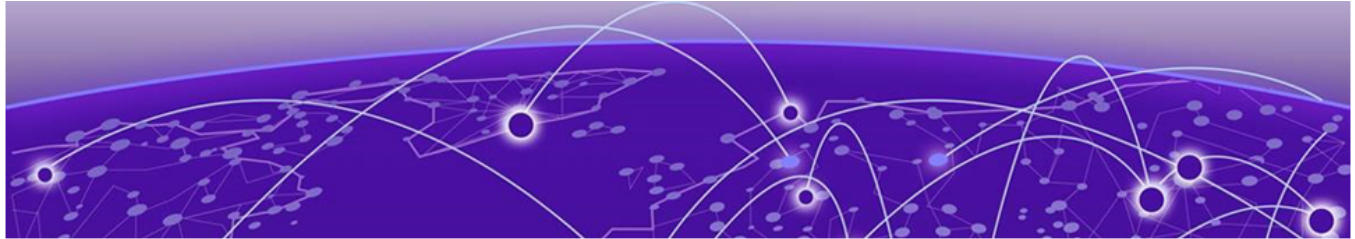
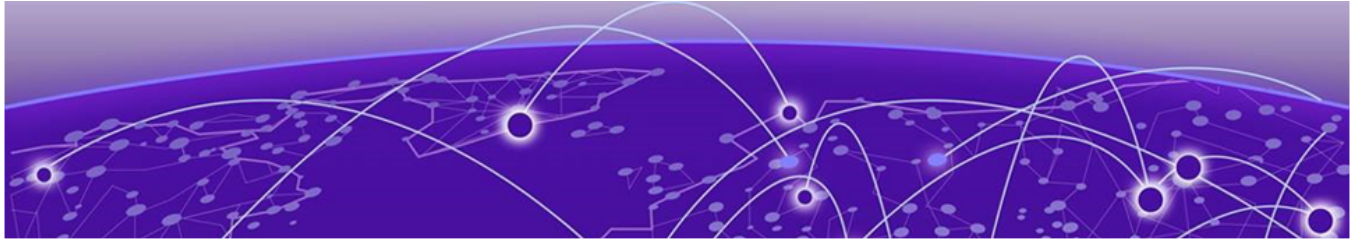


Table of Contents

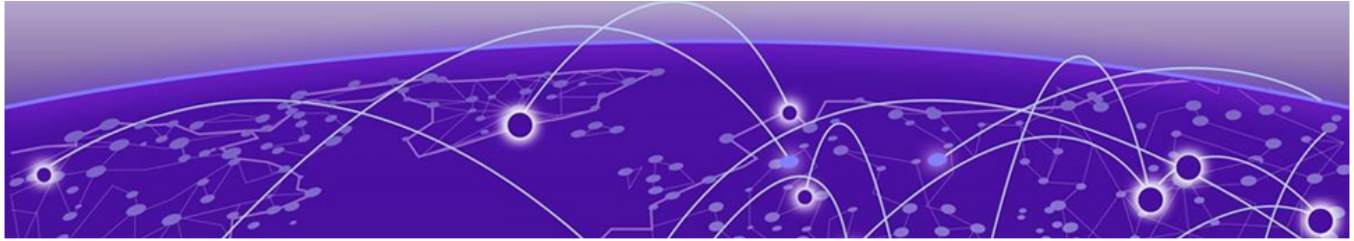
Abstract.....	v
Preface.....	vi
Text Conventions.....	vi
Documentation and Training.....	vii
Open Source Declarations.....	viii
Training.....	viii
Help and Support.....	viii
Subscribe to Product Announcements.....	ix
Send Feedback.....	ix
What's New in this Document.....	10
Supported Platforms.....	11
Deployment Preparation.....	12
Supported Device Information.....	12
Extreme OS ONE Software.....	12
Extreme OS ONE Operating System.....	13
Run Operational Diagnostics.....	13
BMC Thermal Policy.....	15
BMC Thermal Management Process for Optics.....	15
Threshold Calculations.....	15
Thermal Monitoring.....	15
Warning Threshold.....	15
Alarm Threshold and Low Power Mode.....	16
Reset Mode.....	16
Recovery from Low Power Mode.....	16
Reset Mode Recovery.....	16
Continuous Reset Mode.....	16
Limitations.....	16
Installation and Upgrade.....	17
Install Extreme OS ONE Switching and Routing Using ONIE.....	17
Recover via USB Disk.....	20
Recover via NFS.....	20
Recover via HTTP.....	21
Recover via FTP.....	21
Recover via TFTP.....	22
Firmware Fullinstall Support.....	23
Key Features.....	23
Event Log Messages.....	23
Important Extreme OS ONE Configuration and Certificate Changes.....	23
CLI Commands.....	24
View Firmware Version Information.....	28

Extreme OS ONE Firmware Upgrade Example Using CLI.....	28
Upgrade Low-Level Firmware on Supported Hardware Platforms.....	29
Automated BMC Firmware Update with OS ONE.....	33
Supported Platforms.....	33
Limitations.....	34
Automated BMC Firmware Update Implementation.....	34
SLX-OS to OS ONE Migration.....	40
Supported Migration Method.....	40
Limitations.....	40
Install OS ONE on SLX Platforms	41
OS ONE to SLX-OS Migration.....	42
Supported Migration Method.....	42
SLX-OS Image Selection (Mandatory).....	42
Install SLX-OS on OS ONE Platforms	42
Supported Upgrade Paths.....	43
Upgrade Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0.....	44



Abstract

This *Extreme OS ONE Switching and Routing Deployment Guide* version 22.2.3.0 details ONIE-based installation and upgrade procedures, firmware lifecycle operations, and platform support for Extreme 8520/8720/8730/8820. It explains Base OS vs Application OS microservices, operational diagnostics (Alpha image) on 8730, and BMC-driven thermal policy for 400C optics with warning/alarm thresholds, low-power/reset modes, and recovery behaviors. Intended for advanced IT professionals familiar with CLI, ONIE, and fabric operations.



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

[Extreme Portal](#)

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

[The Hub](#)

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

[Call GTAC](#)

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

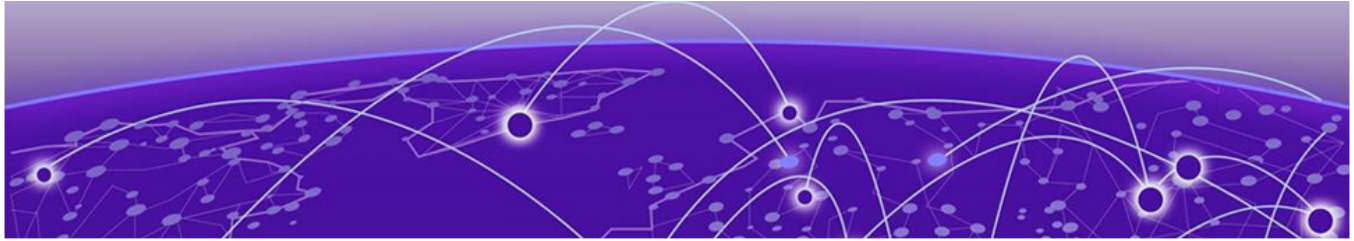
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

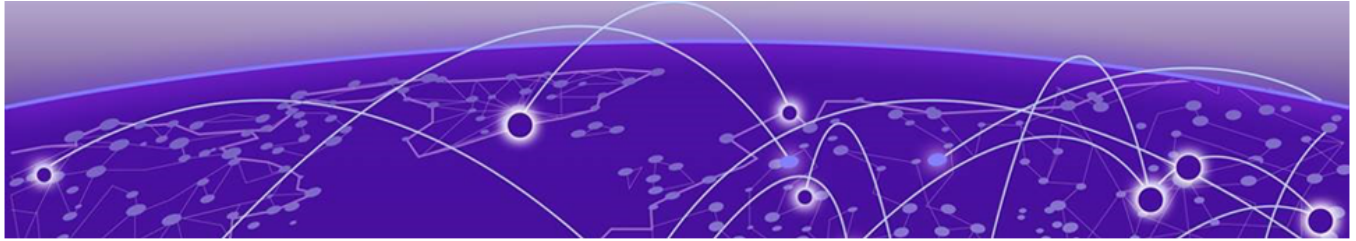


What's New in this Document

The following table describes the information added to this guide for Extreme OS ONE Switching and Routing, release 22.2.3.0:

Feature	Link
OS ONE Upgrade Switching	• Supported Upgrade Paths on page 43 • Upgrade Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0 on page 44
Automated BMC update with OS ONE	• Automated BMC Firmware Update with OS ONE on page 33 • Automated BMC Firmware Update Implementation on page 34

For more information about this release, see the *Extreme OS ONE Switching and Routing Release Notes*.



