Extreme ONE OS Switching v22.2.1.0 Deployment Guide

Installation, Configuration, and Firmware Upgrades

9039421-00 Rev AA
December 2025

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/

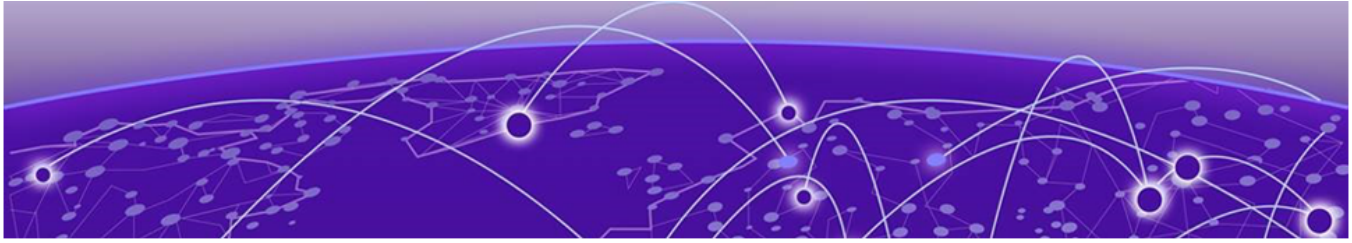
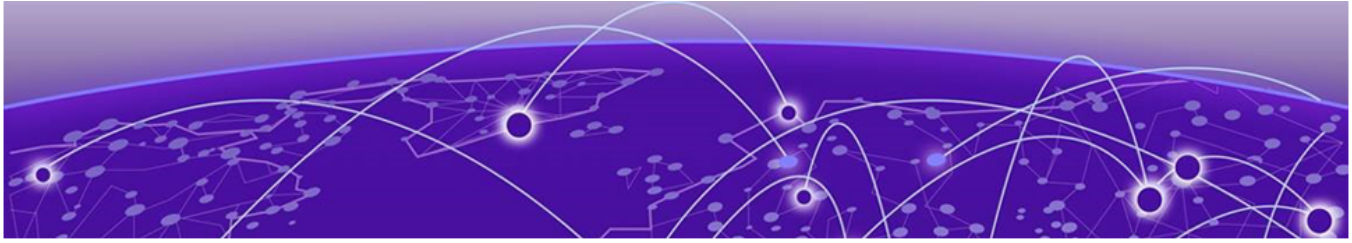


Table of Contents



Abstract

This Extreme ONE OS Switching Deployment Guide version 22.2.1.0 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 400G 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 *enter* and *type*	When you see the word *enter* 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 *type*.
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**
Words in italicized type	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.
italic 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, *member*[*member*...].
\	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 ONE OS Switching, release 22.2.1.0:

Feature	Description	Link
ONE OS Upgrade Switching	Updated procedure of the existing topic "Upgrade Extreme ONE OS Switching Release 22.2.0.0 to Release 22.2.1.0".	Upgrade Extreme ONE OS Switching Release 22.2.0.0 to Release 22.2.1.0 on page 33

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

Supported Platforms

Extreme ONE OS Switching 22.2.1.0 supports 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

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

Supported Device Information

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

Extreme ONE OS Software

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

Extreme ONE OS architecture comprises of various components composed as microservices, such as LLDP microservice and the BFD microservice. Extreme ONE OS 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 ONE OS Switching 22.2.1.0 provides switching and routing capabilities.

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

- FTP
- TFTP
- HTTP

- NFS
- USB

Extreme ONE OS Software Operating System

Extreme ONE OS is built using the standard ONLP (Open Network Linux Platform) procedure. Installation of Extreme ONE OS 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 offers operational diagnostics, a suite of tests provided by Alpha as a bootable image. This image is installed on the switch and accessible through Extreme ONE OS. 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, run 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