Supported Platforms

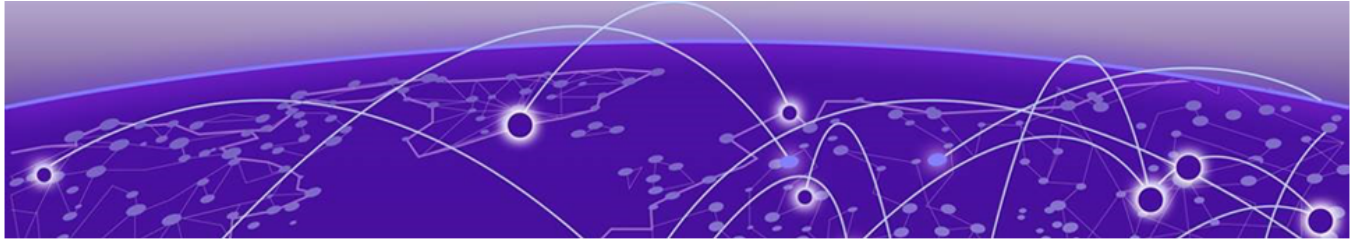
Extreme OS ONE Switching and Routing 22.2.3.0 and later releases support Extreme 8520, Extreme 8720, Extreme 8730, and Extreme 8820 hardware platforms.



Note

Although many software and hardware configurations are tested and supported for this release, all possible configurations and scenarios are beyond this document's scope.

For information about other releases, see the documentation for those releases.



Deployment Preparation

[Supported Device Information](#) on page 12

[Extreme OS ONE Software](#) on page 12

[Run Operational Diagnostics](#) on page 13

[BMC Thermal Policy](#) on page 15

Extreme OS ONE is the new operating system for IP fabrics and data centers. Extreme OS ONE Switching and Routing is an application that provides Switching and Routing functionality. You can customize the Extreme OS ONE Base for Extreme OS ONE Switching and Routing application.

Supported Device Information

Extreme OS ONE is a standalone operating system that runs on various hardware platforms, including the Extreme 8730, 8520, 8720, and 8820. Extreme OS ONE is primarily for managing devices and does not provide networking protocols without the installation of additional applications such as Extreme OS ONE Switching and Routing.

Extreme OS ONE Software

Extreme OS ONE consists of OS software and microservices that provide various services and functionality.

Extreme OS ONE architecture comprises of various components composed as microservices, such as LLDP microservice and the BFD microservice. Extreme OS ONE microservices are grouped into two major categories:

- Base OS - comprises of the application that is essential for deployment
- Application OS - comprises of the services such as Switching and Routing and SDWAN

The Application OS, Extreme OS ONE Switching and Routing 22.2.x.0 provides switching and routing capabilities.

You can download the Extreme OS ONE image from a remote server using any of the following methods:

- FTP (File Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)

- NFS (Network File System)
- USB (Universal Serial Bus)

Extreme OS ONE Operating System

Extreme OS ONE is built using the standard ONLP (Open Network Linux Platform) procedure. Installation of Extreme OS ONE is done using Open Networking Install Environment (ONIE) standard.

ONIE is a combination of a boot loader and a small operating system for bare metal network devices that provides an environment for automated provisioning or recovery of the device. The Extreme 8730 device boots the software from the images stored on its hard disk. ONIE also provides mechanisms to re-install or update the software if the normal software download process fails.

Run Operational Diagnostics

The 8730 platform has operational diagnostics, a set of hardware-level tests available as a bootable image. This image is installed on the switch and accessible through Extreme OS ONE. This is exclusive to the 8730 platform and not supported on other 8000 series platforms.

About This Task

Follow this procedure to run the operation diagnostics.

Procedure

1. To run the test suite, use the following CLIs:

```
system diagnostics run <normal | extended>
```

The command reboots the switch and runs the diagnostics image.

```
show system diagnostics
```

The command displays the test results.

2. To upgrade the image, run the **system diagnostics update** command.

```
# system diagnostics update
URL Firmware URL
disk://firmware/<filename>
usb://<filename>
scp://<username>[:<password>]@<host>[:<port>]/<filepath>
sftp://<username>[:<password>]@<host>[:<port>]/<filepath>
http[s]://[username:password@]<host>[:<port>]/<filepath>
```



Note

- The filename would be like the 'summit-aoede.1.3', which is currently packaged with OS ONE.
- You can also run operational diagnostics directly from the GRUB menu.

Example

```
32d# system diagnostics run normal
WARNING: system will be rebooted! Do you want to continue? [y/n]: y
```

```

Reloading.... please wait

                                GNU GRUB  version 2.06

/-----\
| Open Network Linux              |
| *Operational Diagnostics        |
| ONIE                            |
|                                 |
|                                 |
|                                 |
|                                 |
\-----/

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands
    before booting or `c' for a command-line.
    The highlighted entry will be executed automatically in 0s.


    Booting `Operational Diagnostics'

Loading Operational Diagnostics ...
error: no suitable video mode found.
Booting in blind mode

Initializing operational diagnostics...
Version 1.0T-1, 13:54:59 25/03/2024

Running Power On Self Test...(Normal mode)

i2c environment          PASS
fantray                  PASS
internal flash           PASS
memory                   PASS
management interface     PASS
side_band interface      PASS
loopback pci             PASS
loopback mac interface   PASS
loopback phy fiber       PASS
snake interface          PASS
asic0 reg                PASS
asic0 mem                SKIPPED

Storing diagnostics result.
Diagnostics completed.
Waiting for reboot...
[NS Info] Validating Primary BMC Image
[NS Info] Primary BMC Image Validated

<snip>

32d# show system diagnostics
Date: Sep-01-2024 03:48:56

Version: 1.0T-1
Summary: Diagnostics Pass
Mode: Normal

8730-32D:                801157-00-02 AD012350G-00043
PSU-1: Present           801162-00-00 P0142342A-C0149
PSU-2: Empty
FAN-1: Present           801166-00-02 F0032349G-00345
FAN-2: Present           801166-00-02 F0032349G-00346

```

```

FAN-3: Present      801166-00-02 F0032349G-00382
FAN-4: Present      801166-00-02 F0032349G-00391
FAN-5: Present      801166-00-02 F0032349G-00545
FAN-6: Present      801166-00-02 F0032349G-00523
FAN-7: Present      801166-00-02 F0032349G-00509

```

```

Test                Result
=====
i2c environment     PASS
fantray             PASS
internal flash      PASS
memory              PASS
management interface PASS
side_band interface PASS
loopback pci        PASS
loopback mac interface PASS
loopback phy fiber  PASS
snake interface     PASS
asic0 reg           PASS
asic0 mem           SKIPPED
32d#

```

BMC Thermal Policy

Use this topic to learn about the BMC (Baseboard Management Controller) thermal policy for Optics temperature.

BMC Thermal Management Process for Optics

The BMC thermal policy manages Optics temperature using two threshold values: Warning and Alarm (Warning < Alarm).

Threshold Calculations

- Warning Threshold = Optics Warning Threshold + Warning Threshold
- Alarm Threshold = Optics Alarm Threshold + Alarm Threshold.

Thermal Monitoring

- Every 10 seconds, sends thermal messages to the Baseboard Management Controller (BMC) with the highest temperature optics and its warning threshold.
- BMC adjusts FAN speeds based on these values.

Warning Threshold

- Extreme OS ONE generates a warning log when an optic's temperature exceeds its warning threshold. The following is an example:

```

Temperature detected on Port 5: Current Temp 66, TempHighWarn 65, TempHighAlarm
70

```

Alarm Threshold and Low Power Mode

- When an optic's temperature exceeds its alarm threshold, it enters low power mode.
- This brings down links on the port and generates error and info logs.
- Example: "QSFP 5 temperature Value: 71, Crossed Critical Threshold 70" and "QSFP 5 transitioned to LowPower mode".

Reset Mode

- If the optic's temperature continues to rise in low power mode, it enters reset mode.
- Error log: "QSFP 5 has been reset, please remove and insert the optics".

Recovery from Low Power Mode

- When the optic's temperature drops below the warning threshold in low power mode, it returns to normal power mode.
- Info log: "QSFP 5 transitioned power mode to Default".

Reset Mode Recovery

- When the optic's temperature drops below the warning threshold in reset mode, Extreme OS ONE takes it out of reset mode.
- Info log: "QSFP 5 taken out of reset mode"

Continuous Reset Mode

If the optics enters reset mode and is subsequently taken out of reset mode five times via software, the user must physically remove and re-insert the optics to restore connectivity.

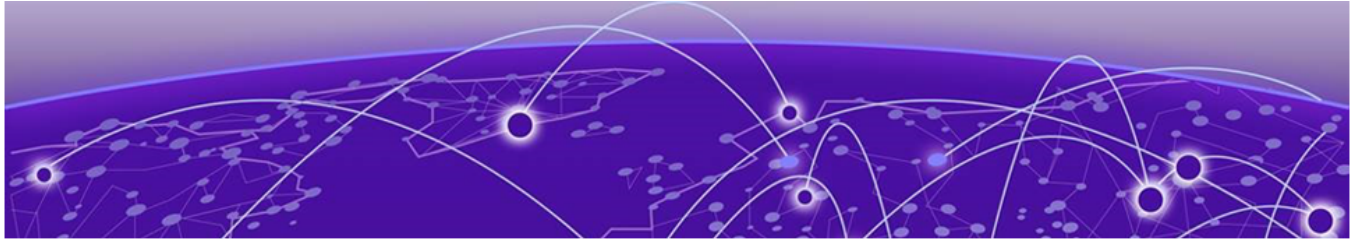
Limitations

- Only Extreme Qualified optics participate in the thermal policy.
- Only 400G Fiber optics are eligible to participate in the thermal policy.



Note

Correction threshold values are not available, so the thresholds read from the Optics are considered final thresholds.



Installation and Upgrade

[Install Extreme OS ONE Switching and Routing Using ONIE](#) on page 17
[Firmware Fullinstall Support](#) on page 23
[View Firmware Version Information](#) on page 28
[Extreme OS ONE Firmware Upgrade Example Using CLI](#) on page 28
[Upgrade Low-Level Firmware on Supported Hardware Platforms](#) on page 29
[Automated BMC Firmware Update with OS ONE](#) on page 33
[SLX-OS to OS ONE Migration](#) on page 40
[OS ONE to SLX-OS Migration](#) on page 42
[Supported Upgrade Paths](#) on page 43

The topics in this section provide the information required to install and upgrade Extreme OS ONE Switching and Routing on a device.

For TPVM installation, see the *TPVM IAH Extension* topic in the *Extreme OS ONE Switching and Routing Management Configuration Guide*.



Note

Platform migration is supported on the Extreme 8520, 8720, and 8820 series. The Extreme 8730 ships with Extreme OS ONE and does not support migration.

Install Extreme OS ONE Switching and Routing Using ONIE

You can install Extreme OS ONE Switching and Routing software using ONIE.

Before You Begin

Open Network Install Environment (ONIE) acts as a bootloader and a lightweight Linux-based provisioning framework that allows vendors and users to install a network operating system over the network or from local media. You can install Extreme OS ONE Switching and Routing software onto a bare metal device that has ONIE preinstalled.

- Throughout the installation process, a serial console must be connected to the device.

- The out-of-band management Ethernet interface must be connected if you are using a remote NFS share, HTTP, FTP, or TFTP:
 - The availability of a DHCP server on the LAN for this Ethernet interface may enable you to skip the need to manually configure the ONIE to connect to one of the network-based methods of transferring the software.
 - If a DHCP server is not available, you need the default gateway, network mask, and an IP address that is not in use on the network to which the Ethernet interface is connected.

About This Task

Follow this procedure from the serial console to install Extreme OS ONE Switching and Routing software using ONIE:

Procedure

1. Access the ONIE Recovery Shell.

After updating the passwords, the system confirms that the admin and Grub passwords have been updated successfully.



Note

- **First Login Requirements:** The device is pre-configured with a default username 'admin'. Upon first login, you are prompted to update the default password. Contact your Extreme Networks sales representative for the default password.
- **Changing Admin and Grub Passwords:** During the first login via CLI, users are prompted to change both the admin and Grub passwords. Users can choose to
 - a. Set a new password for the "admin" user.
 - b. Use the same admin password for Grub (by pressing Enter)

```
Device: login: admin
Password:

*** Please change password for admin account and Grub bootloader now.
***
Use Control-C to exit or press 'Enter' key to proceed.

Changing default password for "admin" and Grub
Current admin password:
Enter new admin password:
Re-type new admin password:
Enter new password for Grub 'root' user login (Press Enter to use admin
password for Grub) : OS ONE 'admin' and Grub 'root' user passwords
updated successfully
device#
```

- a. Reboot the device using the CLI or power-cycle.
- b. When the BIOS (Basic Input/Output System) splash screen is displayed, use the **Down Arrow** key to access the GRUB boot menu and stop the boot timer.
- c. Select **ONIE** from the first menu, and press the **Down Arrow** key to stop the boot timer.

- d. Update the Grub login credentials by entering the following details:

Grub username: root

Grub password: As set during the first login

To change or reconfigure the Grub password again, use the CLI command:

configure terminal -> system -> grub -> username <name> password <password>.



Note

Factory Default and Grub Login:

- Post-factory reset, the admin and Grub passwords revert to defaults and need to be changed by the user.
- When entering the ONIE prompt during reload, users must enter the Grub login credentials (username: root, password: user-set password).

- e. Select **ONIE: Rescue**, and press **Enter** when prompted.

The ONIE shell opens.

You can use ONIE for recovering or upgrading the device.

2. Complete one of the following step:

- If a DHCP server is running on the network, proceed to the next step.
- If you are using a remote server to download the firmware, go to step 5 on page 19.

3. Check connectivity to the server hosting the software.

- a. Ping the remote server from which you intend to download the software.
- b. If the ping fails, run the following commands to gather information on the connection state.

```
ip addr
ip route show
ifconfig
```

If there are any errors, complete the step 4 to resolve them. Otherwise, proceed to step 5 on page 19 .