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# system internal update opdiag disk://firmware/summit-aoede.1.0T-2
32d# start-shell
[admin@32d]# sudo bash
[root@32d]# ls /mnt/onl/diagnostics/
lost+found  operational-results-1.txt  summit-aoede.1.0T-2
[root@32d]#
```

BMC Thermal Policy

Use this topic to learn about the BMC 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, Extreme ONE OS 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 ONE OS 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 ONE OS takes it out of reset mode.
- Info log: "QSFP 5 taken out of reset mode"

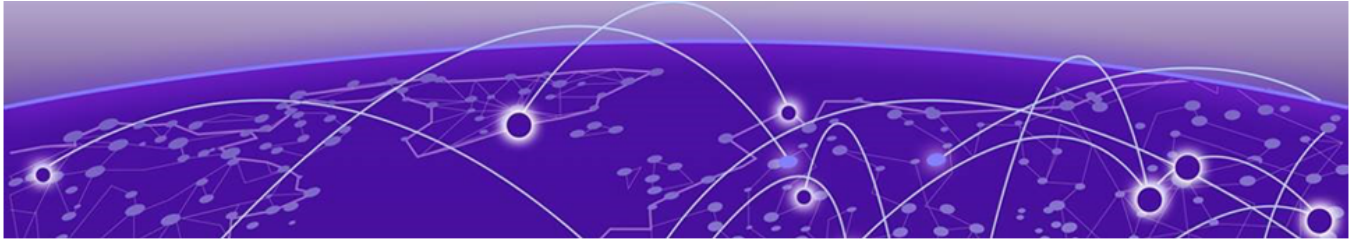
Continuous Reset Mode

If the optics enters reset mode and is subsequently taken out of reset mode five times via software, the user will need to 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

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

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

Install Extreme ONE OS Switching Software Using ONIE

Before You Begin

ONIE (Open Network Install Environment) 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 ONE OS Switching 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:
  - Availability of a DHCP server on the LAN for this Ethernet interface might 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

Perform the following steps from the serial console:

Procedure

1. Access the ONIE Recovery Shell.

   After updating the passwords, the system will confirm 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 will be prompted to update the default password. For more information. see *Force Password Change at First Login* in the *Extreme ONE OS Switching Management Configuration Guide.*
   - **Changing Admin and Grub Passwords:**: During the first login via CLI, users will be 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) : ONE OS 'admin' and Grub 'root' user passwords
updated successfully
device#
```

   a. Reboot the device using the CLI or power-cycle.
   b. When the BIOS 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:
   - After a factory reset, both admin and Grub passwords will be reset and must be changed by the user.
   - When entering the ONIE prompt during reload, users will need to 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. Perform one of the following:
   - 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, perform 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 ONE OS firmware using one of the following remote server methods:
   - Perform USB Disk-Based Recovery on page 20
   - Perform NFS-Based Recovery on page 20
   - Perform HTTP-Based Recovery on page 21
   - Perform FTP-Based Recovery on page 21
   - Perform TFTP-Based Recovery 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`.

Perform USB Disk-Based Recovery

About This Task

Follow this procedure to perform USB disk-based recovery.

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 should mount.
6. Change directory to the Extreme ONE OS 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 ExtremeOneSR-22.2.1.0.bin_<version_date_build>_UTC
   ```

   The device reboots and loads the software.

Perform NFS-Based Recovery

About This Task

Follow this procedure to perform NFS-based recovery.

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 ONE OS software that you want to install.

```
ONIE:/ #cd media/

ONIE:/ media/ #ls ExtremeOneSR-22.2.1.0.bin_<version_date_build>_UTC
```

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.

Perform HTTP-Based Recovery

About This Task

Follow this procedure to perform HTTP-based recovery.

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>/
ExtremeOneSR-22.2.1.0.bin_<version_date_build>_UTC
```

Perform FTP-Based Recovery

About This Task

Follow this procedure to perform FTP-based recovery.

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>/
   ExtremeOneSR-22.2.1.0.bin_<version_date_build>_UTC
   ```

Perform TFTP-Based Recovery

About This Task

Follow this procedure to perform TFTP-based recovery.

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>/
   ExtremeOneSR-22.2.1.0.bin_<version_date_build>_UTC
   ```

Firmware Fullinstall Support

This topic outlines the step-by-step process for performing a full, clean install of the provided Extreme ONE OS 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 ExtremeONEOS binary image.