4. Configure static networking on eth3 for ONIE.

- a. Add the IP address to the eth3 interface.

```
ONIE:/ #ip addr add <ip-addr/mask> dev eth3
```

- b. Configure the default gateway.

```
ONIE:/ # ip route add default gw <gateway-ip-addr> eth3
```

5. Download and install the Extreme OS ONE firmware using one of the following remote server methods:

- [Recover via USB Disk](#) on page 20
- [Recover via NFS](#) on page 20
- [Recover via HTTP](#) on page 21
- [Recover via FTP](#) on page 21
- [Recover via TFTP](#) on page 22

A checksum validation is done before installing the firmware.

6. Activate the firmware using `Activate gRPCs`.
7. Verify if the installation is successful using `Verify gRPCs`.

Recover via USB Disk

You can recover via USB disk.

About This Task

Follow this procedure to recover the system configuration via USB disk.

Procedure

1. From the serial console, download and decompress the software tarball.
2. Transfer the resulting directory to an inserted USB 3.0 device.
3. Eject or unmount the USB device and insert it into the USB port on the front panel of the 8730-32D device.
4. Run the `fdisk -l` command. In the output, locate the device identifier of the inserted USB device.

The USB device is generally the last device listed.

5. Run the `mkdir /media` and `mount /dev/<device-identifier> /media` commands.

You might see a warning, but the disk will mount.

6. Change directory to the Extreme OS ONE software that you want to install and start the installation using the `onie-nos-install file://`
7. Select the binary file for the Extreme 8730-32D.

```
ONIE:/ #cd media/  
ONIE:/ media/ #ls OSOneSR-22.2.3.0-110.bin
```

The device reboots and loads the software.

Recover via NFS

You can recover via NFS.

About This Task

Follow this procedure to recover the system configuration via NFS.

Procedure

1. On a Linux device, configure an NFS share, download and decompress the software tarball, and move the resulting directory to the root of the NFS share.
2. On the Extreme 8730-32D device, configure and verify network connectivity to the server.

- a. Configure the network.

```
# ifconfig eth3 10.xxx.xx.xxx netmask 255.x.x.x up
```

- b. Configure the default route.

```
# route add default gw 10.xxx.xx.x
```

- c. Verify network connectivity to the server.

```
# ping 10.xxx.xx.x
```

3. Run the **mkdir /media** and **mount /<path-to-NFS-share>/ /media** commands.
If an error results, troubleshoot the **mount** command. You might need more parameters or a more explicit path.
4. Change directory to the Extreme OS ONE software that you want to install.

```
ONIE:/ #cd media/  
ONIE:/ media/ #ls OSOneSR-22.2.3.0-110.bin
```

5. Select the binary file using the **onie-nos-install file://** for the Extreme 8730-32D.

The process takes approximately 15 to 20 minutes to complete. The device reboots and loads the software.

Recover via HTTP

You can recover via HTTP.

About This Task

Follow this procedure to recover the system configuration via HTTP.

Procedure

1. On a web server, download and decompress the software tarball and move the resulting directory to the root of the web server.
2. Modify the permissions of the directory to allow access for the web server daemon.
3. Verify that the software directory is accessible by using a web browser to access the directory.
4. On the Extreme 8730-32D, configure and verify network connectivity to the server.
 - a. Configure the network.

```
# ifconfig eth3 10.xxx.xx.xxx netmask 255.xxx.xxx.x up
```

- b. Configure the default route.

```
# route add default gw 10.xxx.xx.x
```

- c. Verify network connectivity to the server.

```
# ping 10.xxx.xx.x
```

5. Run the **onie-nos-install** command with the URL to the binary for the device.

```
ONIE:/ #onie-nos-install http://<URL-to-binary>/OSOneSR-22.2.3.0-110.bin
```

Recover via FTP

You can recover via FTP.

About This Task

Follow this procedure to recover the system configuration via FTP.

Procedure

1. On an FTP server, download and decompress the software tarball and move the resulting directory to the root of the FTP server.

2. Modify the permissions of the directory to allow access for the FTP server daemon. The FTP server must allow anonymous access.
3. Verify that the software directory is accessible by using an FTP client to access the directory.
4. On the Extreme 8730-32D device, configure and verify network connectivity to the server.

- a. Configure the network.

```
# ifconfig eth3 10.xxx.xx.x netmask 255.xx.xx.x up
```

- b. Configure the default route.

```
# route add default gw 10.xxx.xx.x
```

- c. Verify network connectivity to the server.

```
# ping 10.xxx.xx.x
```

5. Run the **onie-nos-install** command with the URL to the binary for the device.

```
ONIE:/ #onie-nos-install ftp://<URL-to-binary>/OSOneSR-22.2.3.0-110.bin
```

Recover via TFTP

You can recover via TFTP.

About This Task

Follow this procedure to recover the system configuration via TFTP.

Procedure

1. On a TFTP server, download and decompress the software tarball and move the resulting directory to the root of the TFTP server.
2. Modify the permissions of the directory to allow access for the TFTP server daemon.
3. On the Extreme 8730-32D device, configure and verify network connectivity to the server.

- a. Configure the network.

```
# ifconfig eth3 10.xx.xx.xx netmask 255.xx.xx.x up
```

- b. Configure the default route.

```
# route add default gw 10.xxx.xx.x
```

- c. Verify network connectivity to the server.

```
# ping 10.xxx.xx.x
```

TFTP might appear to be non-operational while transferring the file.

4. Run the **onie-nos-install** command with the URL to the binary for the device.

```
ONIE:/ #onie-nos-install ftp://<URL-to-binary>/OSOneSR-22.2.3.0-110.bin
```

Firmware Fullinstall Support

This topic outlines the step-by-step process for performing a full, clean install of the provided Extreme OS ONE firmware. The process safely removes existing partitions while preserving essential SSH and certification files.



Note

Ensure that you have a valid URL containing the appropriate Extreme OS ONE binary image.

Key Features

- Installation of firmware using the Extreme OS ONE CLI
- Deletion and creation of managed partition
- Replacement of current configuration with the default Extreme OS ONE settings
- Automatic preservation of SSH certification files

Event Log Messages

Event Type	Log Message
Pre-install event	Preparing Device for Fullinstall. This will take some time
Invalid image extension event	Fullinstall failed. Cannot be done on .app and .incr images
Successful validation event	Device ready for Fullinstall in %s. Device will reboot now.

Important Extreme OS ONE Configuration and Certificate Changes

Extreme OS ONE Configuration: Installing new firmware overwrites your current configuration with the default Extreme OS ONE settings. To preserve your existing configuration, back it up to an external server using **copy running-config file <external server details>** command. You can then restore it using **copy file <external server details> running-config** command.

Management Certificates: The following folders are automatically backed up and restored during the firmware installation. If you want to remove these certificate files, use the 'no-preserve' CLI option.

- /etc/ssh
- /var/data/cert-mgmt/ca-trust
- /var/data/cert-mgmt/app-cert
- /var/data/cert-mgmt/jwt
- /var/data/ztp

CLI Commands

The following table describes CLI commands to complete the system firmware fullinstall:

Full Syntax	system firmware fullinstall <url path of firmware file>		
Parameter descriptions	Parameter	Type	Description
	URL	string	URL or Filepath of firmware. disk://firmware/<filename> -OR- usb://<filename> -OR- scp[sftp]://<username>:<password>@<host>[:port]/<filepath> [vrf vrf-name] -OR- http[https]://[username:password@]<host>[:port]/<filepath> [vrf vrf-name]
	no-preserve	optional argument	By default, it's preserved or optionally you can prefer not to preserve using optional parameter no-preserve. wherever applicable, modify this.
Command mode	exec mode		
Permissions & Validations	Admin user only		
Behavior description	This command simulates the 'onie-nos-install' process for new Extreme OS ONE firmware. Here's what it does: • Deletes all device partitions • Preserves management certification files by default (unless 'no-preserve' option is used) • Initiates new Extreme OS ONE firmware installation from ONIE • Restores SSH configuration file and necessary certification files		

Help strings	<pre> 32d# system firmware commit Commit firmware version fullinstall Full Install firmware on switch rollback firmware version uninstall Uninstall App update Update firmware on switch 32d# system firmware fullinstall URL disk://firmware/<filename> -OR- usb://<filename> -OR- scp[sftp]:// <username>:<password>@<host>[:port]/<filepath> -OR- http[https]: //[username:password@]<host>[:port]/<filepath> 32d# system firmware fullinstall <image path> # system firmware fullinstall dis <cr> no-preserve Remove management certificates </pre>
Error messages	<pre> Fullinstall failed. Cannot be done on .app and .incr images. Firmware image validation failed. Invalid extension for <wrong image path> %Error: Vrf is applicable only for scp[sftp] and http[https]. </pre>
Related commands	show version, show firmware

Related PROTO files	The following openconfig gNOI RPCs are used or supported: <pre>rpc Activate(ActivateRequest) returns (ActivateResponse); rpc Verify(VerifyRequest) returns (VerifyResponse);</pre> The following are the corresponding Request and Response messages: <pre>// The ActivateRequest is sent by the Client to the // Target to initiate a change // in the next bootable OS version that is to be // used on the Target. // Dual Supervisor Target which requires installing // the entire system with // one Install RPC MUST return // NOT_SUPPORTED_ON_BACKUP error when requested // To Activate on standby Supervisor. message ActivateRequest { // The version that is required to be activated // and optionally immediattely // booted. string version = 1; // For dual Supervisors setting this flag // instructs the Target to perform the // action on the Standby Supervisor. bool standby_supervisor = 2; // If set to 'False' the Target will initiate the // reboot process immediattely // after changing the next bootable OS version. // If set to 'True' a separate action to reboot // the Target and start using // the activated OS version is required. This // action CAN be executing // the gNOI.system.Reboot() RPC. bool no_reboot = 3; } // The ActivateResponse is sent from the Target to // the Client in response to the // Activate RPC. It indicates the success of making // the OS package version // active. message ActivateResponse { oneof response { ActivateOK activate_ok = 1; ActivateError activate_error = 2; } } // If the Target is already running the requested // version in ActivateRequest, // then it replies with ActivateOK. If the Target // has the OS package version // requested in ActivateRequest then it replies with // ActivateOK and proceeds to // boot. // A dual Supervisor Target which requires // installing the entire system with // one Install RPC, will activate the image on all // Supervisors in response to // one Activate RPC. The Target should activate the // image on both Supervisors // with the least impact possible to forwarding. //</pre>
----------------------------	---

	<pre> // On a dual Supervisor Target which requires one Install RPC per supervisor, // performing this RPC on the Active Supervisor triggers a switchover before // booting the (old)Active Supervisor. The Target should perform a switchover // with the least impact possible to forwarding. message ActivateOK { } message ActivateError { enum Type { // An unspecified error. Must use the detail value to describe the issue. UNSPECIFIED = 0; // There is no OS package with the version requested for activation. This is // also used for an empty version string. NON_EXISTENT_VERSION = 1; // Dual Supervisor Target which requires installing the entire system // with one Install RPC MUST return NOT_SUPPORTED_ON_BACKUP error when // requested to Activate on standby Supervisor. NOT_SUPPORTED_ON_BACKUP = 2; } Type type = 1; string detail = 2; } message VerifyRequest { } message VerifyResponse { // The OS version currently running. string version = 1; // Informational message describing fail details of the last boot. This MUST // be set when a newly transferred OS fails to boot and the system falls back // to the previously running OS version. It MUST be cleared whenever the // systems successfully boots the activated OS version. string activation_fail_message = 2; VerifyStandby verify_standby = 3; // Dual Supervisor Targets that require the Install/Activate/Verify process // executed once per supervisor reply with individual_supervisor_install set // to true bool individual_supervisor_install = 4; } </pre>
Example output using gNOI	<pre> \$ gnoic -a 192.x.x.x:4x3 -u admin -p <default password> --tls-ca ca.cert.pem os activate --version fullinstall-/var/data/disk/ firmware/OSOneSR-22.2.3.0-110.bin </pre>

View Firmware Version Information

You can view the primary and secondary firmware version information.

About This Task

Follow this procedure to view firmware version information.

Procedure

1. View the primary and secondary firmware version information.

```
show firmware
```

2. View the last five firmware versions activated on the device.

```
show firmware history
```

3. View the firmware logging information.

```
show logging audit firmware
```

Extreme OS ONE Firmware Upgrade Example Using CLI

The Extreme OS ONE firmware contains primary and secondary images. When new firmware is installed, the image in the secondary location is removed and the image in the primary location is moved to the secondary location. The new image is installed in the primary location.

You can upgrade the firmware using one of the following commands.

```
# system firmware update disk://firmware/filename

# system firmware update usb://filename

# system firmware update scp://username:password@host[:port]/filepath

# system firmware update sftp://username:password@host[:port]/filepath

# system firmware update http://[username:password@]host[:port]/filepath

# system firmware update https://[username:password@]host[:port]/filepath
```

For details on command syntax and options such as `vrf`, `force`, and `default-config`, see *ExtremeCloud Orchestrator Command Reference Guide*.

Both IPv4 and IPv6 addresses are supported.

- If the firmware update is successful, the system is rebooted automatically to activate the new version.

The reboot reason is updated to `firmware upgrade` to indicate firmware update or rollback. The reboot reason is stored in the `chassis-0` property.

- Configurations persist after reboot, and all microservices are expected to come up.
- If any microservice fails to come up within the specified duration, an automatic rollback to the previous image is triggered.

Upgrade Low-Level Firmware on Supported Hardware Platforms

You can upgrade the various firmware on the 8730-32D, 8820, and 8520 hardware platforms.

About This Task



Note

USB flash drives are compatible with FAT, EXT, and NTFS file systems. The 8820 and 8520 devices support only BMC upgrade.

Follow this procedure to upgrade the firmware on the Extreme 8730-32D, 8820, and 8520 hardware platforms.

Procedure

1. Upgrade BMC on 8730-32D, 8820, 8720, and 8520 hardware platforms.

To upgrade the BMC firmware, run the following command:

```
system programmable bmc update <file_input>
```

- Supported File Input Formats
 - URL:Firmware URL
 - disk://firmware/<filename>
 - usb://<filename>
 - scp://<username>[:<password>]@<host>[:<port>]/<filepath>
 - sftp://<username>[:<password>]@<host>[:<port>]/<filepath>
 - http[s]://<username>[:<password>]@<host>[:<port>]/<filepath>
- Upgrade Process
 - Warning: Power interruption during the upgrade process may cause issues. Confirm to proceed.
 - Firmware file download and validation.
 - Flashing firmware on BMC (takes approximately 3-4 minutes).
 - BMC reset (occurs after around 8 minutes).
- Error Message
 - Invalid programmable component
 - Firmware image error
 - URL path error/incomplete
 - Downloading firmware image from host failed
 - Wrong IP: port error
 - File transfer failed
 - BMC IP configuration error
 - Flashing operation failed
- Troubleshooting

Check the `/var/log/fw_upgrade.txt` log file for internal errors.