Key Features

- Complete clean firmware installation using the Extreme ONE OS CLI
- Managed partition deletion and creation
- Replacement of current configuration with default Extreme ONE OS 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 ONE OS Configuration and Certificate Changes

Extreme ONE OS Configurations: Installing new firmware will overwrite your current configuration with the default Extreme ONE OS 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 will be 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 users can prefer not to preserve using optional parameter no-preserve. whereever 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 ONE OS firmware. Here's what it does: • Deletes all device partitions • Preserves management certification files by default (unless 'no-preserve' option is used) • Initiates new ExtremeONE OS firmware installation from ONIE • Restores SSH configuration file and necessary certification files"		

Help strings	32d# system firmware
	  commit Commit firmware version
	  fullinstall Full Install firmware on switch
	  rollback firwmare 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> [vrf vrf-name] -OR- http[https]:
	//[username:password@]<host>[:port]/<filepath> [vrf vrf-name]
	32d# system firmware fullinstall <image path>
	# system firmware fullinstall dis <cr>
	  no-preserve Remove management certificates

Error messages	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].
Related commands	show version, show firmware

Related PROTO files	The following openconfig gNOI RPC are used or supported:
	`rpc Activate(ActivateRequest) returns (ActivateResponse);`
	`rpc Verify(VerifyRequest) returns (VerifyResponse);`
	The following are the corresponding Request and Response messages:
	`// 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 immediatelly`
	`  // 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.`
	`//`

	`// 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;`
	`}`

Example output using gNOI	`$ 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/ExtremeOneSR-22.2.1.0.bin`

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
```

Upgrade the Extreme ONE OS Firmware Using CLI

The Extreme ONE OS 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.

About This Task

Follow this procedure to upgrade the firmware.

Procedure

1. Back up the running configuration on the device.

   You will restore the backed up configuration after you upgrade the firmware.

```
# copy running-config file disk://config-file/<yourconfig.cfg>
```

2. Copy the default configuration on the device.

```
# copy default-config running-config
```

3. 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
```

   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 `RR_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. When the microservices come up, the `Firmware Rev` property in the `chassis-0` component is published to `State DB` with the running firmware image.
- If any microservice fails to come up within the specified duration, an automatic rollback to the previous image is triggered.

4. Restore the backed up configuration.

```
# copy file disk://config-file/yourconfigfile.cfg running-config
```

5. (Optional) If the new firmware version is not required, revert to the previous version.

```
# system firmware rollback
```

Upgrade Firmware on the 8730 Hardware Platform

Use this topic to learn about the various firmware upgrades on 8730-32D platform.

About This Task

Note
USB flash drives are compatible with FAT, EXT, and NTFS file systems.

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

Procedure

1. Upgrade BMC on 8730-32D.

   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 8730-32D.

   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 will download and validate the firmware file.
    b. The system will flash the firmware on the um-switch, which may take several minutes.
    c. The um-switch will reset 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.

   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.

   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 will download and validate the firmware file.
  b. The firmware will be flashed onto the micro-controller.
  c. The system will reboot.

- Important Notes
  - Do not interrupt the power supply during the upgrade process.
  - The um-switch will be inaccessible during this time.
- Verification
  - After the system reboots, check the version of HwRoT in the boot logs.
  - The version will be 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 will be displayed on the console, indicating the cause of the failure

5. Upgrade Power/CPU/Port -CPLD.

   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 will take several minutes to complete. Upon completion, a success message will be 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.

  This will display the System CPLD version, including the Port-CPLD, Power-CPLD, and CPU-CPLD versions.

Supported Upgrade Paths

This section provides the supported path for upgrading to Extreme ONE OS Switching, Release 22.2.1.0.

- Extreme ONE OS Switching Release 22.2.0.0 to Release 22.2.1.0

Upgrade Extreme ONE OS Switching Release 22.2.0.0 to Release 22.2.1.0

About This Task

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

Note

To upgrade from Release 22.2.0.0 to Release 22.2.1.0, follow the full install procedure.

For detail procedure, see Firmware Fullinstall Support on page 23..

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. Perform fullinstall of Extreme ONE OS firmware.

   See Firmware Fullinstall Support on page 23.

3. Post installation, users are required to change the default password.
   a. Provide the old password.
   b. Update the new password for the default admin user and grub.
   c. User login will be 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. Cancel the ZTP process using the following command:

```
ztp dhcp cancel
```

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

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

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