- Example Command

```
system programmable bmc update scp://gm@10.xx.xx.xx/home/gmh/source_codes/firmware-  
upgrade/8730_BMC_1.08.00_PriAndGold_signed_DevKey_000_SecRev_000_install.hpm
```

- Verify BMC Firmware Version

```
show bmc-status | include Firmware
```

- Example output

```
Firmware Revision : 1.11
```

2. Upgrade Firelight firmware on the 8730-32D hardware platforms.

To upgrade the Firelight firmware, run the following command:

```
system programmable um-switch update <file input>
```

- Supported File Input Formats

- disk://firmware/<filename>
- usb://<filename>
- scp[sftp]://<username>:<password>@<host>[:port]/<filepath>
- http[https]://[username:password@]<host>[:port]/<filepath>

- Upgrade Process

- a. The system downloads and validates the firmware file.
- b. The system flashes the firmware on the um-switch, which may take several minutes.
- c. The um-switch resets after approximately 5 minutes to complete the backend flash write.

- Error Messages

- Invalid programmable component or firmware image
- URL path error or unknown host IP
- File transfer failure
- BMC IP configuration error
- Flashing operation failure

- Troubleshooting

Check the `/var/log/fw_upgrade.txt` log file for internal errors.

- Verify Firmware Version

To check the Firelight firmware version, run the **show system internal iobm-system-info | include Iobm Fw ver** command.

3. Upgrade BIOS on 8730-32D hardware platforms.

To upgrade BIOS on 8730-32D platform, run the following command:

```
system programmable bios update <file_input>
```

- Supported File Input Formats

- disk://firmware/<filename>: Update from a file on the local disk.
- usb://<filename>: Update from a file on a USB drive.

- `scp[sftp]://<username>:<password>@<host>[:port]/<filepath>`: Update from a file on a remote host using SCP or SFTP.
- `http[https]://[username:password@]<host>[:port]/<filepath>`: Update from a file on a remote host using HTTP or HTTPS.

- Output

```
WARNING: Power must not be interrupted and BIOS will be inaccessible during this
time!
Do you want to continue? [y/n]: y

%Info: Firmware file downloaded and validated for BIOS
%Info: Flashing Firmware on BIOS...This will take some time
%Info: Flashing firmware on BIOS completed in 4m47s
```

- Error Messages

- %Error: Invalid programmable component
- %Error: Firmware image error
- %Error: Invalid firmware image as input for <comp>
- %Error: Downloading firmware image from host failed, wrong URL format or unknown host IP
- %Error: File transfer failed
- %Error: Downloading firmware image from host failed, wrong URL format or unknown host IP
- %Error: BMC IP configuration error
- %Error: Flashing operation failed, error: rpc error: code = Unknown desc = exit status 1

- Verify BIOS Version

To verify the BIOS version, run the following command:

```
32d# show system health | include BIOS Version
BIOS Version:0.20.0
```

4. Upgrade HwRoT on 8730-32D hardware platforms.

To upgrade Hardware Root of Trust (HwRoT) on 8730-32D platform, run the following command:

```
system programmable micro-controller update <file input>
```

- Supported File Input Formats

- `disk://firmware/<filename>`
- `usb://<filename>`
- `scp[sftp]://<username>:<password>@<host>[:port]/<filepath>`
- `http[https]://[username:password@]<host>[:port]/<filepath>`

- Upgrade Process

- a. The system downloads and validates the firmware file.
- b. The system flashes the firmware onto the micro-controller.
- c. The system reboots.

- Important Notes

- Do not interrupt the power supply during the upgrade process.

- The um-switch is inaccessible during this time.
 - Verification
 - After the system reboots, check the version of HwRoT in the boot logs.
 - The version is displayed as "Application version: <version_number>".
 - Error Handling
 - If the upgrade fails, check the /var/log/fw_upgrade.txt file for internal errors.
 - Error messages are displayed on the console, indicating the cause of the failure.
5. Upgrade Power/CPU/Port -CPLD (Complex Programmable Logic Device).

To upgrade CPLD for Power, CPU or Port on 8730-32D platform, run the following command:

```
system programmable <power-cpld | cpu-cpld | power-cpld> update <file input>
```

- Supported File Input Formats
 - disk://firmware/<filename>
 - usb://<filename>
 - scp[sftp]://<username>:<password>@<host>[:port]/<filepath>
 - http[https]://[username:password@]<host>[:port]/<filepath>
- Output

A warning message will be displayed, indicating that power interruption must be avoided and the power-CPLD will be inaccessible during the upgrade process.

Confirmation Prompt
Do you want to continue? [y/n]:

- Upgrade Process
 - a. Firmware file download and validation
 - b. Flashing firmware on the CPLD component
- Upgrade Compilation

The upgrade process takes several minutes to complete. Upon completion, a success message is displayed.

- Error Messages
 - %Error: Invalid programmable component
 - %Error: Firmware image error
 - %Error: Invalid firmware image as input for <comp>
 - %Error: Downloading firmware image from host failed, wrong URL format or unknown host IP
 - %Error: file transfer failed
 - %Error: Downloading firmware image from host failed, wrong URL format or unknown host IP
 - %Error: BMC ip configuration error
 - %Error: Flashing operation failed, error: rpc error: code = Unknown desc = exit status 1
- Troubleshooting

Verify the `/var/log/fw_upgrade.txt` log file for internal errors.

- Verification

To verify the CPLD version, run the **show version | include System CPLD** command.

The command displays the System CPLD version, including the Port-CPLD, Power-CPLD, and CPU-CPLD versions.

What to Do Next

After a firmware upgrade, perform a full power cycle of the device.

- Power cycle the device: Disconnect power from the device, wait at least 30 seconds, and then restore power. This ensures the upgrade is properly applied.
- If a physical power cycle is not possible, perform an IPMI cold reset using the **ipmitool mc reset cold** command.

Automated BMC Firmware Update with OS ONE

The Automated BMC Firmware Update capability ensures that supported switches running Extreme OS ONE are upgraded with the latest validated Baseboard Management Controller (BMC) firmware during an OS ONE software updates.

With this capability, the BMC firmware packaged within the OS ONE software image is automatically installed and activated when a newer version is detected on the device. This ensures your devices always run compatible, tested firmware combinations and helps maintain firmware consistency and reduces the need for manual intervention.

For manual BMC firmware update information, see [Upgrade Low-Level Firmware on Supported Hardware Platforms](#) on page 29.

Supported Platforms

This capability is supported on the following platforms:

- 8520-48y
- 8520-48xt
- 8720-32c
- 8730-32d



Note

- Support is limited to devices running OS ONE SR images.
- Not supported on SD-WAN platforms or non-SR devices (for example, 9740).
- Supported only on production (GA) hardware.

Limitations

- **Downgrade protection:** BMC won't auto-update if you're downgrading to an OS ONE SR image with an older BMC version
- **Minimum version requirement:** Your current BMC needs to be at a certain version (starting with the previous minor version in the first release)
- **SLX to OS ONE migration:** No auto-BMC-update if you're migrating from SLX-OS. Use the CLI to update BMC before/after migration instead.

Automated BMC Firmware Update Implementation

Learn about the automated BMC firmware update implementation strategies.

Firmware Distribution, Detection & Boot Processing

Firmware Packaging & Distribution

- BMC firmware binaries packaged as compressed tar archives
- Metadata descriptors accompany firmware binaries
- Stored in Extreme Networks artifactory infrastructure
- Integrated into OS ONE SR image during build phase
- One latest-compatible binary per supported platform
- Firmware sourced from original equipment manufacturer (OEM) suppliers

Vendor-Provided Update Tools

- IPMItool (Intelligent Platform Management Interface Tool)
- Yafuflash (Yet Another Firmware Update Flash utility)

Pre-Boot Update Detection & Prompting

- Firmware metadata extracted from binary image during update invocation
- Analysis determines if pending SR update involves BMC firmware changes
- Detection also identifies FireLight firmware component updates
- Informational prompt notifies operator of extended update duration
- System requests explicit user confirmation before proceeding
- Update progression contingent upon positive user response

Early Boot Initialization Framework

- `tierra_early_init` service executes during early boot phase
- Service runs before platform and OS ONE service initialization
- Implemented as `systemctl` one-shot service
- All required device drivers pre-initialized by execution time
- Firmware update tools ready and operational

Initialization Sequencing

1. Query current running BMC firmware version via IPMI interface
2. Retrieve target firmware version metadata from installation directory
3. Verify upgrade path compatibility from current to target version
4. Invoke BMC update if version disparity and upgrade path validation confirmed

*Update Execution & Activation***Backend Update Orchestration**

- Existing OS ONE BMC firmware update backend script reused
- Backend module encapsulates platform-dependent behavior
- Implements vendor-recommended firmware update sequences
- Handles platform-specific activation procedures

Backend Script Responsibilities

- Platform-specific update tool selection and invocation
- BMC configuration state preservation (vendor-specific flags)
- Firmware activation and cold reboot coordination
- Post-activation BMC reachability validation
- Error logging and status reporting

Verification & State Management

- Post-activation monitoring of BMC reachability
- Timeout threshold based on expected BMC cold start latency
- Framework validates active BMC firmware version matches target
- For 8730-32d: FireLight fabric firmware update initiated post-BMC
- Sequential update ensures proper state management and dependency resolution
- Update status logged to serial console and filesystem

*Failure Handling & Recovery***Failure Mode Classification****Forgiving Mode (Default)**

- BMC update failure does not impede progression to updated OS ONE version
- Device boots into new SR with legacy BMC firmware
- Prioritizes system availability over firmware synchronization

Hard Dependency Mode

- Automatic rollback triggered if system firmware update methodology used
- ONIE/full-install methodologies continue boot progression (no rollback target)
- Used when OS ONE SR version tightly coupled to BMC version
- Architectural design constraints make this scenario remote

Failure Scenarios & Outcomes

Scenario A: Firmware Update Tool Failure

- Vendor-provided update tool terminates with non-zero exit status
- BMC continues operation with incumbent firmware version
- No firmware state corruption occurs
- BMC remains in operational state

Scenario B: Update Timeout Expiration

- Firmware update tool fails to complete within configured timeout
- Timeout interval based on vendor-specific latency baseline
- Update process forcibly terminated
- BMC retains pre-update firmware
- Device continues normal operations

Scenario C: BMC Reachability Loss

- BMC fails to respond to IPMI probe requests within activation timeout
- Device continues boot in forgiving mode or initiates rollback (hard dependency)
- BMC may recover independently
- Manual intervention may be required in persistent failure scenarios

Persistent Failure State Management

- Failure status recorded in device filesystem upon initial update attempt
- Subsequent device reboots reference state record
- Retry attempts suppressed until next OS ONE image update
- Independent BMC downgrade prevents automatic retry
- Design prevents infinite retry loops in mismatched configurations

Operational Monitoring & Diagnostics

Firmware Version Reporting

- Show version command provides dual-layer firmware information
- Current active firmware: presently running BMC firmware version
- Expected component firmware: target version for installed OS ONE release
- Version mismatch indicator displayed if applicable
- Rapid identification of out-of-sync configurations
- Manual remediation via system programmable update CLI

Techsupport Bundle Integration

- Techsupport diagnostic collection aggregates firmware update logs
- Vendor update tool logs included in support bundle
- Detailed update execution traces captured
- Error diagnostics and state transition events logged

- Enables efficient post-mortem analysis
- Accelerates technical support resolution

Performance Impact & Resource Requirements

Image Size Overhead

- Unified SR image includes all four supported platform BMC binaries
- BMC firmware binaries approximately 30 MB each (uncompressed)
- Total uncompressed size: ~120 MB for all four binaries
- Post-compression size: ~80 MB
- Measurable but acceptable increase to distribution package size

Boot Latency Impact

- Latency increase occurs during initial update cycles
- Firmware version mismatch triggers automatic update execution
- Latency variance is platform-dependent
- Subsequent reboots exhibit normal boot latency (firmware synchronized)
- 8520/8720 series: 4–5 minutes additional boot time
- 8730-32d (BMC + FireLight): 16–18 minutes total impact

Platform-Specific Breakdown

- 8520-48y/48xt: BMC update 2–3 minutes, FireLight N/A
- 8720-32c: BMC update 2–3 minutes, FireLight N/A
- 8730-32d: BMC update 10–12 minutes + FireLight 6 minutes
- Total 8730-32d impact: 16–18 minutes

Computational Requirements

- BMC firmware update operations are I/O-bound
- Not compute-intensive
- No elevated CPU utilization during execution
- No memory pressure introduced
- Update toolsets (IPMItool, Yafuflash) execute asynchronously
- Minimal resource consumption footprint

Technical Dependencies & Prerequisites

IPMI Interface Availability

- Functional IPMI interface required
- Query current firmware version via IPMI interface
- Verify activation via IPMI probe requests
- IPMI LAN interface support

- IPMI serial interface support
- Must be operational prior to update initiation

Vendor Tool Requirements

- Platform-specific firmware update tools mandatory
- Tools pre-installed in early boot environment
- Tools must be operational at initialization time
- IPMITool required for 8520/8720 platforms
- Yafuflash required for 8730-32d platform
- All drivers initialized before tool execution

Metadata Format Specification

- Firmware metadata descriptors conform to standardized schema
- Version specifications included
- Upgrade path constraints enforced
- Failure behavior directives specified
- Timeout values defined
- Dependency information documented

*Implementation Limitations & Design Constraints***Unidirectional Update Path**

- Automated update mechanism enforces upgrade-only progression
- Downgrade operations not automatically executed
- OS ONE release with older BMC firmware triggers no update
- Manual downgrade via CLI possible but unsupported by retry framework
- User agency preserved in exceptional scenarios

Minimum BMC Version Threshold

- Automatic updates only executed from validated upgrade source versions
- Current policy restricts upgrades from immediately preceding minor version
- Significantly older BMC may require manual CLI update first
- Ensures upgrade path stability and compatibility
- Contact Extreme Networks Support for version threshold queries

SLX-OS Migration Exclusion

- Devices migrating from legacy SLX OS do not qualify
- Automatic BMC update disabled during migration
- Manual firmware update via system programmable update CLI required
- Update before migration from SLX OS
- OR update after migration to Extreme OS ONE

GA Device Requirement

- Feature exclusively enabled for GA (General Availability) production devices
- Non-GA and prototype devices excluded
- Device classification determined via Part-number field in ONIE EEPROM
- Ensures tested and certified configuration management

*BMC State Coupling & Service Dependencies***Services Dependent on BMC Functionality**

- Services may experience transient unavailability during update
- Potential failure modes include:
 - Sensor monitoring discontinuity (thermal, power supply status)
 - Serial-over-LAN (SOL) session interruption
 - IPMI event log accumulation pause
 - Out-of-band power management unavailability
- Dependencies are time-limited to update duration
- All unavailability resolves upon BMC reactivation
- Services resume normal operation post-update

Dependency Resolution

- Dependencies are time-limited to update duration
- All unavailability resolves upon BMC reactivation
- Services resume normal operation post-update
- Plan firmware updates during acceptable maintenance windows

*CLI Operations Reference***Firmware Version Inspection**

- Command: show version
- Output includes:
 - Current active BMC firmware version
 - Expected component firmware version for current OS ONE release
 - Version mismatch indicator (if applicable)
- Command: system programmable update
- Manually initiates BMC/FireLight firmware update
- Operates outside automated OS ONE update flow
- Equivalent to legacy OS ONE CLI-initiated BMC update

Manual Firmware Update

- Command: system programmable update
- Manually initiates BMC/FireLight firmware update

- Operates outside automated OS ONE update flow
- Equivalent to legacy OS ONE CLI-initiated BMC update

OS ONE Update Invocation

- Supported methodologies:
 - firmware update <target-image-path>
 - full-install <target-image-path>
 - ONIE install via network boot
- All methodologies trigger identical BMC update detection
- Execution occurs during subsequent boot sequence

SLX-OS to OS ONE Migration

This procedure provides instructions to migrate supported platforms from **SLX-OS** to **OS ONE**.

Supported Migration Method

CLI-based migration method (Recommended for controlled upgrades)



Important

- Migration is **disruptive** and results in a **cold reboot**.
- Post-migration, a **System Firmware Commit** must be executed before the device is placed into use.

Limitations

- Third-Party Virtual Machine (TPVM) partition will be removed as part of the migration and cannot be recovered post-migration.
- Rollback to SLX-OS is not supported after migration is completed. Downgrade requires ONIE-based installation.
- Configuration migration is not supported. Manually reapply configuration after OS ONE installation.
- For SLX-OS to OS ONE 22.2.3.0 migration, executing a system firmware full-install after migration may render the device unusable. Full-install after migration is not recommended.
- Use system firmware upgrade for post-migration upgrades.
- OSOneSR-22.2.3.0-110.bin is the recommended build for migration. Firmware upgrade and firmware full-install function as expected in this release.

Install OS ONE on SLX Platforms

You can install OS ONE on SLX platforms.

Before You Begin

- Upgrade device running with SLX-OS to 20.8.1 before attempting migration
- Valid image is available on SCP/FTP/SFTP/TFTP server or USB
- Reachability to the image server
- Management VRF details (if applicable)
- Maintenance window approved (device reboot required)
- Back-up running configuration before migration



Note

- ONIE menu behavior may vary based on platform and BIOS version.
- When a full ONIE menu is present, **ONIE Rescue mode cannot be used** for ONIE-uninstaller.

About This Task

This method uses the **firmware download migrate** command and is supported from **SLX-OS 20.8.1 and later**.

Procedure

1. Log in to the device running **SLX-OS**.
2. Run the firmware migration command using the appropriate protocol.

```
firmware download migrate <protocol> [options]
```

SCP Example (with VRF):

```
firmware download migrate scp user <username> password <password> host <host-ip>  
directory <image-path> use-vrf mgmt-vrf file <image-name>
```

3. Review all system-generated warnings carefully, including:
 - Hardware profile changes
 - MTU default reset warnings
 - Maximum-path restrictions
 - Confirmation that TPVM partition will be deleted
4. Type **y** and press **Enter** to proceed when prompted.

```
Do you want to continue? [y/n]:
```

The system performs the following:

- Download the OS ONE image
- Validate the image
- Install the firmware
- Automatically reboot the device

5. Perform the Post-Migration Mandatory Actions.

a. Log in using default credentials:

- Username: admin
- Password: password

a. Perform **System Firmware Commit**.

```
system firmware commit
```

b. Verify that OS ONE is correctly installed:

```
show firmware
```

OS ONE to SLX-OS Migration

This procedure provides instructions to migrate supported platforms from **OS ONE** to **SLX-OS** using ONIE.

Supported Migration Method

ONIE Install (clean install using ONIE)



Important

- Migration is **disruptive** and may impact traffic during reboot.
- Configuration is erased during this process. Ensure a backup/restore plan is in place.

SLX-OS Image Selection (Mandatory)



Note

Use the correct image for the hardware platform. Do not interchange images.

SLX-OS Image File Name	Supported Platforms
SLXOS_SWBD3200-20.8.1slxos20.8.11_231201_1030-ONIE.bin	8720, 8520-48XT, 8520-48Y
SLXOS_SWBD4200-20.8.1slxos20.8.1_231201_1030-ONIE.bin	8820-40C, 8820-80C

Install SLX-OS on OS ONE Platforms

You can install SLX-OS on OS ONE platforms.

Before You Begin

- ONIE menu behavior may vary by platform/BIOS.
- Always verify platform-to-image mapping before installation.
- Reapply configuration after migration (backup/restore).

About This Task

Follow this procedure to install SLX-OS on OS ONE platforms.

Procedure

1. Reboot into ONIE.
 - a. Reboot from OS ONE CLI and press Esc within 5 seconds to enter GRUB.
 - b. Select ONIE.

If full ONIE menu is unavailable, use ONIE Rescue.
2. Ensure management connectivity on eth0/eth1 (DHCP or static).
3. Remove the existing OS ONE.

```
onie-uninstaller
```

This may take 20–30 minutes. The device reboots automatically.

4. Install the correct SLX-OS image using the supported methods.

Replace <SWBDxxxx> with the mapped image for your platform.

- HTTP / Wget

```
onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
```

- TFTP

```
tftp -g -r SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin <TFTP_Server_IP>
onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
```

- FTP

```
ftpget -u <username> -p <password> <Server-IP>
SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin onie-nos-install
SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
```

- USB

```
mkdir /mnt/usb
```

```
mount /dev/sda1 /mnt/usb onie-nos-install /mnt/usb/
SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
```

- HTTP / Wget

```
onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
```

5. Perform post-installation validation.

```
dhcp ztp cancel
```

```
show version
```

Supported Upgrade Paths

This section provides the supported path for upgrading to Extreme OS ONE Switching and Routing 22.2.3.0.

- Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0

- Extreme OS ONE Switching and Routing from 22.2.1.0 to 22.2.2.0
- Extreme OS ONE Switching and Routing from 22.2.2.0 to 22.2.3.0

Upgrade Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0

You can upgrade Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0.

About This Task



Note

- The Extreme OS ONE Switching and Routing 22.2.1.0 image format is OOneSR-22.2.3.0-110.bin.
- To upgrade from 22.2.1.0 to 22.2.2.0 or from 22.2.2.0 to 22.2.3.0, follow the regular upgrade workflow.

For a detailed procedure, see [Upgrade Extreme OS ONE Firmware Using CLI](#).

- When upgrading 8720-32C devices from 22.2.1.0 to 22.2.2.0 or from 22.2.2.0 to 22.2.3.0 with XCO deployment/TPVM installed or under heavy load, LACP port channels may flap before the device reboots and upgrades to 22.2.2.0 or 22.2.3.0.
- As a best practice, before upgrading devices, enable maintenance mode on the setup using the **system maintenance-mode enable** command.

Follow this procedure to upgrade Extreme OS ONE Switching and Routing from 22.2.0.0 to 22.2.1.0.

Procedure

1. Backup existing configurations.
 - a. Back up the current configuration and export it to a remote server. Run the following command:

```
copy running-config file scp://user:password@<IP>:/home/user/user.config
```

2. Complete a fullinstall of Extreme OS ONE firmware.
See [Firmware Fullinstall Support](#) on page 23.
3. Post installation, users must change the default password.
 - a. Provide the old password.
 - b. Update the new password for the default admin user and grub.
 - c. User login is successful with the new password.
 - d. Make sure to note down the new password. If forgotten, contact Extreme Networks for assistance.
4. Post login, wait for the following messages:

```
*****  
System is ready for all commands  
*****
```

```
App SR Installation completed.
```

5. Import the backup configuration file using the following command:

```
copy file scp://user:password@<IP>:/home/user/user.config running-config
```

6. Config file replay takes some time to complete based on the scale of the config.
Please wait for it to complete.